IEC 62645

Edition 2.0 2019-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements

Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique – Exigences relatives à la cybersécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-7548-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY REQUIREMENTS

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 power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 2014. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) to align the standard with the new revisions of ISO/IEC 27001;
b) to review the existing requirements and to update the terminology and definitions;
c) to take account of, as far as possible, requirements associated with standards published since the first edition;
d) to take into account the fact that cybersecurity techniques, but also national practices evolve.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1289/FDIS	45A/1295/RVD

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

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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 International Standard focuses on the issue of cybersecurity requirements to prevent and/or minimize the impact of attacks against I&C programmable digital systems on nuclear safety and plant performance. It covers programme level, architectural level and system level requirements.

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 International 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 revision to actually ensure proper reference to and consistency with IEC 62645. IEC 62645 is the top-level document with respect to cybersecurity in the SC 45A standard series. Other documents are developed under IEC 62645 and correspond to third level documents in the IEC SC 45A standards.

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 programmable digital systems, with regard to computer security, and clarifies the processes that I&C programmable digital 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 a framework within which the evolving country specific requirements may be developed and applied.

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 documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series

and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implement and detail the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 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.

NOTE 2 IEC/SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held within IEC/SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC/SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published, this Note 2 of the introduction of IEC/SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY REQUIREMENTS

1 Scope

1.1 General

This document establishes requirements and provides guidance for the development and management of effective computer security programmes for I&C programmable digital systems. Inherent to these requirements and guidance is the criterion that the power plant I&C programmable digital system security programme complies with the applicable country's requirements.

This document defines adequate measures for the prevention of, detection of and reaction to malicious acts by digital means (cyberattacks) on I&C programmable digital 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 programmable digital functions;

– malicious interference with information, data or resources that could compromise operator displays or lead to loss of management of I&C programmable digital systems;

– malicious changes to hardware, firmware or software at the programmable logic controller (PLC) level.

Human errors leading to violation of the security policy and/or easing the aforementioned malicious acts are also in the scope of this document.

This document describes a graded approach scheme for assets subject to digital compromise, based on their relevance to the overall plant safety, availability, and equipment protection.

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

– non-malevolent actions and events such as accidental failures, human errors (except those impacting the performance of cybersecurity controls) and natural events. In particular, good practices for managing applications and data, including back-up and restoration related to accidental failure, are out of scope;

  NOTE 1 Although such aspects are often covered by security programme in other normative contexts (e.g., in the ISO/IEC 27000 series or in the IEC 62443 series), this document is only focused on the protection against malicious acts by digital means (cyberattacks) on I&C programmable digital systems. The main reason is that in the nuclear generation domain, other standards and practices already cover accidental failures, unintentional human errors, natural events, etc. The focus of IEC 62645 is made to provide the maximum consistency and the minimum overlap with these other nuclear standards and practices.

– site physical security, room access control and site security surveillance systems. These systems, while not specifically addressed in this document, are to be covered by plant operating procedures and programmes;

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

– the aspect of confidentiality of information about I&C digital programmable systems is out of the scope of this document (see 5.4.3.2.3).

Annex A provides a rationale for and comments about the scope, definition and the document's application, and in particular about the exclusions and limitations previously mentioned.

Standards such as ISO/IEC 27001 and ISO/IEC 27002 are not directly applicable to the cyber protection of nuclear I&C programmable digital systems. This is mainly due to the specificities of these systems, including the regulatory and safety requirements inherent to nuclear facilities. However, this document builds upon the valid high level principles and main concepts of ISO/IEC 27001:2013, adapts them and completes them to fit the nuclear context.

This document follows the general principles given in the IAEA reference manual NSS17.

1.2 Application

This document is limited to computer security of I&C programmable digital systems (including non-safety systems) used in a NPP as well as associated computer-based tools. This document is applicable to the parts of electrical power systems covered by IEC 63046 which rely on digital programmable technology.

NOTE 1 For the sake of simplicity, the terms “I&C programmable digital systems” in the text refer both to I&C and the parts of electrical power systems covered by IEC 63046 which rely on digital programmable technology.

This document is intended for use in evaluating or changing established NPP security programmes for I&C programmable digital systems, and in establishing new programmes. This document is applied to all NPP I&C programmable digital systems throughout the life cycles of these systems, as specified in this document. It may also be applicable to other types of nuclear facilities.

