IEC 62645

Edition 1.0 2014-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems

Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

X

ICS 27.120.20

ISBN 978-2-8322-1810-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – REQUIREMENTS FOR SECURITY PROGRAMMES FOR COMPUTER-BASED SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62645 has been prepared by subcommittee 45A: Instrumentation, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/961/FDIS	45A/975/RVD

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site 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.

The contents of the corrigendum of March 2015 have been included in this copy.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the standard

This standard specifically focuses on the issue of requirements for computer security programmes and system development processes to prevent and/or minimize the impact of attacks against I&C computer-based systems possibly integrating HPD (HDL (Hardware Description Language) Programmed Devices), hereinafter named I&C CB&HPD systems.

This standard was prepared and based on the ISO/IEC 27000 series, IAEA and country specific guidance in this expanding technical and security focus area.

It is intended that the Standard be used by designers and operators of nuclear power plants (NPPs) (utilities), licensees, systems evaluators, vendors and subcontractors, and by licensors.

b) Situation of the current Standard in the structure of the IEC SC 45A standard series

IEC 62645 is a second level IEC SC 45A document, tackling the generic issue of NPP I&C cybersecurity.

IEC 62645 is considered formally as a second level document with respect to IEC 61513, although IEC 61513 needs revisions to actually ensure proper reference to and consistency with IEC 62645. IEC 62645 is the top-level document with respect to cyber security in the SC 45A standard series. Other documents will be developed under IEC 62645 and will correspond to third level documents in the IEC SC 45A standards.

This IEC Standard is expected to coordinate more closely with the IEC 62443 (Bibliography) series in the next few years.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of this standard

This standard establishes requirements for I&C CB&HPD systems, with regard to computer security, and clarifies the processes that I&C CB&HPD systems are designed, developed and operated under in NPPs.

It is recognized that this standard addresses an evolving area of regulatory requirements, due to the changing and evolving nature of computer security threats. Therefore, the standard defines the framework within which the evolving country specific requirements may be developed and applied. An upcoming process for this standard is anticipated in the near term, to address these evolving issues. It is intended to take into account coordination with new IEC and ISO standards, evolving and new national regulations, best practices and technical advances from IEC members on issues including graded approach and security degrees, refined consideration of security requirements to meet plant performance objectives, risk assessment or cybersecurity of legacy systems.

It is also recognized that products derived from application of this subject matter require protection. Release of the standard's country specific requirements should be controlled to limit the extent to which organizations or individuals intending to access nuclear plant systems illegally, improperly or without authorization may benefit from this information.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these

documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45A standard series corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements SSR-2/1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NOTE It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied, that are based on the requirements of a standard such as IEC 61508.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – REQUIREMENTS FOR SECURITY PROGRAMMES FOR COMPUTER-BASED SYSTEMS

1 Scope

1.1 General

This International Standard establishes requirements and provides guidance for the development and management of effective security programmes for I&C computer-based systems for NPPs, possibly integrating HPD (HDL (Hardware Description Language) Programmed Devices), hereinafter named I&C CB&HPD systems. Inherent to these requirements and guidance is the criterion that the power plant I&C CB&HPD system security programme complies with the applicable country's I&C CB&HPD security requirements.

The primary objective of this standard is to define adequate programmatic measures for the prevention of, detection of and reaction to malicious acts by digital means (cyber attacks) on I&C CB&HPD systems. This includes any unsafe situation, equipment damage or plant performance degradation that could result from such an act, such as:

- malicious modifications affecting system integrity,
- malicious interference with information, data or resources that could compromise the delivery of or performance of the required I&C CB&HPD functions,
- malicious interference with information, data or resources that could compromise operator displays or lead to loss of management of I&C CB&HPD systems,
- malicious changes to hardware, firmware or software at the programmable logic controller (PLC) level.

Effective security policies need to implement a graded protection scheme, as described in this standard for assets subject to computer-based security, based on their relevance to the overall plant safety, availability, and equipment protection.

