



INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-3719-9

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

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	8
2 Normative references	8
3 Terms and definitions	9
4 Symbols and abbreviations.....	11
5 Coordinating safety and cybersecurity at the overall architecture level	12
5.1 General.....	12
5.2 Fundamental and generic principles.....	12
5.3 Thematic requirements and recommendations	13
5.3.1 Delineation of security zones	13
5.3.2 Provisions for coping with common cause failures (including diversity)	13
5.3.3 Separation provisions	14
5.3.4 Data communications	14
6 Coordinating safety and cybersecurity at the individual system level.....	14
6.1 General.....	14
6.2 Fundamental and generic principles.....	14
6.3 Safety and cybersecurity coordination during the I&C system lifecycle	15
6.3.1 General	15
6.3.2 Requirements and planning activities.....	15
6.3.3 Design activities	15
6.3.4 Implementation activities	16
6.3.5 Verification and validation activities	16
6.3.6 Installation and acceptance testing activities	16
6.3.7 Operations and maintenance activities.....	16
6.3.8 Change management.....	16
6.3.9 Decommissioning activities.....	16
6.4 Selected technical aspects of I&C systems constrained by safety and cybersecurity	17
6.4.1 General	17
6.4.2 Logical access control for HMIs of I&C programmable digital systems in control rooms.....	17
6.4.3 Software modification	17
6.4.4 Logging and audit capability	18
6.4.5 Use of cryptography by I&C systems	18
6.4.6 System availability and function continuity.....	19
7 Organizational and operational issues	19
7.1 Governance and responsibilities	19
7.2 Coordination between safety and cybersecurity staff during operations.....	19
7.3 Safety and cybersecurity culture	19
7.4 Emergency response management	19
Annex A (informative) Rationale for, and notes related to, the scope of this document.....	21
A.1 General.....	21
A.2 Inclusion of I&C programmable digital system not important to safety	21
A.3 Exclusion of physical security, room access control and site security surveillance systems.....	21

A.4	Exclusion of non-malevolent actions and events	21
A.5	Exclusion of development tools and platforms.....	22
	Bibliography.....	23

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – REQUIREMENTS FOR COORDINATING SAFETY AND CYBERSECURITY

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 62859 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/1104/FDIS	45A/1118/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 website under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

INTRODUCTION

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

I&C systems have evolved during the last decades from non-digital equipment and stand-alone environments to digital technologies and interconnected systems. Such an evolution exposes them to risks related to cyberattacks. In addition to well-established safety-oriented provisions, more recent cybersecurity requirements and controls now apply to the same systems. A normative framework is needed to master the interactions and potential side-effects when safety and cybersecurity provisions converge on the same I&C systems and architectures, taking into account the nuclear I&C specifics and the SC 45A related standards.

This standard specifically focuses on the issue of requirements for coordinating safety and cybersecurity provisions for I&C programmable digital systems and architectures. It defines both generic principles and guidance for practical situations to integrate cybersecurity requirements in nuclear I&C architectures and systems, fundamentally tailored for safety. Technical but also conceptual, organizational and procedural aspects are covered.

It is intended that this standard be used by designers and operators of nuclear power plants (NPPs) (utilities), 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 62859 is at the second level of the IEC SC 45A standard series. It is to be considered as bridging IEC 62645 (also at the second level of the IEC SC 45A standard series) and IEC 61513, the top level document of the IEC SC 45A standard series. Regarding the specific theme of cybersecurity, IEC 62645 is the top-level in the SC 45A standard series. Both IEC 62645 and IEC 62859 are considered formally as second level documents with respect to IEC 61513, although IEC 61513:2011 does not actually ensure proper reference to and consistency with them (this will be done in a future revision of IEC 61513).

For a generic description of 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

It is important to note that this standard establishes additional requirements for I&C programmable digital systems and architectures, with regard to the coordination between safety and cybersecurity, and clarifies the processes by which I&C programmable digital systems are designed, implemented and operated in nuclear power plants. Aspects for which special requirements and recommendations have been produced are:

- IAEA guidance on I&C;
- IAEA guidance on computer security at nuclear facilities;
- regulatory interpretations for country specific requirements.