NOTE 2 The term NPP is understood in its “physical site” meaning, NPP I&C programmable digital systems including systems within the NPP buildings, but also systems in the nuclear plant switchyard, water treatment facilities, etc.

1.3 Framework

The requirements and recommendations of this document are structured along three main normative clauses.

Clause 5 deals with cybersecurity on the programme life-cycle level; its approach is completely consistent with ISO/IEC 27001:2013. It is based on its structure and content, which are when needed, adapted and completed to fit the nuclear context specificities. Annex C provides a clause-to-clause correspondence table between the IEC 62645 structure and the ISO/IEC 27001:2013 structure. When direct references to ISO/IEC 27001:2013 content are made, the following terminological substitutions are to be made:

– the terms “information security management system” used in the referenced ISO/IEC 27001:2013 content correspond to “I&C digital programmable system cybersecurity program” in this document (as defined in Clause 3);

NOTE 1 This document focuses on the part of the program, or the dedicated program, related to I&C. This can be part of a larger program at the corporate level, which is out of the scope of this document.

– the term “information security” used in the referenced ISO/IEC 27001:2013 content correspond to “cybersecurity” in this document (as defined in Clause 3);

– the terms “information security policy” used in the referenced ISO/IEC 27001:2013 content correspond to “I&C digital programmable system policy” in this document.

NOTE 2 Some subclauses of ISO/IEC 27001:2013 contain internal references to other subclauses of ISO/IEC 27001. When relevant, the references used in these subclauses are to be considered in the IEC 62645 context, however, they do not reference IEC 62645 subclauses. See Annex C for help in the correspondences.

The subclauses related to the graded approach and security categorization are organized in a similar way to IEC 61226.

Clause 6 deals with cybersecurity on a system life-cycle level. It is structured along the system life-cycle of IEC 61513, adapted to take into account specifics of cybersecurity.

Clause 7 deals with cybersecurity at the cybersecurity control level. It provides the high level principles of an approach consistent with ISO/IEC 27002:2013, further detailed in IEC 63096.

Figure 1 presents the overall framework of this document.