Excluded from the scope of this standard are considerations related to:

- non-malevolent actions and events such as accidental failures, human errors and natural events. In particular, good practices for managing applications and data software, including back-up and restoration related to accidental failure, which should be implemented even if I&C CB&HPD system security was not studied, are out of scope;

  NOTE 1 Although such aspects may be considered as covered by security programme in other normative contexts (e.g., in the ISO/IEC 27000 series, the IEC 62443 series or the NIST framework), this standard is only focused on the protection against malicious acts by digital means (cyber attacks) on I&C CB&HPD systems. This is made to provide the maximum consistency and the minimum overlap with other nuclear standards and practices, which already cover accidental failures, unintentional human errors, natural events, etc.

- site physical security and room access control and site security surveillance systems. These issues, while not addressed in this standard, should still be addressed by plant operating procedures and programmes.

  NOTE 2 This exclusion does not deny that cyber security has clear dependencies on the security of the physical environment (e.g., physical protection, power, heating/ventilation/air-conditioning systems (HVAC) , etc.).

Standards such as ISO/IEC 27001 and ISO/IEC 27002 are not directly applicable to the cyber protection of nuclear I&C CB&HPD systems. This is mainly due to the specificities of these systems, including the regulatory and safety requirements inherent to nuclear facilities.

However, this standard builds upon the valid high level principles and main concepts of ISO/IEC 27001 and 27002, adapts them and completes them to fit the nuclear context.

Particular differentiators that justify a targeted NPP I&C CB&HPD system standard include:

- These systems are required to comply with IEC safety standards related to nuclear power plant I&C systems.
- A cyber attack could lead to significant adverse effects on plant equipment, reliable plant operation, or safety and may result in major impact to surrounding population, plant personnel and the environment.
- Target of cyber threats are typically equipment and process, but may include I&C CB&HPD systems. I&C CB&HPD systems may also be used as the attack vectors.
- The unavailability of a NPP's I&C system due to cyber attack may place the plant in an unacceptable safety position and increase the likelihood of nuclear accidents.
- The effect of a cyber attack may jeopardize or degrade critical devices such as the turbo-generator set or the line transformer, and thus may generate expensive repairs and cause long plant unavailability.
- A nuclear facility operates at a high level of safety and requires rapid, real time responses to emerging situations. An operator shall respond quickly to inputs and available data and shall be able to rely on what information is available.

The possible damage resulting from a cyber attack at a nuclear facility has the potential for much greater impact than that occurring at other industrial facilities. Therefore, while existing and future industrial cyber security guidance may provide information and procedures beneficial to nuclear facilities, a targeted nuclear standard is still required.

NOTE This edition of IEC 62645 is aligned to the defined editions of ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002. A future revision will update this standard to align to the new editions of these standards. In the meantime, the user should exercise caution in reconciling the technical differences between these documents.

1.2 Application

This standard is limited to computer security of I&C CB&HPD systems (including non-safety systems) used in a NPP. This standard is intended for use in evaluating or changing established NPP security programmes for I&C CB&HPD systems, and in establishing new programmes. This standard is applied to all NPP I&C CB&HPD systems throughout the life cycles of these systems, as specified in this standard. It may also be applicable to other types of nuclear facilities.

NOTE The term NPP is understood in its site acceptance, NPP I&C CB&HPD system including systems within the NPP buildings, but also systems in the nuclear plant switchyard, water treatment facilities, etc.

1.3 Framework

Figure 1 presents the overall framework of this standard, with its normative clauses:

- Clause 5 deals with a security life-cycle on the programme level; its approach is consistent with the ISO/IEC 27001 Plan Do Check Act (PDCA) loop (with "security programme" here corresponding to "ISMS" in ISO/IEC 27001). Moreover, the graded approach and security categorization subclauses are organized in a similar way to IEC 61226.
- Clause 6 deals with a security life-cycle on a system level.
- Clause 7 deals with security thematic areas on a control level; its structure is consistent with the ISO/IEC 27002:2005 organization (and ISO/IEC 27001:2005, normative Annex A).

NOTE Annex B provides a correspondence table between the IEC 62645 structure and the ISO/IEC 27001:2005 structure. Annex C provides the same kind of correspondence with the NIST SP800-82 framework.

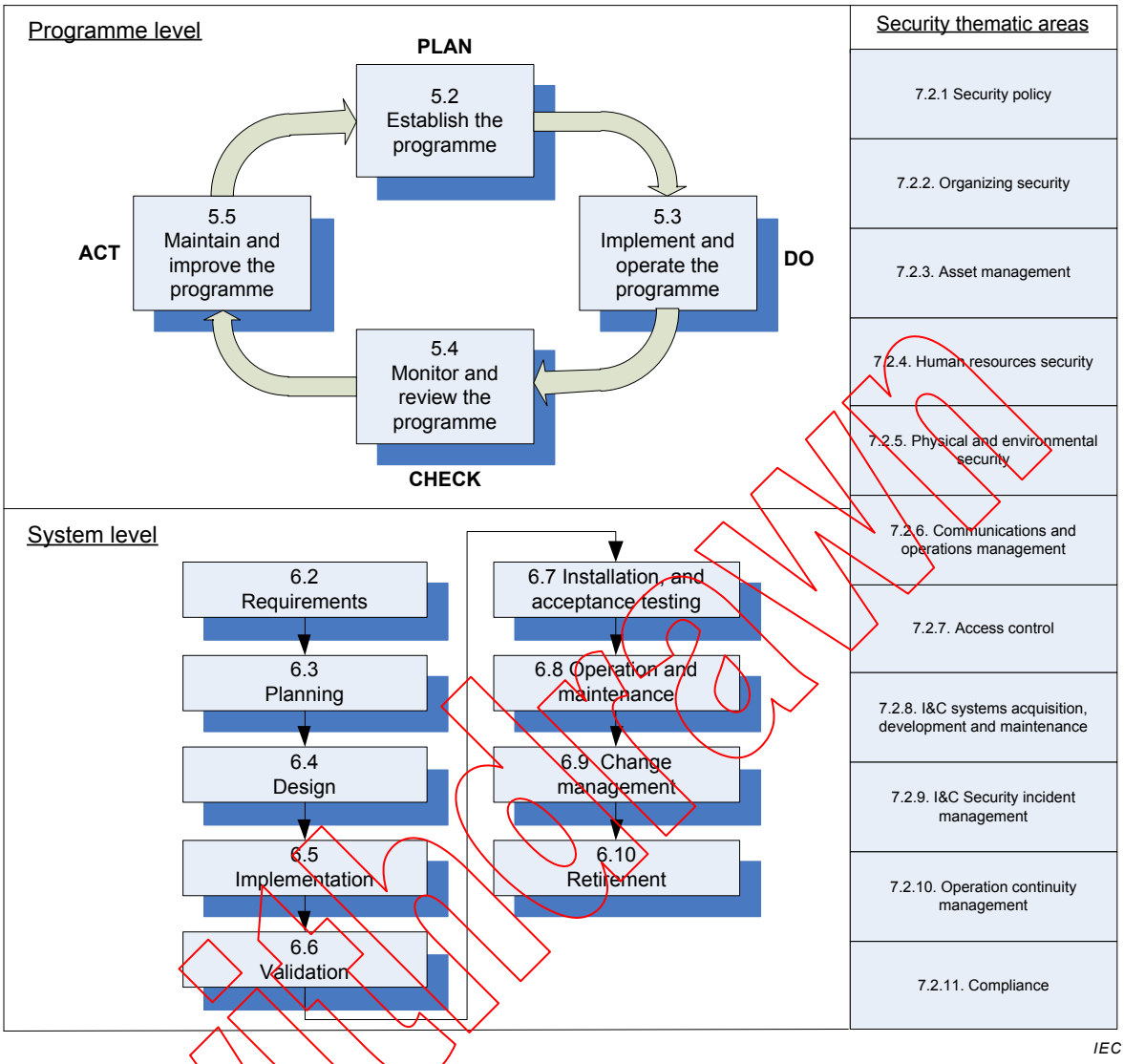

Figure 1 – Overall framework of IEC 62645

IEC 61513 addresses the concept of a safety life cycle for the total I&C system architecture, and a safety life cycle for the individual systems. As part of the overall framework, IEC 61513 calls for establishment of an overall security plan to specify the procedural and technical measures to be taken to protect the architecture of I&C systems from digital attacks that may jeopardise functions important to safety. The provisions of the overall security plan may differentiate between requirements for systems supporting category A, B or C functions, as defined in IEC 61226 and include the establishment of controls for electronic and physical access. This standard provides more detailed requirements for the overall security plan, as called for in IEC 61513.

Additional requirements for software of systems supporting category A functions are provided in IEC 60880 and IEC 62566. Additional requirements for software of systems supporting category B and C functions are provided in IEC 62138.

This standard also covers security requirements for I&C CB&HPD systems which are not in the scope of IEC 61513, IEC 60880, IEC 62138 and IEC 62566 but have a potential impact on plant equipment, availability and performance.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61226, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61513, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62566, *Nuclear power plants – Instrumentation and control important for safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

ISO/IEC 27000:2009, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*

ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE – EXIGENCES RELATIVES AUX PROGRAMMES DE SÉCURITÉ APPLICABLES AUX SYSTÈMES PROGRAMMÉS

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 62645 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et électriques des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/961/FDIS	45A/975/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.

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.

Le contenu du corrigendum de mars 2015 a été pris en considération dans cet exemplaire.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

a) Contexte technique, questions importantes et structure de la norme