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 63046¹. 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

¹ In preparation. Stage at the time of publication: IEC ANW 63046:2016.

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 implements and details 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 (NPP), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPP, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPP, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPP 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-3 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, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A 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 in 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 will be published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – REQUIREMENTS FOR COORDINATING SAFETY AND CYBERSECURITY

1 Scope

This document provides a framework to manage the interactions between safety and cybersecurity for nuclear power plant (NPP) systems, taking into account the current SC 45A standards addressing these issues and the specifics of nuclear I&C programmable digital systems.

NOTE In this document (as in IEC 62645), cybersecurity relates to prevention of, detection of, and reaction to malicious acts perpetrated by digital means (cyberattacks). In this context, it does not cover considerations related to non-malevolent actions and events such as accidental failures, natural events or human errors (except those degrading cybersecurity). Those aspects are of course of prime importance but they are covered by other SC 45A documents and standards, and are not considered as cybersecurity related in this document.

This document establishes requirements and guidance to:

- integrate cybersecurity provisions in nuclear I&C architectures and systems, which are fundamentally tailored for safety;
- avoid potential conflicts between safety and cybersecurity provisions;
- aid the identification and the leveraging of the potential synergies between safety and cybersecurity.

This document is intended to be used for designing new NPPs, or modernizing existing NPPs, throughout I&C programmable digital systems lifecycle. It is also applicable for assessing the coordination between safety and cybersecurity of existing plants. It may also be applicable to other types of nuclear facilities.

This document addresses I&C programmable digital systems important to safety and I&C programmable digital systems not important to safety. It does not address programmable digital systems dedicated to site physical security, room access control and site security surveillance.

This document is limited to I&C programmable digital systems of NPPs, including their on-site maintenance and configuration tools.

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

This document comprises three normative clauses:

- Clause 5 deals with the overall I&C architecture;
- Clause 6 focuses on the system level;
- Clause 7 deals with organizational and operational issues.

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 60709:2004, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

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

IEC 61500:2009, *Nuclear power plants – Instrumentation and control systems important to safety – Data communication in systems performing category A functions*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IEC 62645:2014, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

SOMMAIRE

AVANT-PROPOS	28
INTRODUCTION	30
1 Domaine d'application	33
2 Références normatives	34
3 Termes et définitions	34
4 Symboles et abréviations	37
5 Coordination de la sûreté et de la cybersécurité au niveau de l'architecture d'ensemble	37
5.1 Généralités	37
5.2 Principes fondamentaux et génériques	37
5.3 Recommandations et exigences thématiques	38
5.3.1 Délimitation des zones de sécurité	38
5.3.2 Dispositions relatives à la gestion des défaillances de cause commune (comprenant la diversité)	39
5.3.3 Dispositions relatives à la séparation	39
5.3.4 Communications de données	40
6 Coordination de la sûreté et de la cybersécurité au niveau des systèmes individuels	40
6.1 Généralités	40
6.2 Principes fondamentaux et génériques	40
6.3 Coordination de la sûreté et de la cybersécurité au cours du cycle de vie des systèmes numériques programmables d'I&C	41
6.3.1 Généralités	41
6.3.2 Exigences et activités de planification	41
6.3.3 Activités de conception	41
6.3.4 Activités de mise en œuvre	42
6.3.5 Activités de vérification et de validation	42
6.3.6 Activités d'installation et d'essais de réception	42
6.3.7 Activités d'exploitation et de maintenance	42
6.3.8 Gestion des modifications	42
6.3.9 Activités de mise hors service	43
6.4 Aspects techniques particuliers aux systèmes d'I&C soumis à des contraintes de sûreté et de cybersécurité	43
6.4.1 Généralités	43
6.4.2 Contrôle d'accès logique pour les IHM des systèmes numériques programmables d'I&C dans les salles de commande	43
6.4.3 Modifications logicielles	43
6.4.4 Fonctionnalités de journalisation et d'audit	44
6.4.5 Utilisation de la cryptographie par des systèmes d'I&C	45
6.4.6 Disponibilité du système et continuité des fonctions	45
7 Questions d'organisation et d'exploitation	45
7.1 Gouvernance et responsabilités	45
7.2 Coordination entre le personnel de sûreté et de cybersécurité en cours d'exploitation	46
7.3 Culture de sûreté et de cybersécurité	46
7.4 Gestion des mesures d'urgence	46