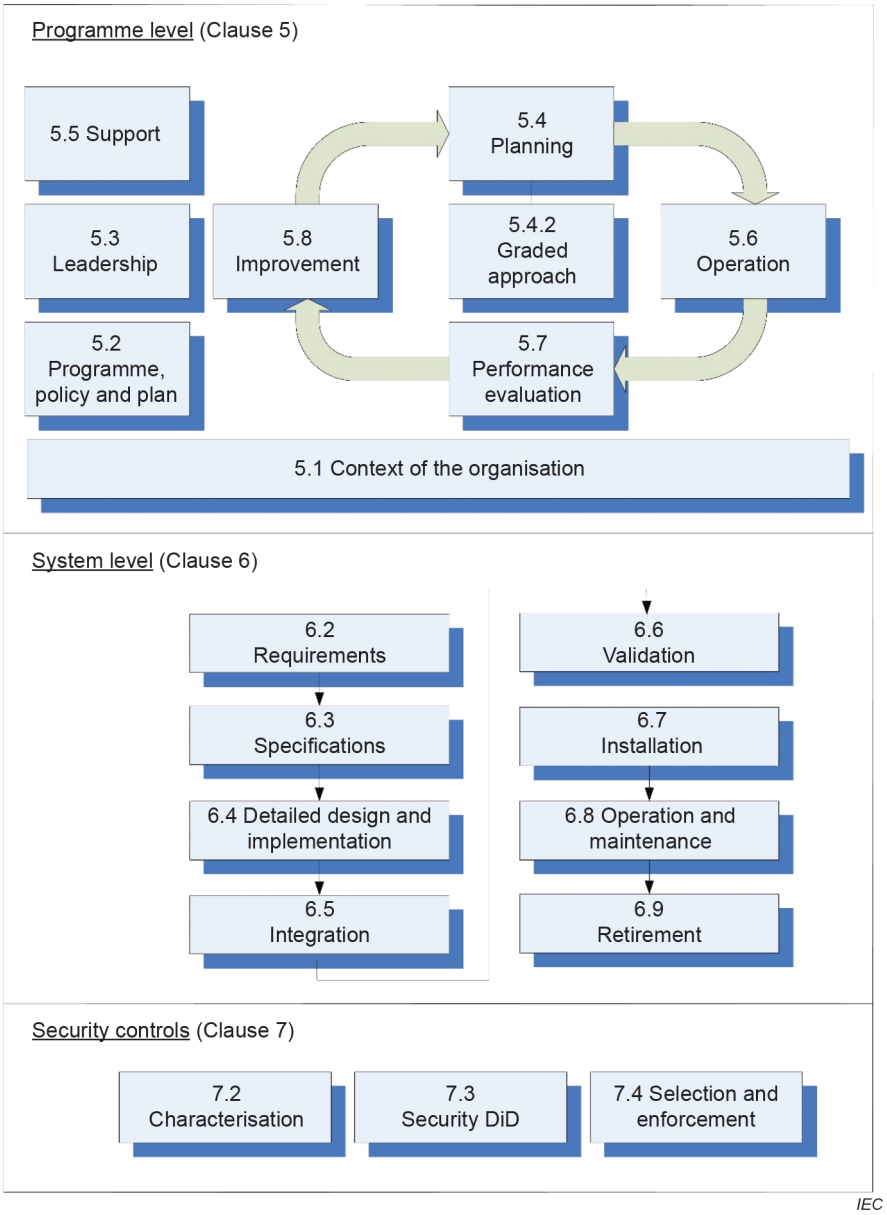

Figure 1 – Overall framework of IEC 62645

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 jeopardize 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 document 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 document also covers security requirements for I&C programmable digital 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 are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

IEC 62988:2018, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of wireless devices*

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

ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management*

IAEA TLD-006, *Conducting Computer Security Assessments at Nuclear Facilities,* 2016

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION, DE CONTRÔLE-COMMANDE ET D'ALIMENTATION ÉLECTRIQUE – EXIGENCES RELATIVES À LA CYBERSÉCURITÉ

AVANT-PROPOS

1) La Commission Électrotechnique 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. À 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 d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition parue en 2014. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) aligner la norme sur les nouvelles révisions de l'ISO/IEC 27001;
b) passer en revue les exigences existantes et mettre à jour la terminologie et les définitions;
c) prendre en compte, autant que possible, les exigences associées aux normes publiées depuis la parution de la première édition;

d) prendre en compte le fait que les techniques de cybersécurité, mais aussi les pratiques nationales évoluent.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1289/FDIS	45A/1295/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 internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document 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 au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

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 internationale s'intéresse principalement à la question des exigences relatives à la cybersécurité pour empêcher et/ou réduire le plus possible l'impact des attaques contre les systèmes numériques programmables d'I&C (Instrumentation et Contrôle-commande) sur la sûreté nucléaire et les performances d'une centrale. Elle couvre les exigences au niveau du programme, au niveau architectural et au niveau du système.

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 internationale 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 le document de deuxième niveau du SC 45A de l'IEC qui traite de la question générale de la cybersécurité des systèmes d'I&C utilisés dans des centrales nucléaires de puissance.

L'IEC 62645 est formellement reconnue comme un document de deuxième niveau par rapport à la norme IEC 61513, bien qu'il soit nécessaire de réviser cette dernière pour effectivement garantir une prise en compte appropriée de l'IEC 62645 et y être cohérent. 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 sont élaborés selon l'IEC 62645 et correspondent à des documents de troisième niveau de la série de normes du SC 45A de l'IEC.

Pour de plus amples détails sur la structure de la collection de 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 numériques programmables 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 numériques programmables 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 dû à la nature changeante et évolutive des menaces liées à la sécurité informatique. Ainsi, la présente norme définit un cadre de travail dans lequel les exigences nationales particulières susceptibles d'évoluer peuvent être élaborées et appliquées.

Il est aussi reconnu que les produits résultant de l'application du sujet en la matière exigent une protection. Il convient que la diffusion des exigences normatives particulières nationales soit contrôlée pour limiter les cas où ces informations peuvent profiter 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 de normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont l'IEC 61513 et l'IEC 63046. L'IEC 61513 traite des exigences générales 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 de puissance. L'IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique des centrales nucléaires de puissance; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. L'IEC 61513 et l'IEC 63046 doivent être considérées ensemble et au même niveau. L'IEC 61513 et l'IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

L'IEC 61513 et l'IEC 63046 font 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, la défense contre les défaillances de cause commune, la conception des salles de commande, la compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec l'IEC 61513 et l'IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont pas référencées directement par l'IEC 61513 ou l'IEC 63046, sont relatives à des matériels particuliers, à des méthodes techniques 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.