La présente norme s'intéresse principalement à la question des exigences relatives aux programmes de sécurité informatique et aux processus de développement système pour empêcher les attaques contre les systèmes programmés d'I&C (Instrumentation et Contrôle-commande) qui potentiellement peuvent intégrer des HPD (circuits programmés en HDL(Langage de description de matériel)), ci-après nommés systèmes programmés-HPD d'I&C, et/ou minimiser les conséquences de ces attaques.

La présente norme a été préparée en utilisant comme documents de base: la série de normes ISO/IEC 27000, les recommandations particulières de l'AIEA et des pays qui existent pour ce domaine technique en expansion lié à sécurité.

La présente norme est destinée aux concepteurs, aux opérateurs de centrales nucléaires de puissance (producteurs d'électricité), aux organisations titulaires d'un permis d'exploitation, aux évaluateurs et aux vendeurs de systèmes, à leurs sous-contractants, ainsi qu'aux autorités de sûreté.

b) Position de la présente norme dans la collection de normes du SC 45A de l'IEC

L'IEC 62645 est un document de deuxième niveau de la collection des normes du SC 45A de l'IEC qui traite de la question générale de la cybersécurité.

L'IEC 62645 est formellement reconnue comme un document de deuxième niveau par rapport à l'IEC 61513, bien qu'il soit nécessaire de réviser celle-ci pour effectivement garantir une prise en compte appropriée de l'IEC 62645 et la consistance avec celle-ci. L'IEC 62645 est le document de niveau supérieur pour ce qui concerne la cybersécurité dans la série de normes du SC 45A de l'IEC. D'autres documents seront développés en dessous de l'IEC 62645 et correspondront à des documents de troisième niveau de la série de normes du SC 45A de l'IEC.

Il est prévu d'améliorer dans les prochaines années la coordination de la présente norme avec la série de norme IEC 62443 indiquée dans la bibliographie.

Pour de plus amples détails sur la structure de la collection des normes du SC 45A de l'IEC, voir le point d) de cette introduction.

c) Recommandations et limites relatives à l'application de la présente norme

La présente norme établit des exigences concernant les systèmes programmés-HPD d'I&C, pour ce qui concerne la sécurité informatique, et elle apporte des éléments de clarification pertinents pour les processus régissant la conception, le développement et l'exploitation des systèmes programmés-HPD d'I&C utilisés dans des centrales nucléaires de puissance.

Il est reconnu que la présente norme couvre le domaine des exigences réglementaires en la matière qui est en pleine évolution, ceci étant du à la nature changeante et mutante des menaces liées à la sécurité informatique. Ainsi la présente norme définit le cadre de travail dans lequel les exigences nationales particulières susceptibles d'évoluer peuvent être développées et appliquées. La décision de procéder à la mise à jour rapide de la présente norme est anticipée. L'intention est de coordonner cette norme avec les futures normes IEC et ISO, les évolutions des règles nationales existantes ainsi que les nouvelles normes publiées dans le futur, les meilleures pratiques et les avancées techniques faites par les membres de l'IEC sur ces questions, y compris celles concernant les approches graduées et les degrés de sécurité, les considérations portant sur l'amélioration des exigences de sécurité pour atteindre les objectifs de performances, d'évaluation des risques ou des systèmes légaux concernant la cybersécurité.

Il est aussi reconnu que les produits résultant de l'application du sujet en la matière nécessitent protection. Il convient que la diffusion des exigences normatives particulières nationales soit contrôlée pour limiter les possibilités offertes par ces informations à des organisations ou à des individus qui auraient l'intention d'accéder illégalement, de manière non appropriée ou sans autorisation à des systèmes des installations nucléaires.

d) Description de la structure de la collection des normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC est la norme IEC 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de l'IEC.

L'IEC 61513 fait directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme IEC 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par la norme IEC 61513, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la collection de normes du SC 45A de l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

L'IEC 61513 a adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales de l'IEC 61508-1, l'IEC 61508-2 et l'IEC 61508-4 pour le secteur nucléaire, pour ce qui concerne le domaine de la sûreté nucléaire. Dans ce domaine, l'IEC 60880 et l'IEC 62138 correspondent à l'IEC 61508-3 pour le secteur nucléaire. L'IEC 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales, dont les exigences sont comparables à des normes telles que l'IEC 61508.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE – EXIGENCES RELATIVES AUX PROGRAMMES DE SÉCURITÉ APPLICABLES AUX SYSTÈMES PROGRAMMÉS

1 Domaine d'application

1.1 Généralités

La présente Norme internationale établit des exigences et fournit des recommandations pour le développement et la gestion des programmes de sécurité des systèmes programmés pouvant potentiellement intégrer des HPD (systèmes programmés-HPD d'I&C) et utilisés pour les centrales nucléaires. Le critère de conformité du programme de sécurité de la centrale nucléaire aux exigences de sécurité nationales applicables aux systèmes programmés-HPD d'I&C est inhérent aux exigences et recommandations de la présente norme.

Le but principal de la présente norme est de définir les mesures liées au programme de sécurité, pour ce qui concerne la prévention, la détection et la réaction à des actes malveillants, réalisés en utilisant des moyens informatiques (cyberattaques), portant atteinte aux systèmes programmés-HPD d'I&C. Ceci comprend les situations non sûres, les endommagements d'équipements, la dégradation des performances de la centrale qui pourraient résulter d'une telle action, telles que:

- des modifications malveillantes affectant l'intégrité de systèmes,
- des interactions malveillantes avec des informations, des données ou des ressources qui peuvent compromettre l'exécution des fonctions de systèmes programmés-HPD d'I&C ou dégrader les performances associées à l'exécution de celles-ci,
- des interactions malveillantes avec des informations, des données ou des ressources qui peuvent perturber des affichages opérateur ou entraîner la perte du contrôle des systèmes programmés-HPD d'I&C,
- des modifications malveillantes du matériel, du micro-logiciel ou du logiciel au niveau automate programmable (PLC).

Les politiques de sécurité efficaces ont besoin de mettre en œuvre un schéma de protection gradué, tels que décrits dans la présente norme pour les actifs objets de la sécurité informatique, prenant en compte leur importance au niveau de la sûreté de l'ensemble de l'installation, de sa disponibilité et de la protection des équipements.

Les considérations suivantes sont exclues du domaine de la présente norme:

- Les actions et les évènements non malveillants tels que les défaillances accidentelles, les erreurs humaines et les phénomènes naturels. En particulier, les bonnes pratiques concernant la gestion des applications et des données logicielles, y compris les sauvegardes et les restaurations pour parer aux défaillances accidentelles, qu'il convient de mettre en œuvre même si la sécurité informatique de l'I&C n'était pas considérée, sont hors domaine de la présente norme.

  NOTE 1 Bien que dans d'autres contextes normatifs (par exemple dans la série ISO/IEC 27000, dans la série IEC 62443 ou dans le cadre NIST) de tels aspects puissent être considérés comme couverts par le programme de sécurité, la présente norme s'intéresse seulement à la protection contre les actes malveillants réalisés à partir de moyens numériques (cyberattaques) sur les systèmes programmés-HPD d'I&C. Cela pour garantir un maximum de consistance et un minimum de chevauchement avec les autres normes et les pratiques du secteur nucléaire, couvrant déjà les défaillances accidentelles, les erreurs humaines non intentionnelles et les risques naturels, etc.

- Les systèmes liés à la sécurité physique de site et aux contrôles d'accès aux salles et locaux et à la surveillance de site. Il convient que ces questions qui ne sont pas couvertes

par la présente norme soient quand-même prises en compte dans les programmes et les procédures d'exploitation de la centrale.

NOTE 2 Cette exclusion ne nie pas le fait que la cybersécurité dépend clairement de la sécurité de l'environnement physique (par exemple protection physique, alimentation électrique, systèmes de chauffage, de ventilation et de conditionnement de l'air (CVC), etc.).

Les normes telles que l'ISO/IEC 27001 et l'ISO/IEC 27002 ne sont pas directement applicables pour la cyberprotection des systèmes programmés-HPD d'I&C du nucléaire. Ceci est principalement dû à l'existence de spécificités propres à ces systèmes, qui comprennent les exigences de sûreté et règlementaires inhérentes aux installations nucléaires. Cependant la présente norme construite sur les principes pertinents de haut niveau et les principaux concepts de l'ISO/IEC 27001 et l'ISO/IEC 27002, les adapte et les complète pour qu'ils s'accordent au contexte nucléaire.

Les différences particulières qui justifient l'existence d'une norme spécifique pour l'I&C programmés-HPD des centrales nucléaires sont en particulier liées aux faits:

- que ces systèmes ont l'obligation d'être conformes aux normes de sûreté de l'IEC applicables aux systèmes d'I&C des centrales nucléaires;
- qu'une cyberattaque pourrait avoir des conséquences négatives significatives au niveau des équipements de la centrale, de l'exploitation fiable de la centrale, ou de sa sûreté ce qui pourrait se traduire par un impact majeur au niveau des populations environnantes, du personnel de la centrale et de l'environnement;
- que les cybermenaces portent typiquement sur les équipements et les processus, mais peuvent aussi inclure les systèmes programmés. Les systèmes programmés-HPD d'I&C peuvent aussi être utilisés comme des vecteurs d'attaque;
- que l'indisponibilité des systèmes d'I&C d'une centrale conséquence d'une cyberattaque peut mettre la centrale dans un état non acceptable par rapport à la sûreté et augmenter la probabilité d'accidents nucléaires;
- qu'une cyberattaque peut avoir pour conséquence la mise en danger ou l'endommagement d'équipements critiques, tels que l'ensemble turbogénérateur ou le transformateur réseau, et ainsi entraîner des réparations couteuses et de longues indisponibilités de la centrale;
- qu'une installation nucléaire fonctionne à un haut niveau de sûreté et nécessite des réponses temps-réel rapides lors des situations d'urgence. Un opérateur doit répondre rapidement en fonction des entrées et des données disponibles et doit pouvoir faire confiance à l'information qui est disponible.

Les dommages pouvant résulter d'une cyberattaque sur une installation nucléaire peuvent potentiellement avoir un impact bien plus important que celui qui pourrait être observé pour d'autres installations industrielles. Ainsi, alors que des recommandations portant sur la cybersécurité industrielle, existantes ou à paraître, peuvent fournir des informations et procédures utiles pour les installations nucléaires, une norme ciblée pour l'industrie nucléaire est quand même nécessaire.

NOTE La présente édition de l'IEC 62645 est alignée sur les éditions définies des ISO/IEC 27000, ISO/IEC 27001 et ISO/IEC 27002. Une prochaine révision alignera la présente norme sur les nouvelles éditions de ces normes. En attendant, il convient que l'utilisateur soit vigilant en réconciliant les différences techniques entre ces documents.

1.2 Application

L'application de la présente norme est limitée à la sécurité informatique des systèmes programmés-HPD d'I&C (y compris les systèmes non classés de sûreté) utilisés dans les centrales nucléaires. La présente norme est destinée à être utilisée pour l'évaluation ou pour la modification des programmes de sécurité de centrales nucléaires déjà établis pour les systèmes programmés-HPD d'I&C et pour établir de nouveaux programmes. La présente norme est appliquée pour tous les systèmes programmés-HPD d'I&C et pendant tout leurs cycles de vie, tel que spécifié dans la présente norme. Elle peut être aussi applicable à d'autres types d'installations nucléaires.

NOTE L'expression centrale nucléaire est comprise comme couvrant le site, les systèmes programmés-HPD d'I&C de la centrale nucléaire incluent ceux situés dans les bâtiments de la centrale nucléaire, mais aussi les systèmes des postes électriques associés à la centrale nucléaire, les installations de traitement des eaux, etc.

1.3 Cadre général

La Figure 1 présente le cadre général de la présente norme, ainsi que ses articles normatifs.

- L'Article 5 traite du cycle de vie de sécurité au niveau programme; son approche est cohérente avec la boucle de l'ISO/IEC 27001 Planifier-Déployer-Contrôler-Agir (PDCA) (où «le programme de sécurité» correspond ici au «SMSI» de l'ISO/IEC 27001). De plus, les paragraphes concernant l'approche graduée et la catégorisation de sécurité sont organisé d'une façon comparable à l'IEC 61226.
- L'Article 6 traite du cycle de vie de sécurité au niveau du système.
- L'Article 7 traite des parties thématiques de la sécurité au niveau des exigences et des mesures; sa structure est cohérente avec celle de l'ISO/IEC 27002:2005 (et de l'Annexe normative A de l'ISO/IEC 27001:2005).

NOTE L'Annexe B fournit un tableau de correspondance entre la structure de l'IEC 62645 et celle de l'ISO/IEC 27001:2005. L'Annexe C fournit le même genre de tableau de correspondance avec le cadre référentiel de la NIST SP800-82.

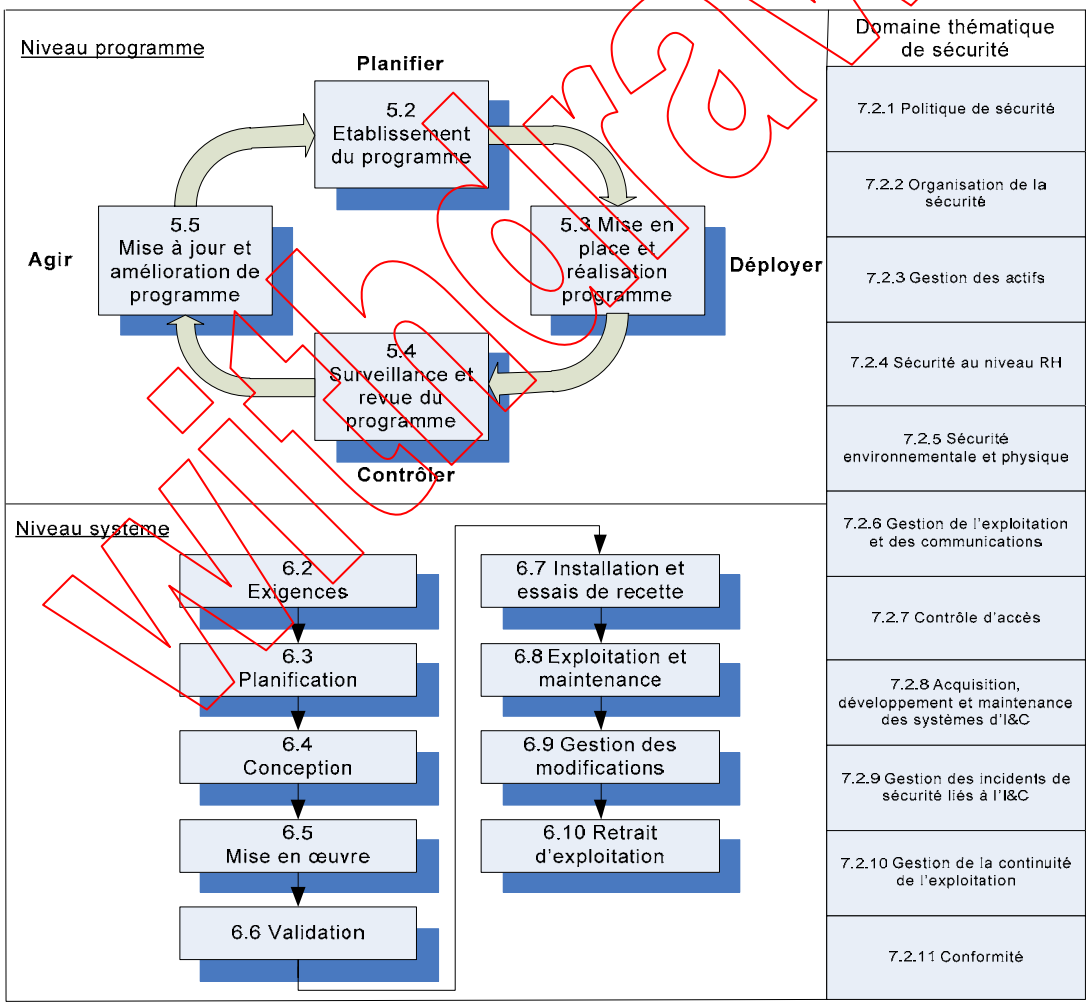

Figure 1 – Cadre général de l'IEC 62645

L'IEC 61513 présente le concept de cycle de vie de sûreté de l'architecture d'ensemble des systèmes d'I&C, et un cycle de vie de sûreté par système individuel. L'IEC 61513 demande la mise en place d'un plan de sécurité d'ensemble, pour préciser les mesures procédurales et

techniques à mettre en œuvre pour protéger l'architecture des systèmes d'I&C des attaques digitales qui peuvent mettre en péril des fonctions importantes pour la sûreté. Les dispositions du plan de sécurité d'ensemble peuvent faire la différence entre les exigences applicables aux systèmes réalisant des fonctions de catégorie A, B ou C, telles que définies dans l'IEC 61226 et comprendre la mise en place de contrôle d'accès au niveau physique et électronique. La présente norme établit des exigences plus détaillées portant sur le plan de sécurité, comme demandé par l'IEC 61513.

Des exigences supplémentaires portant sur le logiciel des systèmes support de fonctions de catégorie A sont fournies par l'IEC 60880 et l'IEC 62566. Des exigences supplémentaires portant sur le logiciel des systèmes support de fonctions de catégories B et C sont fournies par l'IEC 62138.

La présente norme traite aussi des exigences de sécurité portant sur les systèmes programmés-HPD d'I&C qui sont hors des domaines des normes IEC 61513, IEC 60880, IEC 62138 et IEC 62566, mais qui peuvent avoir un impact possible sur les équipements de la centrale, sa disponibilité et ses performances.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

IEC 61226, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

IEC 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 62138, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

IEC 62566, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A*

ISO/IEC 27000:2009, *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (disponible en anglais seulement)

ISO/IEC 27001:2005, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l information – Exigences*

ISO/IEC 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*

ISO/IEC 27005:2011, *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information*