Annexe A (informative) Justifications et notes relatives au domaine d'application du présent document	47
A.1 Généralités	47
A.2 Inclusion des systèmes numériques programmables d'I&C non importants pour la sûreté.....	47
A.3 Exclusion des systèmes de sécurité physique, de contrôle d'accès aux salles de commande et de surveillance sécuritaire du site	47
A.4 Exclusion des actions et événements non malveillants.....	47
A.5 Exclusion des outils et plateformes de développement.....	48
Bibliographie.....	49

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE – EXIGENCES POUR COORDONNER SÛRETÉ ET CYBERSÉCURITÉ

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 62859 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/1104/FDIS	45A/1118/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.

INTRODUCTION

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

Les systèmes d'instrumentation et de contrôle-commande (I&C) ont connu au cours des dernières décennies une évolution majeure, les équipements non numériques et les environnements autonomes laissant la place aux technologies numériques et aux systèmes interconnectés. Cette évolution les expose à des risques de cyberattaques. Ces mêmes systèmes font l'objet de dispositions de sûreté bien établies, mais également d'exigences et de mesures plus récentes en matière de cybersécurité. Un cadre normatif est nécessaire pour maîtriser les interactions et les effets secondaires potentiels lorsque des dispositions en matière de sûreté et de cybersécurité convergent vers les mêmes architectures et systèmes d'I&C, en tenant compte des exigences spécifiques aux systèmes d'I&C nucléaires ainsi que des normes connexes du SC 45A.

La présente norme traite spécifiquement de la question des exigences relatives à la coordination des dispositions en matière de sûreté et de cybersécurité pour les architectures et systèmes numériques programmables d'I&C. Elle définit des principes génériques, ainsi que des lignes directrices pour des cas pratiques d'intégration d'exigences de cybersécurité à des architectures et systèmes d'I&C nucléaires, fondamentalement conçus pour la sûreté. Elle couvre les aspects techniques, conceptuels, ainsi que les questions d'organisation et de procédure.

La présente norme est destinée à être utilisée par les concepteurs et les opérateurs de centrales nucléaires de puissance (NPP, *Nuclear Power Plant*), les évaluateurs de systèmes, les fournisseurs et sous-traitants, ainsi que les régulateurs.

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

L'IEC 62859 est un document de deuxième niveau de la série de normes du SC 45A de l'IEC. Elle doit être considérée comme le point de liaison entre l'IEC 62645 (qui est également un document de deuxième niveau dans la série de normes du SC 45A de l'IEC) et l'IEC 61513, document de niveau supérieur de la série de normes du SC 45A de l'IEC. En ce qui concerne la cybersécurité, l'IEC 62645 est le document de niveau supérieur dans la série de normes du SC 45A de l'IEC. L'IEC 62645 et l'IEC 62859 sont officiellement considérées comme des documents de deuxième niveau par rapport à l'IEC 61513, même si l'IEC 61513:2011 n'est pas forcément alignée et cohérente avec ces normes (cela fera l'objet d'une révision ultérieure de l'IEC 61513).

Pour une description générique de la structure de la série de normes du SC 45A de l'IEC, se reporter au point d) de cette introduction.

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

Il est important de noter que la présente norme établit des exigences supplémentaires pour les architectures et systèmes numériques programmables d'I&C en ce qui concerne la coordination entre la sûreté et la cybersécurité, et qu'elle clarifie les processus de conception, de mise en œuvre et d'exploitation des systèmes numériques programmables d'I&C dans les NPP. Des exigences et recommandations spéciales ont été produites pour les aspects suivants:

- les lignes directrices établies par l'Agence internationale de l'énergie atomique (AIEA) concernant l'I&C;
- les lignes directrices établies par l'AIEA concernant la sécurité informatique dans les installations nucléaires;
- les interprétations légales en ce qui concerne les exigences nationales spécifiques.

d) Description de la structure de la série de normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC et des documents 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 63046¹. 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. L'IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; 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, cohérent et consistant 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 des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes programmés numériques, 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 généralement pas référencées directement par l'IEC 61513 ou l'IEC 63046, 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.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau 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, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 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.