Les normes de la collection de documents produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes et aspects fondamentaux de sûreté et de sécurité établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires de puissance, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires de puissance, avec le guide de sûreté SSG-39 qui traite de la conception des systèmes d'instrumentation et de contrôle-commande des centrales nucléaires de puissance, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires de puissance, et avec le guide de mise en œuvre NSS 17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de la publication fondamentale de sécurité IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau de la sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce cadre, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au deuxième niveau, la norme IEC 62645 est le document chapeau des normes du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes pertinents de haut niveau et des concepts principaux des normes génériques de sécurité, en particulier l'ISO/IEC 27001 et l'ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le

secteur nucléaire; elle est coordonnée étroitement avec la série IEC 62443. Au deuxième niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et l'IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 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 dangers chimiques et la prévention contre les dangers liés au procédé énergétique) des normes nationales ou internationales sont appliquées.

NOTE 2 Le domaine de l'IEC/SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein de l'IEC/SC 45A pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts de l'IEC/SC 45A ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée la présente Note 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION, DE CONTRÔLE-COMMANDE ET D'ALIMENTATION ÉLECTRIQUE – EXIGENCES RELATIVES À LA CYBERSÉCURITÉ

1 Domaine d'application

1.1 Généralités

Le présent document établit des exigences et fournit des recommandations pour le développement et la gestion des programmes de sécurité informatique des systèmes numériques programmables d'I&C. Le critère de conformité du programme de sécurité des systèmes numériques programmables d'I&C de la centrale nucléaire aux exigences nationales applicables est inhérent aux exigences et recommandations du présent document.

Le présent document définit les mesures adéquates 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 numériques programmables d'I&C. Ceci comprend les situations non sûres, les endommagements d'équipements ou la dégradation des performances de la centrale qui pourraient résulter d'une telle action, par exemple:

– 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 exigées de systèmes numériques programmables 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 numériques programmables d'I&C;
– des modifications malveillantes du matériel, du micrologiciel ou du logiciel au niveau de l'automate programmable (PLC).

Les erreurs humaines se traduisant par une violation de la politique de sécurité et/ou facilitant les actions malveillantes susmentionnées relèvent également du domaine d'application du présent document.

Le présent document décrit un schéma d'approche graduée pour les actifs susceptibles d'être compromis sur le plan numérique, 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 du présent document:

– les actions et les événements non malveillants tels que les défaillances accidentelles, les erreurs humaines (à l'exception de celles affectant les performances des mesures de cybersécurité) et les phénomènes naturels. En particulier, les bonnes pratiques concernant la gestion des applications et des données, y compris les sauvegardes et les restaurations pour parer aux défaillances accidentelles sont hors domaine du présent document;.

NOTE 1 Bien que dans d'autres contextes normatifs (par exemple dans la série ISO/IEC 27000, ou dans la série IEC 62443) de tels aspects soient souvent couverts par le programme de sécurité, le présent document s'intéresse seulement à la protection contre les actes malveillants réalisés à partir de moyens numériques (cyberattaques) sur les systèmes numériques programmables d'I&C. Cela s'explique essentiellement par le fait que, dans le domaine de la production nucléaire, d'autres normes et pratiques couvrent déjà les défaillances accidentelles, les erreurs humaines non intentionnelles et les risques naturels, etc. Le périmètre ciblé par l'IEC 62645 a pour objet de fournir un maximum de cohérence et un minimum de chevauchement avec ces autres normes et pratiques du secteur nucléaire.

– les systèmes liés à la sécurité physique de site, aux contrôles d'accès aux salles et locaux et à la surveillance de site. Ces systèmes, qui ne sont pas couverts de manière spécifique par le présent document, doivent être pris en compte dans les programmes et les procédures d'exploitation de la centrale;

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

– l'aspect de la confidentialité des informations relatives aux systèmes numériques programmables d'I&C ne relève pas du domaine d'application du présent document (voir 5.4.3.2.3).

L'Annexe A fournit des justifications et des commentaires concernant la définition du domaine d'application et l'application du document, en particulier les exclusions et limites indiquées précédemment.

Les normes telles que l'ISO/IEC 27001 et l'ISO/IEC 27002 ne sont pas directement applicables pour la cyberprotection des systèmes numériques programmables 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 réglementaires inhérentes aux installations nucléaires. Cependant, le présent document, construit sur les principes pertinents de haut niveau et les principaux concepts de l'ISO/IEC 27001:2013, les adapte et les complète pour qu'ils s'accordent au contexte nucléaire.

Le présent document respecte les principes généraux fournis dans le manuel de référence NSS 17 de l'AIEA.

1.2 Application

L'application du présent document est limitée à la sécurité informatique des systèmes numériques programmables d'I&C (y compris les systèmes non classés de sûreté) utilisés dans les centrales nucléaires de puissance, ainsi qu'aux outils logiciels associés. Le présent document s'applique aux parties de systèmes d'alimentation électrique couvertes par l'IEC 63046 qui dépendent de la technologie numérique programmable.

NOTE 1 À des fins de simplification, l'expression "systèmes numériques programmables d'I&C" figurant dans le texte fait référence à l'I&C et aux parties de systèmes d'alimentation électrique couvertes par l'IEC 63046 qui dépendent de la technologie numérique programmable.

Le présent document est destiné à être utilisé pour l'évaluation ou pour la modification des programmes de sécurité de centrales nucléaires de puissance déjà établis pour les systèmes numériques programmables d'I&C et pour établir de nouveaux programmes. Le présent document est appliqué pour tous les systèmes numériques programmables d'I&C de centrales nucléaires de puissance et pendant tous leurs cycles de vie, comme cela est spécifié dans le présent document. Il peut être aussi applicable à d'autres types d'installations nucléaires.

NOTE 2 L'expression "centrale nucléaire de puissance" est comprise comme "site physique", les systèmes numériques programmables d'I&C de la centrale nucléaire de puissance incluant ceux situés dans les bâtiments de la centrale nucléaire de puissance, mais aussi les systèmes des postes électriques associés à la centrale nucléaire de puissance, les installations de traitement des eaux, etc.

1.3 Cadre général

Les exigences et recommandations du présent document sont structurées selon trois articles normatifs principaux.

L'Article 5 traite de la cybersécurité au niveau du cycle de vie des programmes; son approche est complètement cohérente avec l'ISO/IEC 27001:2013. Il est fondé sur la structure et le contenu de ladite norme, qui sont, le cas échéant, adaptés et complétés pour s'adapter aux spécificités du contexte nucléaire. L'Annexe C fournit une correspondance entre les articles de la structure de l'IEC 62645 et ceux de la structure de l'ISO/IEC 27001:2013. Lorsque des

références directes au contenu de l'ISO/IEC 27001:2013 sont faites, les remplacements terminologiques suivants doivent être effectués:

– l'expression "système de management de la sécurité de l'information" utilisée dans le contenu de la norme ISO/IEC 27001:2013 référencée correspond au "programme de cybersécurité des systèmes numériques programmables d'I&C" dans le contexte du présent document (comme cela est défini dans l'Article 3);

NOTE 1 Le présent document se concentre sur la partie de programme ou le programme dédié à l'I&C. Celle-ci peut faire partie d'un programme plus large au niveau de l'entreprise, ce qui est hors du domaine du présent document.

– l'expression "sécurité de l'information" utilisée dans le contenu de la norme ISO/IEC 27001:2013 référencée correspond à la "cybersécurité" dans le contexte du présent document (comme cela est défini dans l'Article 3);

– l'expression "politique de sécurité de l'information" utilisée dans le contenu de la norme ISO/IEC 27001:2013 référencée correspond à la "politique de systèmes numériques programmables d'I&C" dans le contexte du présent document.

NOTE 2 Certains paragraphes de l'ISO/IEC 27001:2013 contiennent des références internes à d'autres paragraphes de l'ISO/IEC 27001. Le cas échéant, les références utilisées dans ces paragraphes sont prises en considération dans le cadre de l'IEC 62645; cependant, ils ne font pas référence aux paragraphes de l'IEC 62645. Voir l'Annexe C pour de plus amples informations sur les correspondances.

Les paragraphes liés à l'approche graduée et la catégorisation de sécurité sont organisés d'une façon comparable à l'IEC 61226.

L'Article 6 traite de la cybersécurité au niveau du cycle de vie des systèmes. Il est structuré selon le cycle de vie des systèmes indiqué dans l'IEC 61513, adapté pour prendre en compte les spécificités de la cybersécurité.

L'Article 7 traite de la cybersécurité au niveau des mesures de cybersécurité. Il fournit les principes de haut niveau d'une approche cohérente avec l'ISO/IEC 27002:2013, détaillés davantage dans l'IEC 63096.

La Figure 1 représente le cadre général du présent document.

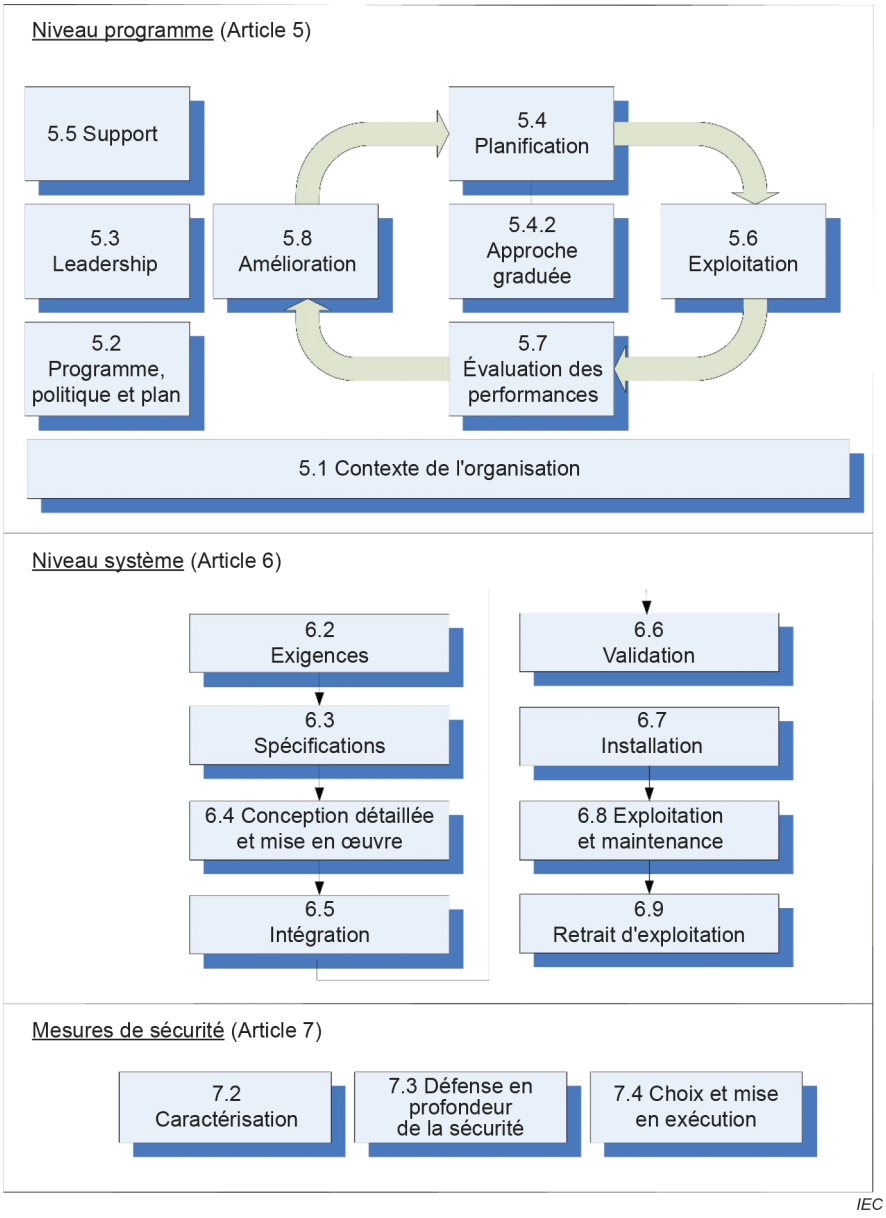

Figure 1 – Cadre général de l'IEC 62645

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. Le présent document établit des exigences plus détaillées portant sur le plan de la de sécurité d'ensemble, 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.

Le présent document traite aussi des exigences de sécurité portant sur les systèmes numériques programmables d'I&C qui sont hors des domaines d'application 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 cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. 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 de puissance – Systèmes d'instrumentation et de 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*

IEC 62859, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences pour coordonner sûreté et cybersécurité*

IEC 62988:2018, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils sans fil*

ISO/IEC 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*

ISO/IEC 27002:2013, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information*

ISO/IEC 27005:2018, *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*

AIEA TLD-006, *Conducting Computer Security Assessment at Nuclear Facilities*, 2016 (disponible en anglais seulement)