L'IEC 61513 et l'IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, l'IEC 61513 et l'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 domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. L'IEC 61513 et l'IEC 63046 font 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. Au second niveau, l'IEC 62645 est le document chapeau des normes du SC 45A de l'IEC portant sur la cybersécurité. Elle est élaborée sur principes pertinents de haut niveau des normes ISO/IEC

¹ En préparation. Étape au moment de la publication: IEC ANW 63046:2016.

27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec l'IEC 62443. Au second niveau, l'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 risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales.

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 l'IEC 63046 sera publiée la présente NOTE 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE – EXIGENCES POUR COORDONNER SÛRETÉ ET CYBERSÉCURITÉ

1 Domaine d'application

Le présent document fournit un cadre de travail permettant de gérer les interactions entre sûreté et cybersécurité pour les systèmes dans les NPP, en prenant en compte les normes du SC 45A traitant de ces questions et des particularités des systèmes programmables numériques utilisés pour l'I&C dans le nucléaire.

NOTE Dans le présent document (comme dans l'IEC 62645), la cybersécurité se réfère à la prévention, la détection et la réaction à des actes malveillants, réalisés en utilisant des moyens informatiques (cyberattaques). Dans ce contexte, elle ne couvre pas les considérations relatives aux actions et événements non malveillants, tels que les défaillances accidentelles, les événements naturels ou les erreurs humaines (à l'exception des erreurs humaines compromettant la cybersécurité). Ces aspects sont bien entendu de grande importance, mais ils sont couverts par d'autres documents et normes du SC 45A, et ne sont pas considérés comme relevant de la cybersécurité dans ce cadre de travail.

Le présent document établit des exigences et des lignes directrices pour:

- intégrer des dispositions en matière de cybersécurité à des architectures et systèmes d'I&C nucléaires, fondamentalement conçus pour la sûreté;
- éviter d'éventuelles divergences entre les dispositions en matière de sûreté et de cybersécurité;
- favoriser l'identification et l'exploitation des synergies potentielles entre la sûreté et la cybersécurité.

Le présent document est destiné à être utilisé dans le cadre de la conception de nouvelles NPP, ou de la modernisation de NPP existantes, tout au long du cycle de vie des systèmes numériques programmables d'I&C. Il s'applique également à l'évaluation de la coordination entre la sûreté et la cybersécurité des centrales existantes. Il peut également s'appliquer à d'autres types d'installations nucléaires.

Le présent document s'intéresse aux systèmes numériques programmables d'I&C importants pour la sûreté, ainsi qu'aux systèmes numériques programmables d'I&C non importants pour la sûreté. Il ne couvre pas les systèmes numériques programmables dédiés à la sécurité physique du site, au contrôle d'accès aux salles de commande ni à la surveillance de sécurité du site.

Le présent document est limité aux systèmes numériques programmables d'I&C des NPP, y compris leurs outils configuration et de maintenance sur site.

L'Annexe A donne les justifications et des remarques à propos de la définition du domaine d'application du présent document, notamment concernant les exclusions et limitations mentionnées précédemment.

Le présent document comporte trois articles normatifs:

- l'Article 5 traite de l'architecture d'I&C d'ensemble;
- l'Article 6 traite des systèmes;
- l'Article 7 s'intéresse aux questions d'organisation et de procédure.

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 60709:2004, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Séparation*

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 61500:2009, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Communication de données dans les systèmes réalisant des fonctions de catégorie A*

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 62138:2004, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

IEC 62340, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences permettant de faire face aux défaillances de cause commune (DCC)*

IEC 62566:2012, *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 62645:2014, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés*