IEC 62859

Edition 1.1 2019-10
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

IEC 62859:2016-10+AMD1:2019-10 CSV(en-fr)

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

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC 62859

Edition 1.1 2019-10
CONSOLIDATED VERSION

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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 978-2-8322-7484-2

IEC 62859

Edition 1.1 2019-10
CONSOLIDATED VERSION

REDLINE VERSION

VERSION REDLINE

colour inside

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

IEC 62859:2016-10+AMD1:2019-10 CSV(en-fr)

CONTENTS

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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62859 edition 1.1 contains the first edition (2016-10) [documents 45A/1104/FDIS and 45A/1118/RVD] and its amendment 1 (2019-10) [documents 45A/1279/FDIS and 45A/1286/RVD].

In this Redline version, a vertical line in the margin shows where the technical content is modified by amendment 1. Additions are in green text, deletions are in strikethrough red text. A separate Final version with all changes accepted is available in this publication.

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.

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

The committee has decided that the contents of the base publication and its amendment 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.

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 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 63046[1]. 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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62645, in IEC 61513 and the following apply.

NOTE If for a given term, different definitions are provided in these three sources, the definition of the present document applies.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
computer-based item
item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: A computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to software-based item.

3.2
cyberattack
attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Note 1 to entry: Cyberattacks include targeted and non-targeted (e.g. malwares) attacks by digital means. Cyberattack is synonymous with digital attack.

3.3
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

– malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

Note 1 to entry: This definition is tailored with respect to this standard scope and overall SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the SC 45A standard series. See Annex A.4 for more detail about such exclusions.

Note 2 to entry: Computer security, security and cybersecurity are considered synonymous in this document.

3.4
cybersecurity event
identified occurrence of a system, service or network state indicating a possible breach of cybersecurity policy or failure of controls, or a previously unknown situation that may be cybersecurity relevant

3.5
cybersecurity-driven software modification
software modification of which the main reason is to implement one or more cybersecurity features, or remediate one or several security vulnerabilities in a I&C programmable digital component, or to prevent successful exploitation of these vulnerabilities or to mitigate attackers’ capabilities to exploit these vulnerabilities

3.6
cybersecurity feature
provision, control or function specifically designed for cybersecurity purposes

Note 1 to entry: Non-cybersecurity features implementation can have negative, neutral, but also positive impact on cybersecurity. This is particularly the case of some safety features, as discussed in this document.

Note 2 to entry: The terms “feature” and “provision” are considered synonymous in this document.

3.7
HDL-Programmed Device
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools

Note 1 to entry: HDLs and related tools (e.g. simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2 to entry: The development of HPDs can use pre-developed blocks.

Note 3 to entry: HPDs are typically based on blank FPGAs (Field Programmable gate Arrays) or similar programmable integrated circuits.

[SOURCE: IEC 62566:2012, 3.7]

3.8
logical separation
separation from a digital data network perspective involving the absence of direct data communications (i.e. without any proxy or cybersecurity filtering device)

3.9
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: The main programmable digital items are computer-based items and programmable logic items.

Note 3 to entry: This term used by SC 45A is equivalent to Programmable Electronic item used in IEC 61508.

3.10
programmable logic item
item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: A programmable logic item is a kind of programmable digital item.

3.11
safety feature
provision, control or function specifically designed for safety purposes

Note 1 to entry: Non-safety features implementation can have negative, neutral, but also positive impact on safety. This is particularly the case of some cybersecurity features, as discussed in this standard.

Note 2 to entry: The terms “feature” and “provision” are considered synonymous.

3.12
software modification
change in an already agreed document (or documents) leading to an alteration of the executable code

Note 1 to entry: Software modifications may occur either during initial software development (e.g. to remove faults found in later stages of development), or after the software is already in service.

[SOURCE: IEC 60880:2006, 3.36]

3.13
software security update
piece of software provided by a digital system supplier and designed to fix one or several security vulnerabilities in a digital component, or implement one or more cybersecurity features

Note 1 to entry: Security patches are considered as software security updates.

4 Symbols and abbreviations

BIOS	Basic Input/Output System
CB	Computer-Based
CCF	Common Cause Failure
CRC	Cyclic Redundancy Check
FPGA	Field-Programmable Gate Array
HDL	Hardware Description Language
HMI	Human-Machine Interface

HPD HDL-Programmed Device

I&C Instrumentation and Control

NPP Nuclear Power Plant

5 Coordinating safety and cybersecurity at the overall architecture level

5.1 General

Several safety features and architectural characteristics implemented in order to address design basis requirements are in some cases directly beneficial to cybersecurity: this includes some of the features that support equipment independence, system reliability or system diversity. However, considering that the design of these features may not have adequately taken into account potential vulnerabilities to cyberattacks, dedicated cybersecurity measures may be needed to achieve adequate cybersecurity, without degrading safety.

This clause provides requirements and recommendations to enable a smooth integration of cybersecurity requirements as per IEC 62645 in a nuclear I&C architecture, fundamentally and firstly structured by safety-oriented requirements (in particular those of IEC 61513 and several second level documents of the SC 45A series, including IEC 62340 or IEC 60709).

5.2 Fundamental and generic principles

The following principles apply for the treatment of cybersecurity at the I&C architectural level:

a) Cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realisation. It shall not compromise the effectiveness of the diversity and defence-in-depth features implemented by the I&C architecture.

b) Cybersecurity requirements impacting the overall I&C architecture shall be addressed after the overall I&C architecture design and assignment of the I&C functions have been first made as per 5.4 of IEC 61513:2011. The integration of architectural cybersecurity requirements may lead to an iterative design process.

NOTE The objective is to secure a safe I&C architecture. Such a sequence is already implicit in IEC 62645, as the assignment of security degrees (and their associated requirements) assumes that safety categories are already assigned to safety functions, and that the safety functions are already assigned to I&C systems.

c) Cybersecurity features shall not adversely impact the required performance (including response time), required effectiveness, required reliability or required operation of functions important to safety.

d) The failure modes and consequences of cybersecurity features on the functions important to safety shall be analysed and taken into account.

e) When two architecture designs offer equivalent level of safety, priority should be given to the most secure one. Unnecessary complexity shall be avoided as it is detrimental to both safety and cybersecurity.

f) Any architectural property or characteristics designed for safety reason (e.g., independence between systems), which has value as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined taking into account context-relevant cyberattacks, by staff responsible for cybersecurity, to confirm its cybersecurity effectiveness.

A particular case corresponds to communications between systems important to safety and systems not important to safety, or between systems of different safety classes. IEC 61513 already requires that communication links are designed in such a way that data communication and operation of the higher safety category function cannot be jeopardised by data communication with lower classified systems. However, the provisions taken to fulfil such safety requirements are not necessarily robust against malicious threats and cyberattacks.

5.3 Thematic requirements and recommendations

5.3.1 Delineation of security zones

5.3.1.1 General

As defined in IEC 62645, security zones are practical and architectural implementations of a graded approach to cybersecurity; they allow I&C systems with similar importance concerning safety and plant performance (i.e. having the same security degree) to be grouped together for administration and application of protective measures. As per IEC 62645, criteria for defining a security zone include organizational issues (such as ownership/responsibility), localisation, architectural or technical aspects. In practice, security zones are implemented as means against the propagation of cyberattacks. In such context, when a zone model is enforced as recommended by IEC 62645, the following applies:

a) The delineation of security zones, as per IEC 62645, shall take into account and leverage independence and physical separation requirements introduced for the purpose of enhancing safety.

b) Data communication aspects (incl. logical separation) and geographical/physical separation as well as independence aspects shall be considered together to delineate security zones.

NOTE Geographical separation and independence features are not sufficient to delineate security zones.

5.3.1.2 Dealing with systems with several divisions

a) The divisions (or trains) of a given I&C programmable digital system should be grouped in the same security zone, unless the communications between divisions can be efficiently filtered and monitored from a cybersecurity perspective.

b) The divisions (or trains) of a given I&C programmable digital system shall be grouped in the same security zone if a common engineering tool is used to configure them.

NOTE This requirement holds even if the tool is connected only to one division at a time: if the tool is compromised, it can support an asynchronous attack, compromising divisions one after the other.

5.3.1.3 Dealing with systems sharing common resources

a) I&C programmable digital systems sharing common computer-based tools (e.g. configuration, testing, and/or maintenance tools) shall be grouped in the same security zone, unless it is demonstrated from a cybersecurity perspective that the tools cannot directly impact the systems they are connected to.

b) I&C programmable digital systems sharing a common network or communication bus without cybersecurity technical provisions securing the communications should be grouped in the same security zone, even if they perform functions of different safety categories. As per IEC 62645, the security degree assignment shall take into account the most sensitive safety category.

5.3.2 Provisions for coping with common cause failures (including diversity)

a) In some cases, provisions taken in order to cope with common cause failures (CCF), including diversity, can be leveraged from a cybersecurity perspective, and should be leveraged in such cases. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and potential cyberattacks (consistently with 5.2 f).

NOTE 1 Provisions resulting from requirements, recommendations and associated safety practices as per 5.4.2.6 of IEC 61513:2011 (for all I&C systems important to safety), Clause 13 of IEC 60880:2006 (for software aspects of systems performing category A functions), IEC 62340 or equivalent (for systems performing category A functions), are for instance directly concerned by 5.3.2a).

NOTE 2 As for safety, diversity is also commonly used in cybersecurity: examples include the use of diverse penetration testing tools, diverse skills of cybersecurity team members or auditors. However, expecting benefit from diversity in all situations for both safety and cybersecurity is questionable. Diversity is generally used “in series” to bring cybersecurity benefit (involving the need to compromise one system after another to reach a target), whereas it is generally used “in parallel” to bring benefit in safety. Such use “in parallel” is in some

cases antagonistic with cybersecurity, increasing the attack surface. Moreover, even from a pure cybersecurity perspective there are pros and cons to diversity. Used “in series” (for instance two firewalls from different providers), diversity makes the attacker task more complex (avoiding common vulnerabilities, cybersecurity functions completing each others), but at the same time, it introduces complexity leading to higher risk of configuration errors, difficulty of maintenance, etc.

b) Any cybersecurity measures considered for inclusion in the design shall be assessed for their potential to introduce fault leading to CCF between systems diversified for safety reasons. Where such risks are found, alternative means of achieving adequate cybersecurity shall be implemented as necessary.

5.3.3 Separation provisions

a) In some cases, provisions taken for separation purposes can be leveraged from a cybersecurity perspective, and should be leveraged in such cases.

b) Requirements, recommendations and associated safety practices as per 5.4 of IEC 60709:2004 on independence from control systems (for systems supporting category A functions), or equivalent, are potentially beneficial both in terms of safety and cybersecurity. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and potential cyberattacks (consistently with 5.2 f).

5.3.4 Data communications

a) Requirements, recommendations and associated safety practices as per IEC 61500:2009 on data communications (for systems supporting category A functions), or equivalent, are potentially beneficial both in terms of safety and cybersecurity. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and cyberattacks (consistently with 5.2 f).

b) A detailed knowledge of data communications in use by and between I&C programmable digital systems (incl. protocols, roles, initiatives, sources and destinations) is beneficial both for safety and cybersecurity and shall be maintained and documented, from design to implementation and operations.

6 Coordinating safety and cybersecurity at the individual system level

6.1 General

In addition to the architectural level treated in Clause 5, coordination of safety and cybersecurity shall also be considered at the individual system level. This clause provides requirements and recommendations for such coordination.

6.2 Fundamental and generic principles

The following principles apply for the treatment of cybersecurity features on I&C programmable digital systems:

a) Implementation of cybersecurity features directly in systems important to safety shall be justified.

NOTE 1 Adding cybersecurity features to system important to safety increases system complexity and has the potential to introduce new failure modes to the system. Such consequences can challenge the system ability to perform its function(s) important to safety in a reliable manner. Moreover, the rapid evolution pace of cybersecurity threats, vulnerabilities and techniques is hard to conciliate with the modification processes of systems important to safety. However, a limited number of cybersecurity controls are still in some cases implemented in systems important to safety: examples include logging capability and authentication mechanisms, as per 5.5.3 of IEC 61513:2011 and as per IEC 62645.

NOTE 2 Implementation of cybersecurity features outside systems important to safety ease separate qualification of cybersecurity related features when required by national regulations.

b) Cybersecurity features shall not adversely impact the realisation of functions important to safety, the required performance (including response time), required reliability, or required operation of programmable digital systems important to safety.

NOTE 3 Key elements of I&C programmable digital system performance are for example task ordering, functional parameters, maximum response time of functions and maximum usage of resources. Cybersecurity features implementation is likely to influence, even marginally, one or several of these elements: the important criterion is that it does not prevent the system from meeting the required performance to ensure its functions.

c) The failure modes and consequences of these cybersecurity features on the system's functions important to safety shall be analysed and taken into account.

d) Cybersecurity features implemented in systems important to safety shall be developed and qualified to the same level as the system these features reside in.

e) If cybersecurity features are implemented in displays and controls of systems important to safety, they shall not adversely impact the operator's ability to maintain plant safety.

f) When a cybersecurity requirement cannot be met by the implementation of a cybersecurity feature in a system important to safety, alternative cybersecurity measures shall be implemented. These alternative measures shall at least ensure that the system's security degree requirements (as per IEC 62645) are met.

NOTE 4 Such alternative measures can be for instance organisational, architectural, or in particular dealing with the communications and interfaces with the system.

g) Safety-oriented procedures (e.g. surveillance tests) or functions have been implemented to fulfil safety objectives. When reusing a safety procedure or function to achieve cybersecurity objectives, both the safety objectives and the cybersecurity objectives of the reused procedure or function shall be described, and their achievement shall be justified and documented.

h) The extension or modification of a safety-oriented procedure (e.g., surveillance tests) or function for cybersecurity purpose can only be made if it has been previously justified and documented that its safety objectives are still achieved.

6.3 Safety and cybersecurity coordination during the I&C system lifecycle

6.3.1 General

The requirements and recommendations provided in 6.2 do not specifically consider the lifecycle phases of I&C programmable digital systems. The objective of 6.3 is to provide additional requirements and considerations with respect to I&C programmable digital system lifecycle activities. For consistency reasons, the activities considered are those used in Clause 6 of IEC 62645:2014.

NOTE The order of Subclauses 6.3.2 to 6.3.9, adopted from IEC 62645:2014, does not necessarily present the timely order of activities which are sometimes in reality partially executed in parallel, or include iterations.

6.3.2 Requirements and planning activities

a) Cybersecurity requirements should be defined as early as possible in the I&C programmable digital system lifecycle.

b) Potential dependencies, conflicts or reinforcements between safety requirements and cybersecurity requirements should be detected, documented and taken into account to ensure the definition of an integrated solution meeting both the safety and security goals.

6.3.3 Design activities

a) I&C systems should be designed in order to favour reinforcements between safety and cybersecurity features. Related design choices regarding such reinforcements should take into account a trade-off analysis between:

- the gains and drawbacks related to the verification and validation of the systems;
- the gains and drawbacks in terms of system complexity and interfaces.

b) Any system feature initially designed for safety reason which has a potential value as a cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined taking into account context-relevant cyberattacks, by staff responsible for cybersecurity, to confirm its cybersecurity effectiveness.

c) The security features of programmable digital systems important to safety should be designed to limit their dependency on updates.

6.3.4 Implementation activities

This document does not provide any specific requirements or recommendations related to the coordination between safety and cybersecurity for this phase. Refer to IEC 62645 for cybersecurity-related ones, to IEC 60880 and IEC 62138 for software of CB I&C systems supporting functions important to safety, and to IEC 62566 for HDL-programmed integrated circuits for systems performing category A functions.

6.3.5 Verification and validation activities

a) Software code review or analysis of I&C programmable digital systems conducted for safety reasons (see IEC 60880 and IEC 62138 for software of systems performing functions important to safety) may also consider cybersecurity aspects and vulnerabilities associated with unsecure coding practices.

NOTE 1 Skills and tools needed for safety-oriented code review or analysis, and those needed for security-oriented code review or analysis are often overlapping, however, they are different. The optimal level of integration of these activities is highly dependent on the context.

b) Appropriate cybersecurity measures should be taken to protect sensitive data or information associated to software code review and analysis.

c) Software and hardware should be verified and validated in order to avoid unapproved functionalities. This may be required from a safety perspective (as per the applicable standards), but also from a cybersecurity perspective in some cases.

NOTE 2 During inspections made for hardware verification and validation, wireless capabilities or undeclared programmable digital components can be detected.

6.3.6 Installation and acceptance testing activities

a) Security tests should be conducted in a test environment representative of the installed system.

6.3.7 Operations and maintenance activities

a) Off-line maintenance periods should be considered as opportunities for software security updates, if compatible with respect to qualification constraints.

b) Periodic testing of functions important to safety shall not degrade cybersecurity of the involved I&C systems.

c) Cybersecurity verifications may be considered for integration in safety periodic testing.

NOTE Such integrations are subject to restrictions: see 6.2 g) and 6.2 h).

d) Intrusive security testing, including penetration testing, shall not be conducted directly on systems important to safety during operations. A test lab should be available.

6.3.8 Change management

a) There shall be procedures to assess and manage the potential for adverse safety and cybersecurity interactions that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures.

b) There should be procedures to identify and leverage potential mutual reinforcements between safety and cybersecurity that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures.

c) A change driven by safety considerations should be reviewed by staff responsible for cybersecurity.

d) A change driven by cybersecurity considerations should be reviewed by staff responsible for safety.

6.3.9 Decommissioning activities

a) As-built information, including system actual interfaces, should be available and analysed before starting decommissioning individual I&C systems to ensure that the overall cybersecurity and safety objectives of the plant are not compromised by the decommissioning of the system, or by the related steps of the process.

b) In particular, when decommissioning of individual I&C systems leads to temporary provisions in order to maintain the safe operations of the plant, those provisions may induce new cybersecurity issues which should be analysed and addressed if deemed relevant by this analysis.

6.4 Selected technical aspects of I&C systems constrained by safety and cybersecurity

6.4.1 General

The objective of 6.4.2 to 6.4.6 is to provide guidance or requirements on some aspects of I&C programmable digital system design and operation, when they are subject to both safety and cybersecurity constraints. They deal with common situations where safety and cybersecurity technical measures or requirements conflict, depend or reinforce each others. Potential confusion between safety and cybersecurity measures is also addressed.

6.4.2 Logical access control for HMIs of I&C programmable digital systems in control rooms

a) Password-based logical access control for the operators shall not be implemented on HMIs of I&C programmable digital systems which need immediate operator access for plant safety. Alternative access control measures, acceptable from a safety point of view, should be implemented.

NOTE Possible alternative access control measures include permission to physically access the control rooms based on a rigorous screening of personnel, access limitation to operational HMI software (e.g., to BIOS or to the operating system level), software with restricted input (e.g. only from predefined lists). Such alternative access control measures are of particular importance for control rooms which are not permanently staffed (e.g. remote shutdown station).

b) Account/node locking or delayed login after invalid access attempts should not be implemented for I&C programmable digital systems which need immediate operator access for plant safety. Alternative measures, acceptable from a safety point of view, should be implemented.

c) The management of access controls shall take account of specific operational needs with safety implications (e.g., maintenance during night shifts, beyond design basis conditions, nuclear emergencies).

Note that requirements of 6.4.2 are valid for I&C programmable digital systems, not for their maintenance digital tools.

6.4.3 Software modification

6.4.3.1 Cybersecurity-driven software modifications

a) Cybersecurity-driven software modifications (including the application of a software security update) are a type of software modifications and shall be treated accordingly, i.e. in accordance with Clause 11 of IEC 60880:2006 for software of I&C CB systems supporting category A functions, in accordance with 5.10 and 6.10 of IEC 62138:2004 for software of I&C CB systems supporting category B or C functions, and in accordance with relevant local procedures for I&C programmable digital systems not important to safety.

b) The decision to implement a cybersecurity-driven software modification shall be validated by personnel knowledgeable of the targeted systems, their usage and their safety implications, in conjunction with those who are accountable for those systems.

c) Tests shall be conducted to validate that a cybersecurity-driven software modification (including the application of a software security update) does not degrade system ability to ensure its functions important to safety.

d) When it is decided not to apply a software security update, whatever the reason (e.g., tests as per c) or because the change is not possible during operations):

- the vulnerability associated with this non-application shall be traced and managed with the appropriate level of confidentiality;
- a dedicated risk analysis shall characterise the risks associated with this decision;

– if the risk analysis identifies the need for compensating cybersecurity measures, their implementation shall be approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems.

6.4.3.2 Other software modifications

a) Analyses or tests shall be conducted to validate that a software modification, made for safety or other reasons not related to cybersecurity (e.g. reliability, new functionality), does not result in inadequate cybersecurity.

b) Any software modification identified as degrading cybersecurity shall not be implemented on plant I&C systems ~~except if the three~~ unless the four following conditions are met:

– a dedicated risk analysis has been conducted ~~and the residual risks formally accepted~~ to identify the risk;

– ~~the~~ compensating cybersecurity measures potentially identified by the risk analysis ~~(if any)~~ have been approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems;

– ~~these~~ any approved compensating cybersecurity measures ~~(if any)~~ have been implemented;

– the remaining residual risk is approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems.

6.4.4 Logging and audit capability

a) Local record generation, audit reduction and report generation capability intended for cybersecurity should be implemented as much as possible external to systems important to safety.

b) The failure messages generated by a programmable digital I&C equipment should be logged outside this equipment to support safety or cybersecurity analyses.

c) Any logical connectivity implemented to centrally manage systems and/or cybersecurity logs should not interfere with independence requirements imposed upon systems important to safety.

NOTE Among the different possible approaches, strictly unidirectional channels to push logs are beneficial both from a security and safety point of view.

d) Logging mechanisms should be preferably implemented and pre-configured so that no logging management (e.g., level of detail, selectivity of logged events) is needed during plant operation.

6.4.5 Use of cryptography by I&C systems

a) Cryptographic mechanisms may be used by I&C programmable digital systems, but they shall not adversely impact the required performance (including response time), effectiveness, reliability or operation of functions important to safety.

b) For systems important to safety, cryptographic mechanisms aimed at ensuring confidentiality should only be used when justified by a cybersecurity risk analysis.

NOTE 1 I&C environments are usually resource-constrained whereas cryptography is resource-consuming. Integrity and availability are usually more important than confidentiality in I&C environment. Moreover, the use of confidentiality-focused mechanisms involves additional complexity, latency, and potential failures which are antagonistic with safety. Of course, specific contexts and risk analysis results can involve confidentiality needs and lead to the implementation of confidentiality-focused mechanisms. Moreover, I&C related information involves in some cases security classification and use of such confidentiality mechanisms.

c) In the case of I&C systems needed for the real-time management of beyond design basis conditions and nuclear safety emergencies, confidentiality-focused mechanisms should only be used when they can be fully justified.

d) Any communication or data integrity control initially designed for safety or reliability purposes and later considered as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined by staff responsible for cybersecurity, taking into account context-relevant cyberattacks, to confirm its cybersecurity effectiveness.

NOTE 2 As an illustration, the effectiveness of integrity control mechanisms differs largely depending on the nature of the threats: a classical CRC (Cyclic Redundancy Check) code is appropriate with regards to random failures whereas it is inefficient against an attacker, who is able to change the data and recompute the CRC to make the new data considered as valid. Integrity control or assurance mechanisms specifically tailored for cybersecurity would detect the modification in this case.

6.4.6 System availability and function continuity

a) Any control initially designed to protect availability of a system from a safety or reliability perspective and later considered as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined by staff responsible for cybersecurity, taking into account context-relevant cyberattacks, to confirm its cybersecurity effectiveness.

NOTE Availability mechanisms tailored to address non-malicious failures are in some cases completely inefficient against malicious threats. Redundant but non-diversified systems are generally of little help against a cyberattack, as the redundant system will be vulnerable to the same attack.

b) Redundancy and back-up of safety-related data (e.g. configuration, parameters) or of components may be considered as cybersecurity counter-measures only when explicit justifications of their efficiency with respect to the considered malevolent threats are given.

7 Organizational and operational issues

7.1 Governance and responsibilities

a) Both cybersecurity and safety should be represented at the senior management or board level of the organization.

7.2 Coordination between safety and cybersecurity staff during operations

a) For each I&C programmable digital system, all personnel liable to access the system for cybersecurity or safety reasons should be identified. When different staffs, including safety staff and cybersecurity staff, are to access the system, these accesses should be coordinated and the schedules for each optimised.

b) Interventions on I&C programmable digital systems should be authorized both from a cybersecurity point of view and from a safety point of view.

c) Those entities responsible for safety and cybersecurity shall put adequate controls in place to ensure that sub-contractor staff who are granted access to I&C programmable digital systems to perform specific tasks are adequately controlled. In some instances, this may require such staff to be accompanied by a responsible and knowledgeable representative of the system's owner.

d) When a cybersecurity event is detected on a system important to safety, safety impact and cybersecurity impact analyses shall be made.

7.3 Safety and cybersecurity culture

a) Awareness and demonstration activities on I&C programmable digital system cybersecurity threats should be organized for I&C safety staff, in order to help them understand the existence and the nature of such threats and the potential impacts on safety.

b) Reciprocally, staff in charge of cybersecurity should be trained on main safety concepts and associated principles.

c) Opportunities for I&C operators, I&C maintenance staff, safety staff and cybersecurity staff to come together and exchange information about their roles, their practices, their environments and the associated threats should be provided.

NOTE This sort of opportunities is potentially beneficial for cybersecurity threat assessment activities. However, information classification issues are likely to occur; their resolution in a balanced way is a condition to obtain the maximum benefit from such practices.

7.4 Emergency response management

a) Procedures and organisations shall be in place in order to evaluate rapidly and rigorously safety implications of cybersecurity attacks on I&C programmable digital systems.

b) Any cybersecurity response decided in a cybersecurity crisis management context shall be evaluated in terms of safety impact before enforcement.

c) Potential cybersecurity implications of safety events and related response associated to I&C programmable digital systems should be evaluated and managed. Safety shall however remain the priority.

d) Integrated emergency exercise combining both safety and cybersecurity issues should be organized in order to challenge and enhance collaboration between staffs in charge of I&C systems, those in charge of plant safety, and those in charge of cybersecurity (where separated).

e) I&C programmable digital system isolation features and procedures, established for cybersecurity purposes, shall be analyzed in terms of safety consequences before allowance for enforcement.

Annex A
(informative)

Rationale for, and notes related to, the scope of this document

A.1 General

This annex presents the reasons and rationale which have lead to the scope defined in Clause 1.

A.2 Inclusion of I&C programmable digital system not important to safety

This document being focused on the coordination between safety and cybersecurity, a narrower scope, strictly limited to systems important to safety, has been initially considered. The experts involved in the document development have finally decided to include in the scope I&C programmable digital systems not important to safety because:

– it is consistent with the scope of the IEC 62645, to which this document is affiliated;
– assessing the impacts of cyberattacks, including in terms of plant safety, involves a global perspective (for instance, a targeted cyberattack on configuration or maintenance tools can lead to consequences on safety, although these tools can be classified as not important to safety).

The issue of coordinating safety and cybersecurity is better addressed by considering both I&C programmable digital systems important to safety and those not important to safety.

A.3 Exclusion of physical security, room access control and site security surveillance systems

This exclusion is inherited from and consistent with IEC 62645. However, it does not deny that cybersecurity has clear dependencies on the security of the physical environment (e.g., physical protection, power, heating/ventilation/air-conditioning systems, etc.). It is recognized that efficient I&C programmable digital system cybersecurity can only be achieved based on a sound physical security and physical protection regime, complying with national laws and regulations. From an international perspective, the IAEA provides relevant guidance.

A.4 Exclusion of non-malevolent actions and events

In consistence with IEC 62645, cybersecurity relates to prevention of, detection of, and reaction to malicious acts by digital means (cyberattacks) on I&C programmable digital systems. It does not cover considerations related to non-malevolent actions and events such as accidental failures, natural events, or human errors (except for those degrading cybersecurity). Although such aspects are sometimes included in other normative contexts (e.g., in the ISO/IEC 27000 series, the IEC 62443 series or the NIST framework), these exclusions and the focus on the protection against cyberattacks have been decided to provide the maximum consistency and the minimum overlap with the existing nuclear standards and practices. If aspects such as accidental failures, human errors and natural events are of course of prime importance, they are already covered by other SC 45A documents and standards, and are not considered as cybersecurity related in this document (except for human errors degrading cybersecurity).

A.5 Exclusion of development tools and platforms

This document is limited to I&C programmable digital systems used in NPPs, including on-site maintenance and configuration tools. It does not apply directly to development tools and platforms, typically found at the supplier premises. However, development tools and platforms might be impacted by the present document, in order to make the developed I&C systems and architectures meet its requirements. This exclusion does not deny the importance of securing development tools and platforms from a global cybersecurity perspective; it reflects the fact that this document has not been particularly developed to treat these aspects, which deserve due care but are to be treated mostly by non-nuclear specific provisions.

Bibliography

Nuclear I&C system specific references

MDEP, Common Position No. DICWG08, *Common position on the impact of cyber security features on digital I&C safety systems*

IAEA, Nuclear Security Series No. 17, Reference Manual, *Computer security at nuclear facilities*

ORNL, report ref. ORNL/NRC/LTR-07/05, *Safety and non-safety communications and interactions in international nuclear power plants*, 2007

U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, *Cyber security programs for nuclear facilities*, January 2010

U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, Rev. 3, 2011

IEEE, Std 7-4.3.2-2010, *Standard criteria for digital computers in safety systems of nuclear power generating stations*

CSA N290.7 Standard, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities*, 2014

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems in Nuclear Power Plants*

Interface between nuclear safety and nuclear security

IAEA, INSAG-24, *The interface between safety and security at nuclear power plants*

U.S. Nuclear Regulatory Commission, RG 5.74, *Managing the safety-security interface*

WINS, *An integrated approach to nuclear safety and nuclear security*, Rev. 1-1

Non-nuclear I&C system specific references

ISA TR84.00.09-2013, *Security protection layers and considerations related to SIS*

IEC 62443 (all parts), *Security for industrial automation and control systems*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

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

Non I&C-specific IAEA references

IAEA, GS-R-3:2006, *The management system for facilities and activities*

IAEA, Safety Guide No, GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA, Safety Guide No, GS-G-3.5:2009, *Management system for nuclear installations*

IAEA, Safety Standard Series No. SSR-2/1:2012, *Safety of Nuclear Power Plant: Design*

IAEA, Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants*

IAEA, Safety Guide SSG-34, *Design of electrical power systems in Nuclear Power Plants*

IAEA, Safety Glossary, *Terminology used in nuclear safety and radiation protection*

SOMMAIRE

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.

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

L'IEC 62859 édition 1.1 contient la première édition (2016-10) [documents 45A/1104/FDIS et 45A/1118/RVD] et son amendement 1 (2019-10) [documents 45A/1279/FDIS et 45A/1286/RVD].

Dans cette version Redline, une ligne verticale dans la marge indique où le contenu technique est modifié par l'amendement 1. Les ajouts sont en vert, les suppressions sont en rouge, barrées. Une version Finale avec toutes les modifications acceptées est disponible dans cette publication.

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.

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

Le comité a décidé que le contenu de la publication de base et de son amendement 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.

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 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 63046[1]. 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*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC 62645, de l'IEC 61513, et les termes et définitions qui suivent s'appliquent.

NOTE Si ces trois sources donnent des définitions différentes pour un terme donné, la définition du présent document prévaut.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
élément informatique
élément qui s'appuie sur des instructions logicielles s'exécutant sur des microprocesseurs ou des microcontrôleurs

Note 1 à l'article: Le terme "élément" peut être remplacé par le terme «système», «équipement» ou «dispositif».

Note 2 à l'article: Un élément informatique est un type d'élément numérique programmable.

Note 3 à l'article: Ce terme équivaut au terme "élément programmé".

3.2
cyberattaque
tentative, par des moyens numériques, de détruire, de rendre public, de modifier, d'invalider, de voler ou d'obtenir un accès non autorisé ou d'utiliser sans autorisation un actif

Note 1 à l'article: Les cyberattaques incluent les attaques ciblées et non ciblées (p. ex.: logiciels malveillants), réalisées en utilisant des moyens numériques. Le terme "cyberattaque" est synonyme du terme "attaque numérique".

3.3
cybersécurité
ensemble des activités et des mesures dont l'objectif est d'empêcher, de détecter et de réagir:

– à la divulgation malveillante d'informations (confidentialité) susceptibles d'être utilisées pour commettre des actes malveillants, qui pourraient entraîner un accident, une situation non sûre ou une dégradation des performances de la centrale;
– aux modifications malveillantes (intégrité) de fonctions susceptibles de porter atteinte à la fourniture ou à l'intégrité d'un service demandé par des systèmes numériques programmables d'I&C (y compris la perte de contrôle) qui pourraient entraîner un accident, une situation non sûre ou une dégradation des performances de la centrale;
– à la rétention ou à la prévention malveillante de l'accès à ou de la communication d'informations, de données ou de ressources (y compris la perte de visibilité) susceptibles de compromettre la fourniture du service demandé par des systèmes d'I&C (disponibilité) qui pourrait entraîner un accident, une situation non sûre ou une dégradation des performances de la centrale.

Note 1 à l'article: Cette définition est façonnée par rapport au domaine d'application de la présente norme, ainsi qu'à la structure générale des documents du SC 45A. Il est reconnu que le terme «cybersécurité» a un sens plus large dans d'autres normes et guides, où il englobe souvent les menaces non malveillantes, les erreurs humaines et la protection contre les catastrophes naturelles. Ces aspects – à l'exception des erreurs humaines compromettant la cybersécurité – ne relèvent pas du concept de cybersécurité utilisé dans la série de normes du SC 45A. Pour plus de détails sur ces exclusions, se reporter à l'Annexe A.4.

Note 2 à l'article: Les termes «sécurité informatique», «sécurité» et «cybersécurité» sont considérés comme des synonymes dans le présent document.

3.4
évènement de cybersécurité
occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une brèche possible dans la politique de cybersécurité, ou la défaillance de mesure, ou l'apparition d'une situation précédemment inconnue qui pourrait relever de la cybersécurité

3.5
modification logicielle de cybersécurité
modification logicielle dont la raison principale est de mettre en œuvre une ou plusieurs fonctionnalités de cybersécurité, de remédier à une ou plusieurs vulnérabilités de sécurité au sein d'un composant numérique programmable d'I&C, d'empêcher une exploitation réussie de ces vulnérabilités ou de diminuer le plus possible l'aptitude des attaquants à exploiter ces vulnérabilités

3.6
disposition de cybersécurité
mesure ou fonctionnalité conçue spécifiquement à des fins de cybersécurité

Note 1 à l'article: La mise en œuvre de dispositions ne relevant pas de la cybersécurité peut avoir un impact négatif, nul, mais également positif sur la cybersécurité. Cela est notamment le cas de certaines dispositions de sûreté abordées dans le présent document.

Note 2 à l'article: Dans la version anglaises les termes «feature» et «provision» sont synonymes.

3.7
circuit intégré programmé en HDL
HPD
circuit intégré configuré (pour des systèmes d'I&C de centrales nucléaires de puissance) avec des HDLs et outils associés

Note 1 à l'article: Les HDL et outils associés (par exemple simulateur, synthétiseur) sont utilisés pour réaliser les exigences par un assemblage adéquat de ressources microélectroniques prédéveloppées.

Note 2 à l'article: Le développement de HPD peut utiliser des Blocs Prédéveloppés.

Note 3 à l'article: Les HPD sont typiquement basés sur des FPGA ou des circuits intégrés programmables similaires.

[SOURCE: IEC 62566:2012, 3.7]

3.8
séparation logique
séparation du point de vue du réseau de données numériques impliquant l'absence de communications directe de données (c'est-à-dire sans proxy ni dispositif de filtrage de cybersécurité)

3.9
élément numérique programmable
élément qui s'appuie sur des instructions logicielles ou une logique programmable pour accomplir une fonction

Note 1 à l'article: Le terme «élément» peut être remplacé par le terme «système», «équipement» ou «dispositif».

Note 2 à l'article: Les éléments numériques programmables sont les éléments informatiques et les éléments logiques programmables.

Note 3 à l'article: Ce terme utilisé par le SC 45A équivaut au terme "élément électronique programmable" utilisé dans l'IEC 61508.

3.10
élément logique programmable
élément qui s'appuie sur des composants logiques comprenant un circuit intégré composé d'éléments logiques reliés suivant un modèle d'inter-connexion, dont une partie est programmable par l'utilisateur

Note 1 à l'article: Le terme «élément» peut être remplacé par le terme «système», «équipement» ou «dispositif».

Note 2 à l'article: Les éléments logiques programmables constitue une catégorie des éléments numériques programmables.

3.11
disposition de sûreté
mesure ou fonctionnalité conçue spécifiquement à des fins de sûreté

Note 1 à l'article: La mise en œuvre de dispositions ne relevant pas de la sûreté peut avoir un impact négatif, nul, mais également positif sur la sûreté. Cela est notamment le cas de certaines dispositions de cybersécurité abordées dans la présente norme.

Note 2 à l'article: Dans la version anglaises es termes «feature» et «provision» sont synonymes.

3.12
modification du logiciel
modification logicielle
changement dans un document ou des documents déjà approuvés conduisant à un changement dans le code exécutable

Note 1 à l'article: Une modification du logiciel peut être effectuée durant le développement initial (par exemple pour éliminer des défauts mis en évidence dans les phases finales du développement) ou après la mise en service du logiciel.

[SOURCE: IEC 60880:2006, 3.36]

3.13
mise à jour logicielle de sécurité
élément logiciel fourni par un fournisseur de systèmes numériques et conçu dans le but de corriger une ou plusieurs vulnérabilités de sécurité au sein d'un composant numérique, ou de mettre en œuvre une ou plusieurs dispositions de cybersécurité

Note 1 à l'article: Les correctifs de sécurité sont considérés comme des mises à jour logicielles de sécurité.

4 Symboles et abréviations

BIOS	(Basic Input/Output System)	Système de base d'entrée/sortie
CB	(Computer-Based)	Informatique
DCC	Défaillance de cause commune	
CRC	Contrôle de redondance cyclique	
FPGA	(Field-Programmable Gate Array)	Réseau de portes programmable sur site
HDL	(Hardware Description Language)	Langage de description de matériel
IHM	Interface Homme Machine	
HPD	(HDL-Programmed Device)	Circuit intégré programmé en HDL
I&C	Instrumentation et contrôle-commande	
NPP	(Nuclear Power Plant)	Centrale nucléaire de puissance

5 Coordination de la sûreté et de la cybersécurité au niveau de l'architecture d'ensemble

5.1 Généralités

Certaines dispositions de sûreté et certaines caractéristiques architecturales mises en œuvre dans le but de satisfaire aux exigences fondamentales de conception ont parfois une influence bénéfique directe sur la cybersécurité: cela est notamment le cas des dispositifs qui garantissent l'indépendance des équipements, la fiabilité des systèmes ou la diversité des systèmes. Néanmoins, étant donné que la conception de ces dispositions peut ne pas avoir pris en compte de façon appropriée des vulnérabilités potentielles liées aux cyberattaques, des mesures dédiées de cybersécurité peuvent être nécessaires pour élaborer et mettre en œuvre une protection adaptée contre les cyberattaques, sans compromettre la sûreté.

Le présent article fournit les exigences et recommandations nécessaires à la bonne intégration des exigences de cybersécurité selon l'IEC 62645 dans une architecture d'I&C nucléaire, structurée fondamentalement et primordialement par des exigences de sûreté (en particulier celles de l'IEC 61513 et de plusieurs documents de deuxième niveau de la série du SC 45A, notamment l'IEC 62340 et l'IEC 60709).

5.2 Principes fondamentaux et génériques

Les principes suivants s'appliquent au traitement de la cybersécurité au niveau architectural des systèmes d'I&C:

a) La cybersécurité ne doit pas interférer avec les objectifs de sûreté de la centrale et doit préserver leur réalisation. Elle ne doit pas compromettre l'efficacité des dispositions de diversité et de défense en profondeur mises en œuvre par l'architecture d'I&C.

b) Les exigences de cybersécurité affectant l'architecture d'I&C d'ensemble doivent être réalisées après que la conception de l'architecture d'I&C d'ensemble et l'affectation des fonctions d'I&C ont été réalisées selon 5.4 de l'IEC 61513:2011. L'intégration des exigences architecturales de cybersécurité peut donner lieu à un processus de conception itératif.

NOTE L'objectif est de maintenir une architecture d'I&C sûre. Une telle séquence est déjà implicite dans l'IEC 62645, car l'assignation des degrés de sécurité (et de leurs exigences associées) repose sur l'hypothèse que des catégories de sûreté sont déjà assignées aux fonctions de sûreté et que des fonctions de sûreté sont déjà assignées aux systèmes d'I&C.

c) Les dispositifs de cybersécurité ne doivent pas affecter de manière préjudiciable les performances requises (y compris le temps de réponse), l'efficacité requise, la fiabilité requise ou le fonctionnement requis des fonctions importantes pour la sûreté.

d) Les modes de défaillances et les effets des dispositions de cybersécurité sur les fonctions importantes pour la sûreté doivent être analysés et pris en compte.

e) Lorsque deux conceptions d'architectures proposent un niveau équivalent de sûreté, il convient de donner la priorité à la plus sécurisée des deux. Toute complexité non nécessaire doit être évitée, car elle est néfaste à la sûreté et à la cybersécurité.

f) Il convient que le personnel en charge de la cybersécurité réexamine les caractéristiques ou propriétés architecturales conçues pour des raisons de sûreté (p. ex.: indépendance entre les systèmes) et qui ont une valeur comme contremesures potentielles de cybersécurité (à la lueur de l'évaluation des risques liés à la cybersécurité par exemple), en tenant compte des cyberattaques pertinentes par rapport au contexte, pour confirmer leur efficacité en termes de cybersécurité.

Les communications entre les systèmes importants pour la sûreté et les systèmes non importants pour la sûreté, ou entre des systèmes de différentes classes de sûreté, constituent un cas particulier et important. L'IEC 61513 exige déjà que "les liaisons de communications doivent être conçues de telle manière que la communication de données et le comportement des fonctions appartenant à une plus haute catégorie de sûreté ne puissent pas être perturbés par les communications de données avec des systèmes de classes inférieures". Néanmoins, les dispositions prises pour satisfaire à de telles exigences de sûreté ne constituent pas nécessairement une protection efficace contre les cyberattaques et les menaces malveillantes.

5.3 Recommandations et exigences thématiques

5.3.1 Délimitation des zones de sécurité

5.3.1.1 Généralités

D'après la définition donnée dans l'IEC 62645, les zones de sécurité correspondent à la mise en œuvre pratique et architecturale d'une approche graduée de la cybersécurité; elles permettent de regrouper des systèmes d'I&C d'importance similaire pour la sûreté et les performances de la centrale (c'est-à-dire qui ont le même degré de sécurité) pour les besoins d'application et d'administration des mesures de protection. D'après l'IEC 62645, les critères de définition des zones de sécurité comprennent les questions d'organisation (telles que la propriété, la responsabilité), la localisation, les aspects architecturaux ou techniques. Dans la pratique, les zones de sécurité sont mises en œuvre pour contrer la propagation des cyberattaques. Dans ce contexte, lorsqu'un modèle de zone est mis en œuvre comme recommandé par l'IEC 62645, les exigences suivantes s'appliquent:

a) La délimitation des zones de sécurité, selon l'IEC 62645, doit prendre en compte et intégrer les exigences d'indépendance et de séparation physique introduites aux fins d'amélioration de la sûreté.

b) Les aspects liés aux communications de données (y compris la séparation logique) ainsi que les aspects liés à la séparation géographique/physique et à l'indépendance doivent être examinés ensemble pour délimiter les zones de sécurité.

NOTE Les dispositifs de séparation géographique et d'indépendance ne sont pas suffisants pour délimiter les zones de sécurité.

5.3.1.2 Prise en compte des systèmes présentant plusieurs divisions

a) Il convient de regrouper dans la même zone de sécurité les divisions (ou trains) d'un système numérique programmable d'I&C donné, sauf si les communications entre divisions peuvent être surveillées et filtrées de façon efficace du point de vue de la cybersécurité.

b) Les divisions (ou trains) d'un système numérique programmable d'I&C donné doivent être regroupées dans la même zone de sécurité si un outil d'ingénierie partagé est utilisé pour les configurer.

NOTE Cette exigence vaut même si l'outil n'est connecté qu'à une division à un instant donné; si l'outil est corrompu, il peut être le vecteur d'une attaque asynchrone, endommageant les divisions l'une après l'autre.

5.3.1.3 Prise en compte des systèmes partageant des ressources communes

a) Les systèmes numériques programmables d'I&C partageant des outils informatiques en commun (p. ex.: outils de configuration, d'essai et/ou de maintenance) doivent être regroupés dans la même zone de sécurité, sauf s'il est démontré du point de vue de la cybersécurité que les outils ne peuvent pas affecter directement les systèmes auxquels ils sont connectés.

b) Il convient de regrouper dans la même zone de sécurité les systèmes numériques programmables d'I&C partageant un réseau ou un bus de communication commun sans dispositions technique de cybersécurité sécurisant les communications, même s'ils accomplissent des fonctions de différentes catégories de sûreté. Selon l'IEC 62645, l'assignation des degrés de sécurité doit tenir compte de la catégorie de sûreté la plus sensible.

5.3.2 Dispositions relatives à la gestion des défaillances de cause commune (comprenant la diversité)

a) Dans certaines situations, des dispositions prises pour gérer les défaillances de cause commune comprenant la diversité peuvent être mises à profit d'un point de vue de la cybersécurité, auquel cas il convient d'y recourir. Lorsque postulé dans des analyses orientées cybersécurité, le bénéfice en termes de cybersécurité doit être évalué et validé par le personnel en charge de la cybersécurité, en tenant compte des cyberattaques potentielles et des menaces malveillantes contextuelles (conformément à 5.2 f).

NOTE 1 Les exigences, les recommandations et les pratiques associées de sûreté définies en 5.4.2.6 de l'IEC 61513:2011 (pour tous les systèmes d'I&C importants pour la sûreté), à l'Article 13 de l'IEC 60880:2006 (pour les aspects logiciels des systèmes réalisant des fonctions de catégorie A), dans l'IEC 62340 ou dans une norme équivalente (pour les systèmes réalisant des fonctions de catégorie A), sont par exemple directement concernées par 5.3.2a).

NOTE 2 A l'instar de la sûreté, le principe de diversité est également fréquemment utilisé en cybersécurité (p. ex.: utilisation d'outils de test d'intrusion diversifiés, de compétences diversifiées parmi les auditeurs ou les membres d'équipe de cybersécurité). Néanmoins, il est permis de se demander si la diversité bénéficie à la fois à la sûreté et à la cybersécurité dans toutes situations. La diversité est généralement utilisée "en série" pour bénéficier à la cybersécurité (ce qui oblige à compromettre un système l'un après l'autre pour atteindre une cible), alors qu'elle est généralement utilisée "en parallèle" pour bénéficier à la sûreté. Cette utilisation "en parallèle" est parfois contradictoire avec la cybersécurité, car elle augmente la surface d'attaque. Par ailleurs, même du point de vue de la cybersécurité pure, la diversité présente des avantages et des inconvénients. Même si la diversité, utilisée "en série" (p. ex.: deux pare-feu de deux fournisseurs distincts), complique la tâche de l'attaquant (en éliminant les vulnérabilités courantes, en favorisant la complémentarité des fonctions de cybersécurité), elle introduit en même temps un degré supplémentaire de complexité qui augmente le risque d'erreurs de configuration, complique la maintenance, etc.

b) Toutes les mesures de cybersécurité considérées pour être intégrées au niveau de la conception doivent être évaluées pour la possibilité qu'elles puissent introduire des fautes conduisant à des défaillances de cause commune entre des systèmes diversifiés pour des raisons de sûreté. Lorsque de tels risques sont découverts d'autres moyens pour garantir de façon appropriée la cybersécurité doivent être mis en œuvre comme nécessaire.

5.3.3 Dispositions relatives à la séparation

a) Dans certaines situations, des dispositions prises à des fins de séparation peuvent être mises à profit d'un point de vue de la cybersécurité, auxquels cas il convient d'y recourir.

b) Les exigences, les recommandations et les pratiques associées de sûreté définies en 5.4 de l'IEC 60709:2004 concernant l'indépendance des systèmes de contrôle-commande (pour les systèmes réalisant des fonctions de catégorie A), ou dans une norme équivalente, sont potentiellement bénéfiques à la fois en termes de sûreté et de cybersécurité. Lorsque postulé des analyses orientées cybersécurité, le bénéfice en termes de cybersécurité doit être évalué et validé par le personnel en charge de la cybersécurité, en tenant compte des cyberattaques potentielles et des menaces malveillantes contextuelles (conformément à 5.2 f).

5.3.4 Communications de données

a) Les exigences, les recommandations et les pratiques associées à la sûreté définies dans l'IEC 61500:2009 concernant les communications de données (pour les systèmes réalisant des fonctions de catégorie A), ou dans une norme équivalente, peuvent être bénéfiques à la fois en termes de sûreté et de cybersécurité. Lorsque postulé dans des analyses orientées cybersécurité, le bénéfice en termes de cybersécurité doit être évalué et validé par le personnel en charge de la cybersécurité, en tenant compte des cyberattaques et des menaces malveillantes contextuelles (conformément à 5.2 f).

b) Une connaissance approfondie des communications de données utilisées par et entre les systèmes numériques programmables d'I&C (y compris les protocoles, rôles, initiatives, sources et destinations) est utile pour la sécurité et la cybersécurité; ces informations doivent être tenues à jour et documentées, de la conception à la fabrication et à l'exploitation.

6 Coordination de la sûreté et de la cybersécurité au niveau des systèmes individuels

6.1 Généralités

En plus de l'aspect architectural abordé à l'Article 5, la coordination de la sûreté et de la cybersécurité doit également être évaluée au niveau des systèmes individuels. Le présent article fournit les exigences et recommandations nécessaires à cette coordination.

6.2 Principes fondamentaux et génériques

Les principes suivants s'appliquent au traitement des dispositions de cybersécurité prises pour les systèmes numériques programmables d'I&C:

a) La mise en œuvre de dispositions de cybersécurité au cœur même des systèmes importants pour la sûreté doit être justifiée.

NOTE 1 L'ajout de fonctionnalités de cybersécurité à un système important pour la sûreté augmente la complexité du système et est susceptible d'introduire de nouveaux modes de défaillances dans le système. Ces effets peuvent compromettre l'aptitude du système à accomplir sa ou ses fonctions importantes pour la sûreté de manière fiable. En outre, l'évolution rapide des menaces de cybersécurité, des vulnérabilités et des techniques est difficile à concilier avec les processus de modification des systèmes importants pour la sûreté. Néanmoins, il demeure qu'un nombre limité de mesures de cybersécurité est dans certains cas toujours mis en œuvre dans les systèmes importants pour la sûreté: les fonctionnalités d'enregistrement et les dispositions d'authentification en sont des exemples (voir 5.5.3 de l'IEC 61513:2011 et l'IEC 62645).

NOTE 2 La mise en œuvre de fonctionnalités de sécurité en dehors des systèmes importants pour la sûreté facilite la qualification des fonctionnalités de cybersécurité au regard de la réglementation nationale.

b) Les dispositions de cybersécurité ne doivent pas affecter de manière préjudiciable la réalisation des fonctions importantes pour la sûreté, les performances requises (y compris le temps de réponse), la fiabilité requise ou le fonctionnement requis des systèmes numériques programmables importants pour la sûreté.

NOTE 3 Par exemple, l'ordonnancement des tâches, les paramètres fonctionnels, le temps de réponse maximal des fonctions et le niveau maximal d'utilisation des ressources constituent des éléments clés des systèmes numériques programmables d'I&C. La mise en œuvre de dispositions de cybersécurité est susceptible d'influencer, même de manière marginale, un ou plusieurs de ces éléments: le critère important est que cela n'empêche pas le système de satisfaire aux performances requises pour accomplir ses fonctions.

c) Les modes de défaillances et les effets de ces dispositions de cybersécurité sur les fonctions importantes pour la sûreté du système doivent être analysés et pris en compte.

d) Les dispositions de cybersécurité mises en œuvre au sein de systèmes importants pour la sûreté doivent être développées et qualifiées au même niveau que le système auquel elles sont intégrées.

e) Si des dispositions de cybersécurité sont mis en œuvre dans les fonctions d'affichage et de commande de systèmes importants pour la sûreté, ces dispositions ne doivent pas affecter de manière préjudiciable l'aptitude de l'opérateur à préserver la sûreté de la centrale.

f) Lorsque la mise en œuvre d'une disposition de cybersécurité au sein d'un système important pour la sûreté ne peut pas satisfaire à une exigence de cybersécurité, des mesures alternatives de cybersécurité doivent être mises en œuvre. Ces mesures alternatives doivent garantir au minimum que le système satisfait aux exigences du degré de sécurité qui lui est attribué (selon l'IEC 62645).

NOTE 4 Ces mesures alternatives peuvent, par exemple, être d'ordre organisationnel, architectural, ou porter plus particulièrement sur les communications et les interfaces avec le système.

g) Des procédures orientées sûreté (p. ex.: essais de surveillance) ou des fonctions orientées sûreté ont été mises en œuvre pour satisfaire aux objectifs de sûreté. Lorsqu'une procédure ou fonction de sûreté est réutilisée pour atteindre les objectifs de cybersécurité, les objectifs de sûreté et de cybersécurité de la procédure ou de la fonction réutilisée doivent être décrits, et leur réalisation doit être justifiée et documentée.

h) L'extension ou la modification d'une procédure orientée sûreté (p. ex.: essais de surveillance) ou d'une fonction pour des raisons de cybersécurité ne peut être réalisée que s'il a été préalablement justifié et documenté qu'elle satisfaisait toujours à ses objectifs de sûreté.

6.3 Coordination de la sûreté et de la cybersécurité au cours du cycle de vie des systèmes numériques programmables d'I&C

6.3.1 Généralités

Les exigences et recommandations données en 6.2 ne prennent pas spécifiquement en compte les phases de cycle de vie des systèmes numériques programmables d'I&C. Le 6.3 vise à fournir des exigences et des considérations supplémentaires en ce qui concerne les activités du cycle de vie des systèmes numériques programmables d'I&C. Pour des raisons de cohérence, les activités considérées sont celles utilisées à l'Article 6 de l'IEC 62645:2014.

NOTE L'ordre des Paragraphes 6.3.2 à 6.3.9, qui est celui adopté dans l'IEC 62645:2014, ne présente pas nécessairement de façon chronologique les activités, qui peuvent être en réalité exécutées en parallèle ou comprendre des itérations.

6.3.2 Exigences et activités de planification

a) Il convient de définir les exigences de cybersécurité le plus tôt possible au cours du cycle de vie des systèmes numériques programmables d'I&C.

b) Il convient de détecter, documenter et prendre en compte les possibles dépendances, conflits ou renforcements entre les exigences de sûreté et de cybersécurité afin de permettre la définition d'une solution intégrée satisfaisant à la fois aux objectifs de sûreté et de sécurité.

6.3.3 Activités de conception

a) Il convient de concevoir les systèmes d'I&C afin de favoriser les renforcements entre les dispositions de sûreté et de cybersécurité. Il convient de fonder les choix de conception relatifs à ces renforcements sur la base d'une analyse comparative entre:

- les avantages et les inconvénients en ce qui concerne la vérification et la validation des systèmes;
- les avantages et les inconvénients en ce qui concerne la complexité et les interfaces du système.

b) Il convient que le personnel en charge de la cybersécurité réexamine les aspects du système initialement conçus pour des raisons de sûreté et qui a une valeur comme une contremesure potentielle de cybersécurité (à la lueur de l'évaluation des risques liés à la cybersécurité par exemple), en tenant compte des cyberattaques contextuelles, pour confirmer leur efficacité en termes de cybersécurité.

c) Il convient que les dispositions de sécurité pour les systèmes numériques programmables importants pour la sûreté soient conçues de façon à limité leur dépendance par rapport aux mises à jour.

6.3.4 Activités de mise en œuvre

Pour cette phase, la coordination entre la sûreté et la cybersécurité n'est soumise par le présent document à aucune exigence ou recommandation spécifique. Se reporter à l'IEC 62645 pour les exigences relatives à la cybersécurité, à l'IEC 60880 et l'IEC 62138 pour les logiciels des systèmes programmés d'I&C réalisant des fonctions importantes pour la sûreté, ainsi qu'à l'IEC 62566 pour les circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A.

6.3.5 Activités de vérification et de validation

a) Les aspects de cybersécurité et les vulnérabilités associées aux pratiques de codage non sûres peuvent également être évalués lors d'un réexamen ou d'une analyse du code logiciel des systèmes numériques programmables d'I&C réalisée pour des raisons de sûreté (voir l'IEC 60880 et l'IEC 62138 pour les logiciels des systèmes réalisant des fonctions importantes pour la sûreté).

NOTE 1 On note que même s'ils se recoupent, les outils et compétences nécessaires aux fins de réexamen ou d'analyse du code pour des raisons de sûreté et de sécurité sont différents. Le niveau optimal d'intégration de ces activités dépend principalement du contexte.

b) Il convient de prendre des mesures de cybersécurité appropriées pour la protection des données sensibles associées aux revues et analyses de code.

c) Pour éviter la mise en œuvre de fonctionnalités non approuvées, il convient de vérifier et valider les logiciels et le matériel. Cet aspect peut être exigé du point de vue de la sûreté (conformément aux normes applicables), mais aussi dans certains cas du point de vue de la cybersécurité.

NOTE 2 Lors des inspections réalisées à des fins de vérification et de validation du matériel, des fonctions sans fil ou des composants numériques programmables non déclarés peuvent être détectés.

6.3.6 Activités d'installation et d'essais de réception

a) Il convient que les essais de sécurité soient réalisés dans un environnement d'essai représentatif du système installé.

6.3.7 Activités d'exploitation et de maintenance

a) Il convient d'envisager les périodes de mise hors service pour maintenance comme des opportunités pour les mises à jour logicielle de sécurité, sous réserve qu'elles soient compatibles avec les contraintes de qualification.

b) Les essais périodiques des fonctions importantes pour la sûreté ne doivent pas compromettre la cybersécurité des systèmes d'I&C concernés.

c) Il peut être envisagé d'intégrer les vérifications de cybersécurité aux essais périodiques de sûreté.

NOTE De telles intégrations sont soumises à des restrictions (voir 6.2 g) et 6.2 h).

d) Les essais de sécurité intrusifs, y compris les tests d'intrusion, ne doivent pas être conduits au cœur même des systèmes importants pour la sûreté durant l'exploitation. Il convient de prévoir un laboratoire d'essai.

6.3.8 Gestion des modifications

a) Des processus doivent être mis en place pour évaluer et gérer le risque d'interactions négatives entre sûreté et cybersécurité pouvant résulter de modifications apportées à un système numérique programmable d'I&C, y compris à sa configuration, à son statut ou aux procédures connexes.

b) Il convient de mettre en place de procédures transversales pour identifier et exploiter les renforcements mutuels potentiels entre sûreté et cybersécurité pouvant résulter de modifications apportées à un système numérique programmable d'I&C, y compris à sa configuration, à son statut ou aux procédures connexes.

c) Il convient que les modifications dictées par la sûreté soient analysées par le personnel de cybersécurité.

d) Il convient que les modifications dictées par la sécurité soient analysées par le personnel de sûreté.

6.3.9 Activités de mise hors service

a) Il convient de rassembler et d'analyser les informations «conforme à exécution», y compris les interfaces réelles du système, avant d'entamer la mise hors service des systèmes d'I&C individuels pour garantir que les objectifs globaux de sûreté et de cybersécurité de la centrale ne soient pas compromis par la mise hors service du système, ou par les étapes connexes du processus.

b) En particulier, lorsque la mise hors service des systèmes d'I&C individuels donne lieu à des dispositions provisoires visant à maintenir la sûreté d'exploitation de la centrale, ces dispositions peuvent induire des questions de cybersécurité qu'il convient d'analyser et de résoudre si cette analyse le juge pertinent.

6.4 Aspects techniques particuliers aux systèmes d'I&C soumis à des contraintes de sûreté et de cybersécurité

6.4.1 Généralités

Les paragraphes 6.4.2 à 6.4.6 visent à fournir des lignes directrices et des exigences concernant certains aspects de conception et d'exploitation des systèmes numériques programmables d'I&C, lorsqu'ils font l'objet de contraintes à la fois de cybersécurité et de sûreté. Ils abordent des situations courantes pour lesquelles, les exigences ou mesures techniques liées à la sûreté et à la cybersécurité restent en conflit, dépendent les unes des autres ou se renforcent. Ils abordent également la confusion possible entre les mesures de sûreté et de cybersécurité.

6.4.2 Contrôle d'accès logique pour les IHM des systèmes numériques programmables d'I&C dans les salles de commande

a) Aucun contrôle d'accès logique par mot de passe pour les opérateurs ne doit être mis en œuvre sur les IHM des systèmes numériques programmables d'I&C qui nécessitent un accès immédiat de l'opérateur pour la sûreté de la centrale. Il convient de mettre en œuvre des mesures alternatives de contrôle d'accès, acceptables du point de vue de la sûreté.

NOTE Il existe d'autres mesures possibles de contrôle d'accès, notamment l'autorisation d'accéder physiquement aux salles de commande après un contrôle rigoureux du personnel, une limitation d'accès aux logiciels IHM opérationnels (p. ex.: pas d'accès au BIOS ou au niveau du système d'exploitation), logiciels avec restrictions d'entrée (p. ex.: uniquement à partir de listes prédéfinies). De telles mesures alternatives de contrôle d'accès sont de grande importance pour les salles de commande qui ne sont pas dotées d'un personnel permanent (p. ex.: salle de replis).

b) Il convient de ne pas mettre en œuvre de mécanisme de verrouillage de compte/nœud ou de connexion différée après des tentatives d'accès non valides pour les systèmes numériques programmables d'I&C qui nécessitent un accès immédiat de l'opérateur pour la sûreté de la centrale. Il convient de mettre en œuvre des mesures alternatives, acceptables du point de vue de la sûreté.

c) La gestion des contrôles d'accès doit prendre en compte les besoins opérationnels spécifiques présentant des implications au niveau de la sûreté (p. ex.: maintenance nocturne, conditions hors dimensionnement et situation de crise nucléaire).

On note que les exigences données en 6.4.2 s'appliquent aux systèmes numériques programmables d'I&C, mais pas à leurs outils numériques de maintenance.

6.4.3 Modifications logicielles

6.4.3.1 Modifications logicielles de cybersécurité

a) Les modifications du logiciel de cybersécurité (y compris l'application d'une mise à jour logicielle de sécurité) constituent un type de modification logicielle et doivent être traitées en conséquence, autrement dit conformément à l'Article 11 de l'IEC 60880:2006 pour les logiciels des systèmes informatisés d'I&C réalisant des fonctions de catégorie A, conformément aux 5.10 et 6.10 de l'IEC 62138:2004 pour les logiciels des systèmes

informatisés d'I&C réalisant des fonctions de catégorie B ou C, et conformément aux procédures locales applicables aux systèmes numériques programmables d'I&C non importants pour la sûreté.

b) La décision de mettre en œuvre une modification logicielle de cybersécurité doit être validée par du personnel qualifié dans le domaine des systèmes ciblés, de leur utilisation et de leurs implications en termes de sécurité, en conjonction avec le personnel responsable de ces systèmes.

c) Des essais doivent être réalisés pour démontrer qu'une modification logicielle de cybersécurité (y compris l'application d'une mise à jour logicielle de sécurité) ne compromet pas l'aptitude du système à accomplir ses fonctions importantes pour la sûreté.

d) Lorsque la décision d'appliquer une mise à jour logicielle de sécurité n'est pas retenue (p. ex.: essais décrits en c) ou parce que la modification n'est pas possible en exploitation):

   – la vulnérabilité associée à cette non-application doit être tracée et gérée, avec le niveau adéquat de confidentialité;

   – une analyse dédiée des risques doit caractériser les risques associés à cette décision;

   – si l'analyse des risques identifie la nécessité de mettre en place des mesures correctives de cybersécurité, leur mise en œuvre doit être approuvée par le responsable de cybersécurité compétent en conjonction avec les personnes responsables des systèmes concernés.

6.4.3.2 Autres modifications du logiciel

a) Des analyses ou des essais doivent être réalisés afin de confirmer qu'une modification logicielle réalisée pour des raisons de sûreté ou d'autres raisons non liées à la cybersécurité (p. ex.: fiabilité, nouvelle fonctionnalité), ne mette pas en défaut la cybersécurité.

b) Aucune modification logicielle identifiée comme compromettant la cybersécurité ne doit être mise en œuvre sur des systèmes d'I&C de centrales, à moins de satisfaire aux ~~trois~~ quatre conditions suivantes:

   – une analyse ~~dédiée~~ des ~~s~~ risque~~s~~ dédiée a été réalisée ~~et que les risques résiduels ont été formellement acceptés~~ pour identifier le risque;

   – les mesures ~~correctives~~ compensatoires de cybersécurité qui auraient pu être identifiées par l'analyse de risques ~~(le cas échéant)~~ ont été approuvées par le responsable de cybersécurité compétent en conjonction avec les personnes responsables des systèmes concernés;

   – ~~ces~~ toutes les mesures de cybersécurité ~~compensatrice~~ compensatoires ont été mises en œuvre ~~le cas échéant~~.

   – le risque résiduel restant est approuvé par le responsable de cybersécurité compétent en conjonction avec les personnes responsables des systèmes concernés.

6.4.4 Fonctionnalités de journalisation et d'audit

a) Il convient de mettre en œuvre les fonctionnalités locales de génération d'enregistrements, de résumé d'audit et de génération de rapports à des fins de cybersécurité le plus possible à l'extérieur des systèmes importants pour la sûreté.

b) Il convient que les messages de défaillances générés par un système d'I&C numérique programmable soient enregistrés en dehors de ce système pour les besoins des analyses de sûreté ou de cybersécurité.

c) Il convient que les connexions logiques éventuellement mises en œuvre pour permettre de gérer de manière centralisée des journaux système et/ou de cybersécurité n'interfèrent pas avec les exigences d'indépendance imposées aux systèmes importants pour la sûreté.

NOTE Parmi les différentes approches possibles, l'utilisation de canaux strictement unidirectionnels pour la transmission des journaux est bénéfique à la fois du point de vue de la sécurité et de la sûreté.

d) Il convient de mettre en œuvre et de préconfigurer préférentiellement les mécanismes de journalisation de manière à ce qu'aucune gestion des journaux (p. ex.: niveau de détail, sélectivité des événements enregistrés) ne soit nécessaire pendant l'exploitation de la centrale.

6.4.5 Utilisation de la cryptographie par des systèmes d'I&C

a) Des mécanismes cryptographiques peuvent être utilisés par des systèmes numériques programmables d'I&C, mais ils ne doivent pas affecter de manière préjudiciable les performances requises (y compris le temps de réponse), l'efficacité, la fiabilité ou le fonctionnement des fonctions importantes pour la sûreté.

b) Pour les systèmes importants pour la sûreté, il convient de n'utiliser les mécanismes cryptographiques destinés à préserver la confidentialité que lorsqu'une analyse des risques de cybersécurité le justifie.

NOTE 1 Les environnements d'I&C sont habituellement contraints en ressources, tandis que la cryptographie est consommatrice de ressources. L'intégrité et la disponibilité sont habituellement plus importantes que la confidentialité dans un environnement d'I&C. Par ailleurs, l'utilisation de mécanismes de confidentialité implique un degré supplémentaire de complexité, de latence ainsi que des défaillances potentielles qui sont contradictoires avec la sûreté. Bien entendu, des contextes spécifiques et les résultats d'analyses de risques peuvent impliquer des besoins de confidentialité et conduire à la mise en œuvre de mécanismes de confidentialité. En outre, les informations relatives aux systèmes d'I&C impliquent dans certains cas une classification de sécurité et l'utilisation de tels mécanismes de confidentialité.

c) Il convient que les mécanismes de confidentialité ne soient utilisés que pour le cas des systèmes indispensables pour la gestion en temps réel des conditions hors dimensionnement et des situations de crise nucléaire lorsque cela peut être pleinement justifié.

d) Il convient que le personnel en charge de la cybersécurité réexamine les mécanismes de contrôle d'intégrité des communications ou des données, initialement conçus pour des raisons de sûreté et de fiabilité, et considérés ultérieurement comme une contremesure potentielle de cybersécurité (à la lueur de l'évaluation des risques liés à la cybersécurité par exemple), en tenant compte des cyberattaques contextuelles, pour confirmer leur efficacité en termes de cybersécurité.

NOTE 2 Pour illustrer le propos on note que l'efficacité des mécanismes de contrôle d'intégrité varie considérablement selon la nature des menaces; un code de contrôle de redondance cyclique (CRC) classique peut s'avérer approprié dans le cas de défaillances aléatoires, mais se révéler inefficace face à un attaquant capable de modifier les données et de recalculer le CRC pour que le tout paraisse valide. Des mécanismes de contrôle d'intégrité ou d'assurance spécifiquement adaptés pour la cybersécurité auraient détecté la modification dans ce cas.

6.4.6 Disponibilité du système et continuité des fonctions

a) Il convient que le personnel en charge de la cybersécurité réexamine les mesures, conçues initialement dans le but de préserver la disponibilité d'un système du point de vue de la sûreté ou de la fiabilité, et considérées ultérieurement comme des contremesures potentielles de cybersécurité (à la lueur de l'évaluation des risques liés à la cybersécurité par exemple), en tenant compte des cyberattaques et des menaces malveillantes contextuelles, pour confirmer leur valeur ajoutée en termes de cybersécurité.

NOTE Les mécanismes de disponibilité adaptés pour traiter les défaillances non malveillantes se révèlent dans certains cas inefficaces contre les menaces malveillantes. Des systèmes redondants, mais non diversifiés, peuvent s'avérer peu utiles en présence d'une cyberattaque, tout comme le serait un système redondant face à la même attaque.

b) La redondance et la sauvegarde des données (p. ex.: configuration, paramètres) ou de composants de sûreté peuvent être considérées comme des contremesures de cybersécurité uniquement si leur efficacité par rapport aux menaces malveillantes considérées a été justifiée de manière explicite.

7 Questions d'organisation et d'exploitation

7.1 Gouvernance et responsabilités

a) Il convient que la sûreté et la cybersécurité soient représentées au niveau de la direction ou du conseil d'administration de l'entreprise.

7.2 Coordination entre le personnel de sûreté et de cybersécurité en cours d'exploitation

a) Pour chaque système numérique programmable d'I&C, il convient d'identifier le personnel autorisé à accéder au système pour des raisons de cybersécurité ou de sûreté. Lorsque des personnels différents, y compris le personnel de sûreté et le personnel de cybersécurité, doivent accéder au système, il convient de coordonner ces accès et d'optimiser les plannings correspondants.

b) Il convient d'autoriser les interventions sur les systèmes numériques programmables d'I&C à la fois du point de vue de la cybersécurité et de la sûreté.

c) Les unités en charge de la sûreté et de la cybersécurité doivent mettre en place des mesures ad hoc pour que les sous-traitants puissent accéder sous contrôle approprié aux systèmes numériques programmables d'I&C pour réaliser des tâches particulières. Dans certains cas, ceci peut nécessiter l'accompagnement par une personne responsable et compétente représentant le propriétaire du système.

d) Lorsqu'un événement de cybersécurité est détecté sur un système important pour la sûreté, des analyses d'impact sur la sûreté et sur la cybersécurité doivent être réalisées.

7.3 Culture de sûreté et de cybersécurité

a) Il convient d'organiser des activités de sensibilisation et de démonstration sur les menaces de cybersécurité portant atteinte aux systèmes numériques programmables d'I&C, à l'intention du personnel sûreté des systèmes d'I&C, dans le but de les aider à mieux comprendre l'existence et la nature de ces menaces ainsi que les impacts potentiels pour la sûreté.

b) Réciproquement, il convient de former le personnel en charge de la cybersécurité aux principaux concepts de sûreté et principes associés.

c) Il convient de permettre aux opérateurs de systèmes d'I&C, au personnel de maintenance d'I&C, au personnel de sûreté et au personnel de cybersécurité de se réunir et de discuter et d'échanger des informations sur leurs responsabilités, les pratiques, les menaces, et il convient de fournir des environnements appropriés pour cela et d'encourager de telles opportunités.

NOTE On note que ce type d'opportunité peut être bénéfique au niveau cybersécurité pour les activités d'évaluation des menaces, même si cela est susceptible d'engendrer des problèmes de classification de l'information qui seront résolus de manière équilibrée pour un bénéfice maximum de ces pratiques.

7.4 Gestion des mesures d'urgence

a) Des procédures et méthodes doivent être mises en place afin d'évaluer de manière rapide et rigoureuse les implications en termes de sûreté que représentent les attaques de cybersécurité pour les systèmes numériques programmables d'I&C.

b) Toute réponse de cybersécurité décidée dans un contexte de gestion de crises de cybersécurité doit être évaluée en termes d'impact pour la sûreté avant mise en œuvre.

c) Il convient d'évaluer et de gérer les implications potentielles en termes de cybersécurité que représentent les événements de sûreté, ainsi que les plans d'action associés qui concernent systèmes numériques programmables d'I&C. La sûreté doit néanmoins rester la priorité.

d) Il convient d'organiser des exercices intégrés de gestion d'urgence couvrant à la fois des problèmes de sûreté et de cybersécurité dans le but d'éprouver et de renforcer la collaboration entre les personnels en charge des systèmes d'I&C, ceux en charge de la sûreté de la centrale et ceux en charge de la cybersécurité (lorsqu'ils sont distincts).

e) Les procédures et dispositifs d'isolement des systèmes numériques programmables d'I&C, définis à des fins de cybersécurité, doivent faire l'objet d'une analyse en termes d'effets pour la sûreté avant toute décision d'exécution.

Annexe A
(informative)

Justifications et notes relatives au domaine d'application du présent document

A.1 Généralités

La présente annexe explique les raisons et les justifications ayant donné lieu au domaine d'application défini à l'Article 1.

A.2 Inclusion des systèmes numériques programmables d'I&C non importants pour la sûreté

Dans la mesure où le présent document traite de la coordination entre la sûreté et la cybersécurité, un domaine d'application plus restreint, limité strictement aux systèmes importants pour la sûreté, avait été envisagé dans un premier temps. Les experts concernés par l'élaboration du document ont finalement décidé d'inclure les systèmes numériques programmables d'I&C non importants pour la sûreté dans le domaine d'application, car:

– il est cohérent avec le domaine d'application de l'IEC 62645, à laquelle le présent document est affilié;
– l'évaluation des impacts des cyberattaques, y compris par rapport à la sûreté de la centrale, implique une perspective globale (p. ex.: une cyberattaque ciblée sur les outils de maintenance ou de configuration peut avoir des conséquenses sur la sûreté, même si ces outils sont classés comme non importants pour la sûreté).

Il est préférable d'aborder la question de la coordination de la sûreté et de la cybersécurité en considérant à la fois les systèmes numériques programmables d'I&C importants pour la sûreté et les systèmes numériques programmables d'I&C non importants pour la sûreté.

A.3 Exclusion des systèmes de sécurité physique, de contrôle d'accès aux salles de commande et de surveillance sécuritaire du site

Cette exclusion est issue de, et est cohérente avec, l'IEC 62645. Néanmoins, elle ne nie pas le fait que la cybersécurité dépend clairement de la sécurité de l'environnement physique (p. ex.: protection physique, alimentation électrique, systèmes de chauffage, de ventilation et de conditionnement de l'air, etc.). Il est reconnu qu'une cybersécurité efficace des systèmes numériques programmables d'I&C ne peut être réalisée qu'à condition de mettre en place un programme solide de sécurité et de protection physiques, en accord avec la réglementation nationale. Au niveau international, l'Agence internationale de l'énergie atomique (AIEA) fournit des lignes directrices pertinentes.

A.4 Exclusion des actions et événements non malveillants

Conformément à l'IEC 62645, la cybersécurité se réfère à la prévention, la détection et la réaction à des actes malveillants portant atteinte aux systèmes numériques programmables d'I&C en utilisant des moyens numériques (cyberattaques). 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). Même si ces aspects sont parfois couverts dans d'autres contextes normatifs, par exemple dans la série ISO/IEC 27000, la série IEC 62443 ou le cadre de travail du NIST (National Institute of Standards and Technology), il a été décidé que ces exclusions et l'intérêt renforcé pour la protection contre les cyberattaques devaient permettre d'améliorer la cohérence et de minimiser les redondances avec les normes et pratiques nucléaires existantes. Même si les aspects tels que les défaillances accidentelles,

les événements naturels et les erreurs humaines sont bien entendu de grande importance, 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 (à l'exception des erreurs humaines compromettant la cybersécurité).

A.5 Exclusion des outils et plateformes de développement

Le présent document est limité aux systèmes numériques programmables d'I&C utilisés dans les NPP, y compris les outils configuration et de maintenance sur site. Il ne s'applique pas directement aux outils et plateformes de développement, se trouvant habituellement dans les locaux du fournisseur. Néanmoins, en cherchant à ce que les architectures et systèmes d'I&C développés satisfassent à leurs exigences, le présent document pourrait impacter les outils et plateformes de développement. Cette exclusion ne nie pas l'importance de sécuriser les outils et plateformes de développement du point de vue global de la cybersécurité; elle reflète le fait que le présent document n'a pas été élaboré dans le but d'aborder ces aspects qui méritent certes de l'attention, mais peuvent être traités en large partie par des dispositions non spécifiques au domaine nucléaire.

Bibliographie

Références spécifiques aux systèmes d'I&C nucléaires

MDEP Common Position No DICWG08, *Common position on the impact of cyber security features on digital I&C safety systems* (disponible en anglais seulement)

Collection Sécurité nucléaire de l'AIEA – N° 17, Manuel de référence, *La sécurité informatique dans les installations nucléaires*

Rapport de l'ORNL réf. ORNL/NRC/LTR-07/05, *Safety and non-safety communications and interactions in international nuclear power plants*, 2007 (disponible en anglais seulement)

U.S. Nuclear Regulatory Commission Regulatory Guide 5.71, *Cyber security programs for nuclear facilities*, janvier 2010 (disponible en anglais seulement)

U.S. Nuclear Regulatory Commission Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, Rev. 3, 2011 (disponible en anglais seulement)

IEEE Std 7-4.3.2-2010, *Standard criteria for digital computers in safety systems of nuclear power generating stations* (disponible en anglais seulement)

CSA N290.7 Standard, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities*, 2014

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems in Nuclear Power Plants*

Interface entre la sûreté nucléaire et la sécurité nucléaire

IAEA INSAG-24, *The interface between safety and security at nuclear power plants* (disponible en anglais seulement)

NRC RG 5.74, *Managing the safety-security interface* (disponible en anglais seulement)

WINS, *An integrated approach to nuclear safety and nuclear security*, Rev. 1-1 (disponible en anglais seulement)

Références spécifiques aux systèmes d'I&C non nucléaires

ISA TR84.00.09-2013, *Security protection layers and considerations related to SIS* (disponible en anglais seulement)

IEC 62443 (toutes les parties), *Sécurité des automatismes industriels et des systèmes de commande*

IEC 61508-1, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

IEC 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

IEC 61508-4, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

Références AIEA spécifiques aux systèmes d'I&C non nucléaires

Normes de sûreté de l'AIEA, Prescriptions N° GS-R-3: 2011, *Système de gestion des installations et des activités*

IAEA Safety Guide N° GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA Safety Guide N° GS-G-3.5:2009, *Management system for nuclear installations*

Normes de sûreté de l'AIEA N° SSR-2/1:2012, *Prescriptions de sureté particulières, Sûreté des centrales nucléaires: Conception*

IAEA Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants*

IAEA Safety Guide SSG-34, *Design of electrical power systems in Nuclear Power Plants*

Glossaire de sûreté de l'AIEA, *Terminologie employée en sûreté nucléaire et radioprotection*

IEC 62859

Edition 1.1 2019-10
CONSOLIDATED VERSION

FINAL VERSION

VERSION FINALE

colour inside

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

IEC 62859:2016-10+AMD1:2019-10 CSV(en-fr)

CONTENTS

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.

This consolidated version of the official IEC Standard and its amendment has been prepared for user convenience.

IEC 62859 edition 1.1 contains the first edition (2016-10) [documents 45A/1104/FDIS and 45A/1118/RVD] and its amendment 1 (2019-10) [documents 45A/1279/FDIS and 45A/1286/RVD].

This Final version does not show where the technical content is modified by amendment 1. A separate Redline version with all changes highlighted is available in this publication.

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.

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

The committee has decided that the contents of the base publication and its amendment 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.

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 63046[1]. 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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62645, in IEC 61513 and the following apply.

NOTE If for a given term, different definitions are provided in these three sources, the definition of the present document applies.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
computer-based item
item that relies on software instructions running on microprocessors or microcontrollers

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: A computer-based item is a kind of programmable digital item.

Note 3 to entry: This term is equivalent to software-based item.

3.2
cyberattack
attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Note 1 to entry: Cyberattacks include targeted and non-targeted (e.g. malwares) attacks by digital means. Cyberattack is synonymous with digital attack.

3.3
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

– malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

Note 1 to entry: This definition is tailored with respect to this standard scope and overall SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the SC 45A standard series. See Annex A.4 for more detail about such exclusions.

Note 2 to entry: Computer security, security and cybersecurity are considered synonymous in this document.

3.4
cybersecurity event
identified occurrence of a system, service or network state indicating a possible breach of cybersecurity policy or failure of controls, or a previously unknown situation that may be cybersecurity relevant

3.5
cybersecurity-driven software modification
software modification of which the main reason is to implement one or more cybersecurity features, or remediate one or several security vulnerabilities in a I&C programmable digital component, or to prevent successful exploitation of these vulnerabilities or to mitigate attackers’ capabilities to exploit these vulnerabilities

3.6
cybersecurity feature
provision, control or function specifically designed for cybersecurity purposes

Note 1 to entry: Non-cybersecurity features implementation can have negative, neutral, but also positive impact on cybersecurity. This is particularly the case of some safety features, as discussed in this document.

Note 2 to entry: The terms “feature” and “provision” are considered synonymous in this document.

3.7
HDL-Programmed Device
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools

Note 1 to entry: HDLs and related tools (e.g. simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2 to entry: The development of HPDs can use pre-developed blocks.

Note 3 to entry: HPDs are typically based on blank FPGAs (Field Programmable gate Arrays) or similar programmable integrated circuits.

[SOURCE: IEC 62566:2012, 3.7]

3.8
logical separation
separation from a digital data network perspective involving the absence of direct data communications (i.e. without any proxy or cybersecurity filtering device)

3.9
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: The main programmable digital items are computer-based items and programmable logic items.

Note 3 to entry: This term used by SC 45A is equivalent to Programmable Electronic item used in IEC 61508.

3.10
programmable logic item
item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable

Note 1 to entry: The term item can be replaced by the terms system, or equipment, or device.

Note 2 to entry: A programmable logic item is a kind of programmable digital item.

3.11
safety feature
provision, control or function specifically designed for safety purposes

Note 1 to entry: Non-safety features implementation can have negative, neutral, but also positive impact on safety. This is particularly the case of some cybersecurity features, as discussed in this standard.

Note 2 to entry: The terms “feature” and “provision” are considered synonymous.

3.12
software modification
change in an already agreed document (or documents) leading to an alteration of the executable code

Note 1 to entry: Software modifications may occur either during initial software development (e.g. to remove faults found in later stages of development), or after the software is already in service.

[SOURCE: IEC 60880:2006, 3.36]

3.13
software security update
piece of software provided by a digital system supplier and designed to fix one or several security vulnerabilities in a digital component, or implement one or more cybersecurity features

Note 1 to entry: Security patches are considered as software security updates.

4 Symbols and abbreviations

BIOS	Basic Input/Output System
CB	Computer-Based
CCF	Common Cause Failure
CRC	Cyclic Redundancy Check
FPGA	Field-Programmable Gate Array
HDL	Hardware Description Language
HMI	Human-Machine Interface

HPD HDL-Programmed Device

I&C Instrumentation and Control

NPP Nuclear Power Plant

5 Coordinating safety and cybersecurity at the overall architecture level

5.1 General

Several safety features and architectural characteristics implemented in order to address design basis requirements are in some cases directly beneficial to cybersecurity: this includes some of the features that support equipment independence, system reliability or system diversity. However, considering that the design of these features may not have adequately taken into account potential vulnerabilities to cyberattacks, dedicated cybersecurity measures may be needed to achieve adequate cybersecurity, without degrading safety.

This clause provides requirements and recommendations to enable a smooth integration of cybersecurity requirements as per IEC 62645 in a nuclear I&C architecture, fundamentally and firstly structured by safety-oriented requirements (in particular those of IEC 61513 and several second level documents of the SC 45A series, including IEC 62340 or IEC 60709).

5.2 Fundamental and generic principles

The following principles apply for the treatment of cybersecurity at the I&C architectural level:

a) Cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realisation. It shall not compromise the effectiveness of the diversity and defence-in-depth features implemented by the I&C architecture.

b) Cybersecurity requirements impacting the overall I&C architecture shall be addressed after the overall I&C architecture design and assignment of the I&C functions have been first made as per 5.4 of IEC 61513:2011. The integration of architectural cybersecurity requirements may lead to an iterative design process.

NOTE The objective is to secure a safe I&C architecture. Such a sequence is already implicit in IEC 62645, as the assignment of security degrees (and their associated requirements) assumes that safety categories are already assigned to safety functions, and that the safety functions are already assigned to I&C systems.

c) Cybersecurity features shall not adversely impact the required performance (including response time), required effectiveness, required reliability or required operation of functions important to safety.

d) The failure modes and consequences of cybersecurity features on the functions important to safety shall be analysed and taken into account.

e) When two architecture designs offer equivalent level of safety, priority should be given to the most secure one. Unnecessary complexity shall be avoided as it is detrimental to both safety and cybersecurity.

f) Any architectural property or characteristics designed for safety reason (e.g., independence between systems), which has value as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined taking into account context-relevant cyberattacks, by staff responsible for cybersecurity, to confirm its cybersecurity effectiveness.

A particular case corresponds to communications between systems important to safety and systems not important to safety, or between systems of different safety classes. IEC 61513 already requires that communication links are designed in such a way that data communication and operation of the higher safety category function cannot be jeopardised by data communication with lower classified systems. However, the provisions taken to fulfil such safety requirements are not necessarily robust against malicious threats and cyberattacks.

5.3 Thematic requirements and recommendations

5.3.1 Delineation of security zones

5.3.1.1 General

As defined in IEC 62645, security zones are practical and architectural implementations of a graded approach to cybersecurity; they allow I&C systems with similar importance concerning safety and plant performance (i.e. having the same security degree) to be grouped together for administration and application of protective measures. As per IEC 62645, criteria for defining a security zone include organizational issues (such as ownership/responsibility), localisation, architectural or technical aspects. In practice, security zones are implemented as means against the propagation of cyberattacks. In such context, when a zone model is enforced as recommended by IEC 62645, the following applies:

a) The delineation of security zones, as per IEC 62645, shall take into account and leverage independence and physical separation requirements introduced for the purpose of enhancing safety.

b) Data communication aspects (incl. logical separation) and geographical/physical separation as well as independence aspects shall be considered together to delineate security zones.

NOTE Geographical separation and independence features are not sufficient to delineate security zones.

5.3.1.2 Dealing with systems with several divisions

a) The divisions (or trains) of a given I&C programmable digital system should be grouped in the same security zone, unless the communications between divisions can be efficiently filtered and monitored from a cybersecurity perspective.

b) The divisions (or trains) of a given I&C programmable digital system shall be grouped in the same security zone if a common engineering tool is used to configure them.

NOTE This requirement holds even if the tool is connected only to one division at a time: if the tool is compromised, it can support an asynchronous attack, compromising divisions one after the other.

5.3.1.3 Dealing with systems sharing common resources

a) I&C programmable digital systems sharing common computer-based tools (e.g. configuration, testing, and/or maintenance tools) shall be grouped in the same security zone, unless it is demonstrated from a cybersecurity perspective that the tools cannot directly impact the systems they are connected to.

b) I&C programmable digital systems sharing a common network or communication bus without cybersecurity technical provisions securing the communications should be grouped in the same security zone, even if they perform functions of different safety categories. As per IEC 62645, the security degree assignment shall take into account the most sensitive safety category.

5.3.2 Provisions for coping with common cause failures (including diversity)

a) In some cases, provisions taken in order to cope with common cause failures (CCF), including diversity, can be leveraged from a cybersecurity perspective, and should be leveraged in such cases. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and potential cyberattacks (consistently with 5.2 f).

NOTE 1 Provisions resulting from requirements, recommendations and associated safety practices as per 5.4.2.6 of IEC 61513:2011 (for all I&C systems important to safety), Clause 13 of IEC 60880:2006 (for software aspects of systems performing category A functions), IEC 62340 or equivalent (for systems performing category A functions), are for instance directly concerned by 5.3.2a).

NOTE 2 As for safety, diversity is also commonly used in cybersecurity: examples include the use of diverse penetration testing tools, diverse skills of cybersecurity team members or auditors. However, expecting benefit from diversity in all situations for both safety and cybersecurity is questionable. Diversity is generally used “in series” to bring cybersecurity benefit (involving the need to compromise one system after another to reach a target), whereas it is generally used “in parallel” to bring benefit in safety. Such use “in parallel” is in some

cases antagonistic with cybersecurity, increasing the attack surface. Moreover, even from a pure cybersecurity perspective there are pros and cons to diversity. Used “in series” (for instance two firewalls from different providers), diversity makes the attacker task more complex (avoiding common vulnerabilities, cybersecurity functions completing each others), but at the same time, it introduces complexity leading to higher risk of configuration errors, difficulty of maintenance, etc.

b) Any cybersecurity measures considered for inclusion in the design shall be assessed for their potential to introduce fault leading to CCF between systems diversified for safety reasons. Where such risks are found, alternative means of achieving adequate cybersecurity shall be implemented as necessary.

5.3.3 Separation provisions

a) In some cases, provisions taken for separation purposes can be leveraged from a cybersecurity perspective, and should be leveraged in such cases.

b) Requirements, recommendations and associated safety practices as per 5.4 of IEC 60709:2004 on independence from control systems (for systems supporting category A functions), or equivalent, are potentially beneficial both in terms of safety and cybersecurity. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and potential cyberattacks (consistently with 5.2 f).

5.3.4 Data communications

a) Requirements, recommendations and associated safety practices as per IEC 61500:2009 on data communications (for systems supporting category A functions), or equivalent, are potentially beneficial both in terms of safety and cybersecurity. When claimed in cybersecurity oriented analyses, the cybersecurity benefit shall be assessed and validated by staff responsible for cybersecurity, taking into account context-relevant malicious threats and cyberattacks (consistently with 5.2 f).

b) A detailed knowledge of data communications in use by and between I&C programmable digital systems (incl. protocols, roles, initiatives, sources and destinations) is beneficial both for safety and cybersecurity and shall be maintained and documented, from design to implementation and operations.

6 Coordinating safety and cybersecurity at the individual system level

6.1 General

In addition to the architectural level treated in Clause 5, coordination of safety and cybersecurity shall also be considered at the individual system level. This clause provides requirements and recommendations for such coordination.

6.2 Fundamental and generic principles

The following principles apply for the treatment of cybersecurity features on I&C programmable digital systems:

a) Implementation of cybersecurity features directly in systems important to safety shall be justified.

NOTE 1 Adding cybersecurity features to system important to safety increases system complexity and has the potential to introduce new failure modes to the system. Such consequences can challenge the system ability to perform its function(s) important to safety in a reliable manner. Moreover, the rapid evolution pace of cybersecurity threats, vulnerabilities and techniques is hard to conciliate with the modification processes of systems important to safety. However, a limited number of cybersecurity controls are still in some cases implemented in systems important to safety: examples include logging capability and authentication mechanisms, as per 5.5.3 of IEC 61513:2011 and as per IEC 62645.

NOTE 2 Implementation of cybersecurity features outside systems important to safety ease separate qualification of cybersecurity related features when required by national regulations.

b) Cybersecurity features shall not adversely impact the realisation of functions important to safety, the required performance (including response time), required reliability, or required operation of programmable digital systems important to safety.

NOTE 3 Key elements of I&C programmable digital system performance are for example task ordering, functional parameters, maximum response time of functions and maximum usage of resources. Cybersecurity features implementation is likely to influence, even marginally, one or several of these elements: the important criterion is that it does not prevent the system from meeting the required performance to ensure its functions.

c) The failure modes and consequences of these cybersecurity features on the system's functions important to safety shall be analysed and taken into account.

d) Cybersecurity features implemented in systems important to safety shall be developed and qualified to the same level as the system these features reside in.

e) If cybersecurity features are implemented in displays and controls of systems important to safety, they shall not adversely impact the operator's ability to maintain plant safety.

f) When a cybersecurity requirement cannot be met by the implementation of a cybersecurity feature in a system important to safety, alternative cybersecurity measures shall be implemented. These alternative measures shall at least ensure that the system's security degree requirements (as per IEC 62645) are met.

NOTE 4 Such alternative measures can be for instance organisational, architectural, or in particular dealing with the communications and interfaces with the system.

g) Safety-oriented procedures (e.g. surveillance tests) or functions have been implemented to fulfil safety objectives. When reusing a safety procedure or function to achieve cybersecurity objectives, both the safety objectives and the cybersecurity objectives of the reused procedure or function shall be described, and their achievement shall be justified and documented.

h) The extension or modification of a safety-oriented procedure (e.g., surveillance tests) or function for cybersecurity purpose can only be made if it has been previously justified and documented that its safety objectives are still achieved.

6.3 Safety and cybersecurity coordination during the I&C system lifecycle

6.3.1 General

The requirements and recommendations provided in 6.2 do not specifically consider the lifecycle phases of I&C programmable digital systems. The objective of 6.3 is to provide additional requirements and considerations with respect to I&C programmable digital system lifecycle activities. For consistency reasons, the activities considered are those used in Clause 6 of IEC 62645:2014.

NOTE The order of Subclauses 6.3.2 to 6.3.9, adopted from IEC 62645:2014, does not necessarily present the timely order of activities which are sometimes in reality partially executed in parallel, or include iterations.

6.3.2 Requirements and planning activities

a) Cybersecurity requirements should be defined as early as possible in the I&C programmable digital system lifecycle.

b) Potential dependencies, conflicts or reinforcements between safety requirements and cybersecurity requirements should be detected, documented and taken into account to ensure the definition of an integrated solution meeting both the safety and security goals.

6.3.3 Design activities

a) I&C systems should be designed in order to favour reinforcements between safety and cybersecurity features. Related design choices regarding such reinforcements should take into account a trade-off analysis between:

- the gains and drawbacks related to the verification and validation of the systems;
- the gains and drawbacks in terms of system complexity and interfaces.

b) Any system feature initially designed for safety reason which has a potential value as a cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined taking into account context-relevant cyberattacks, by staff responsible for cybersecurity, to confirm its cybersecurity effectiveness.

c) The security features of programmable digital systems important to safety should be designed to limit their dependency on updates.

6.3.4 Implementation activities

This document does not provide any specific requirements or recommendations related to the coordination between safety and cybersecurity for this phase. Refer to IEC 62645 for cybersecurity-related ones, to IEC 60880 and IEC 62138 for software of CB I&C systems supporting functions important to safety, and to IEC 62566 for HDL-programmed integrated circuits for systems performing category A functions.

6.3.5 Verification and validation activities

a) Software code review or analysis of I&C programmable digital systems conducted for safety reasons (see IEC 60880 and IEC 62138 for software of systems performing functions important to safety) may also consider cybersecurity aspects and vulnerabilities associated with unsecure coding practices.

NOTE 1 Skills and tools needed for safety-oriented code review or analysis, and those needed for security-oriented code review or analysis are often overlapping, however, they are different. The optimal level of integration of these activities is highly dependent on the context.

b) Appropriate cybersecurity measures should be taken to protect sensitive data or information associated to software code review and analysis.

c) Software and hardware should be verified and validated in order to avoid unapproved functionalities. This may be required from a safety perspective (as per the applicable standards), but also from a cybersecurity perspective in some cases.

NOTE 2 During inspections made for hardware verification and validation, wireless capabilities or undeclared programmable digital components can be detected.

6.3.6 Installation and acceptance testing activities

a) Security tests should be conducted in a test environment representative of the installed system.

6.3.7 Operations and maintenance activities

a) Off-line maintenance periods should be considered as opportunities for software security updates, if compatible with respect to qualification constraints.

b) Periodic testing of functions important to safety shall not degrade cybersecurity of the involved I&C systems.

c) Cybersecurity verifications may be considered for integration in safety periodic testing.

NOTE Such integrations are subject to restrictions: see 6.2 g) and 6.2 h).

d) Intrusive security testing, including penetration testing, shall not be conducted directly on systems important to safety during operations. A test lab should be available.

6.3.8 Change management

a) There shall be procedures to assess and manage the potential for adverse safety and cybersecurity interactions that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures.

b) There should be procedures to identify and leverage potential mutual reinforcements between safety and cybersecurity that may result from changes to an I&C programmable digital system, including to its configuration, status or to its related procedures.

c) A change driven by safety considerations should be reviewed by staff responsible for cybersecurity.

d) A change driven by cybersecurity considerations should be reviewed by staff responsible for safety.

6.3.9 Decommissioning activities

a) As-built information, including system actual interfaces, should be available and analysed before starting decommissioning individual I&C systems to ensure that the overall cybersecurity and safety objectives of the plant are not compromised by the decommissioning of the system, or by the related steps of the process.

b) In particular, when decommissioning of individual I&C systems leads to temporary provisions in order to maintain the safe operations of the plant, those provisions may induce new cybersecurity issues which should be analysed and addressed if deemed relevant by this analysis.

6.4 Selected technical aspects of I&C systems constrained by safety and cybersecurity

6.4.1 General

The objective of 6.4.2 to 6.4.6 is to provide guidance or requirements on some aspects of I&C programmable digital system design and operation, when they are subject to both safety and cybersecurity constraints. They deal with common situations where safety and cybersecurity technical measures or requirements conflict, depend or reinforce each others. Potential confusion between safety and cybersecurity measures is also addressed.

6.4.2 Logical access control for HMIs of I&C programmable digital systems in control rooms

a) Password-based logical access control for the operators shall not be implemented on HMIs of I&C programmable digital systems which need immediate operator access for plant safety. Alternative access control measures, acceptable from a safety point of view, should be implemented.

NOTE Possible alternative access control measures include permission to physically access the control rooms based on a rigorous screening of personnel, access limitation to operational HMI software (e.g., to BIOS or to the operating system level), software with restricted input (e.g. only from predefined lists). Such alternative access control measures are of particular importance for control rooms which are not permanently staffed (e.g. remote shutdown station).

b) Account/node locking or delayed login after invalid access attempts should not be implemented for I&C programmable digital systems which need immediate operator access for plant safety. Alternative measures, acceptable from a safety point of view, should be implemented.

c) The management of access controls shall take account of specific operational needs with safety implications (e.g., maintenance during night shifts, beyond design basis conditions, nuclear emergencies).

Note that requirements of 6.4.2 are valid for I&C programmable digital systems, not for their maintenance digital tools.

6.4.3 Software modification

6.4.3.1 Cybersecurity-driven software modifications

a) Cybersecurity-driven software modifications (including the application of a software security update) are a type of software modifications and shall be treated accordingly, i.e. in accordance with Clause 11 of IEC 60880:2006 for software of I&C CB systems supporting category A functions, in accordance with 5.10 and 6.10 of IEC 62138:2004 for software of I&C CB systems supporting category B or C functions, and in accordance with relevant local procedures for I&C programmable digital systems not important to safety.

b) The decision to implement a cybersecurity-driven software modification shall be validated by personnel knowledgeable of the targeted systems, their usage and their safety implications, in conjunction with those who are accountable for those systems.

c) Tests shall be conducted to validate that a cybersecurity-driven software modification (including the application of a software security update) does not degrade system ability to ensure its functions important to safety.

d) When it is decided not to apply a software security update, whatever the reason (e.g., tests as per c) or because the change is not possible during operations):

- the vulnerability associated with this non-application shall be traced and managed with the appropriate level of confidentiality;
- a dedicated risk analysis shall characterise the risks associated with this decision;

– if the risk analysis identifies the need for compensating cybersecurity measures, their implementation shall be approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems.

6.4.3.2 Other software modifications

a) Analyses or tests shall be conducted to validate that a software modification, made for safety or other reasons not related to cybersecurity (e.g. reliability, new functionality), does not result in inadequate cybersecurity.

b) Any software modification identified as degrading cybersecurity shall not be implemented on plant I&C systems unless the four following conditions are met:

– a dedicated risk analysis has been conducted to identify the risk;

– compensating cybersecurity measures potentially identified by the risk analysis have been approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems;

– any approved compensating cybersecurity measures have been implemented;

– the remaining residual risk is approved by the relevant persons accountable for cybersecurity in conjunction with the persons accountable for the involved systems.

6.4.4 Logging and audit capability

a) Local record generation, audit reduction and report generation capability intended for cybersecurity should be implemented as much as possible external to systems important to safety.

b) The failure messages generated by a programmable digital I&C equipment should be logged outside this equipment to support safety or cybersecurity analyses.

c) Any logical connectivity implemented to centrally manage systems and/or cybersecurity logs should not interfere with independence requirements imposed upon systems important to safety.

NOTE Among the different possible approaches, strictly unidirectional channels to push logs are beneficial both from a security and safety point of view.

d) Logging mechanisms should be preferably implemented and pre-configured so that no logging management (e.g., level of detail, selectivity of logged events) is needed during plant operation.

6.4.5 Use of cryptography by I&C systems

a) Cryptographic mechanisms may be used by I&C programmable digital systems, but they shall not adversely impact the required performance (including response time), effectiveness, reliability or operation of functions important to safety.

b) For systems important to safety, cryptographic mechanisms aimed at ensuring confidentiality should only be used when justified by a cybersecurity risk analysis.

NOTE 1 I&C environments are usually resource-constrained whereas cryptography is resource-consuming. Integrity and availability are usually more important than confidentiality in I&C environment. Moreover, the use of confidentiality-focused mechanisms involves additional complexity, latency, and potential failures which are antagonistic with safety. Of course, specific contexts and risk analysis results can involve confidentiality needs and lead to the implementation of confidentiality-focused mechanisms. Moreover, I&C related information involves in some cases security classification and use of such confidentiality mechanisms.

c) In the case of I&C systems needed for the real-time management of beyond design basis conditions and nuclear safety emergencies, confidentiality-focused mechanisms should only be used when they can be fully justified.

d) Any communication or data integrity control initially designed for safety or reliability purposes and later considered as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined by staff responsible for cybersecurity, taking into account context-relevant cyberattacks, to confirm its cybersecurity effectiveness.

NOTE 2 As an illustration, the effectiveness of integrity control mechanisms differs largely depending on the nature of the threats: a classical CRC (Cyclic Redundancy Check) code is appropriate with regards to random failures whereas it is inefficient against an attacker, who is able to change the data and recompute the CRC to

make the new data considered as valid. Integrity control or assurance mechanisms specifically tailored for cybersecurity would detect the modification in this case.

6.4.6 System availability and function continuity

a) Any control initially designed to protect availability of a system from a safety or reliability perspective and later considered as a potential cybersecurity counter-measure (during cybersecurity risk analysis activity for instance) should be re-examined by staff responsible for cybersecurity, taking into account context-relevant cyberattacks, to confirm its cybersecurity effectiveness.

NOTE Availability mechanisms tailored to address non-malicious failures are in some cases completely inefficient against malicious threats. Redundant but non-diversified systems are generally of little help against a cyberattack, as the redundant system will be vulnerable to the same attack.

b) Redundancy and back-up of safety-related data (e.g. configuration, parameters) or of components may be considered as cybersecurity counter-measures only when explicit justifications of their efficiency with respect to the considered malevolent threats are given.

7 Organizational and operational issues

7.1 Governance and responsibilities

a) Both cybersecurity and safety should be represented at the senior management or board level of the organization.

7.2 Coordination between safety and cybersecurity staff during operations

a) For each I&C programmable digital system, all personnel liable to access the system for cybersecurity or safety reasons should be identified. When different staffs, including safety staff and cybersecurity staff, are to access the system, these accesses should be coordinated and the schedules for each optimised.

b) Interventions on I&C programmable digital systems should be authorized both from a cybersecurity point of view and from a safety point of view.

c) Those entities responsible for safety and cybersecurity shall put adequate controls in place to ensure that sub-contractor staff who are granted access to I&C programmable digital systems to perform specific tasks are adequately controlled. In some instances, this may require such staff to be accompanied by a responsible and knowledgeable representative of the system's owner.

d) When a cybersecurity event is detected on a system important to safety, safety impact and cybersecurity impact analyses shall be made.

7.3 Safety and cybersecurity culture

a) Awareness and demonstration activities on I&C programmable digital system cybersecurity threats should be organized for I&C safety staff, in order to help them understand the existence and the nature of such threats and the potential impacts on safety.

b) Reciprocally, staff in charge of cybersecurity should be trained on main safety concepts and associated principles.

c) Opportunities for I&C operators, I&C maintenance staff, safety staff and cybersecurity staff to come together and exchange information about their roles, their practices, their environments and the associated threats should be provided.

NOTE This sort of opportunities is potentially beneficial for cybersecurity threat assessment activities. However, information classification issues are likely to occur; their resolution in a balanced way is a condition to obtain the maximum benefit from such practices.

7.4 Emergency response management

a) Procedures and organisations shall be in place in order to evaluate rapidly and rigorously safety implications of cybersecurity attacks on I&C programmable digital systems.

b) Any cybersecurity response decided in a cybersecurity crisis management context shall be evaluated in terms of safety impact before enforcement.

c) Potential cybersecurity implications of safety events and related response associated to I&C programmable digital systems should be evaluated and managed. Safety shall however remain the priority.

d) Integrated emergency exercise combining both safety and cybersecurity issues should be organized in order to challenge and enhance collaboration between staffs in charge of I&C systems, those in charge of plant safety, and those in charge of cybersecurity (where separated).

e) I&C programmable digital system isolation features and procedures, established for cybersecurity purposes, shall be analyzed in terms of safety consequences before allowance for enforcement.

Annex A
(informative)

Rationale for, and notes related to, the scope of this document

A.1 General

This annex presents the reasons and rationale which have lead to the scope defined in Clause 1.

A.2 Inclusion of I&C programmable digital system not important to safety

This document being focused on the coordination between safety and cybersecurity, a narrower scope, strictly limited to systems important to safety, has been initially considered. The experts involved in the document development have finally decided to include in the scope I&C programmable digital systems not important to safety because:

– it is consistent with the scope of the IEC 62645, to which this document is affiliated;
– assessing the impacts of cyberattacks, including in terms of plant safety, involves a global perspective (for instance, a targeted cyberattack on configuration or maintenance tools can lead to consequences on safety, although these tools can be classified as not important to safety).

The issue of coordinating safety and cybersecurity is better addressed by considering both I&C programmable digital systems important to safety and those not important to safety.

A.3 Exclusion of physical security, room access control and site security surveillance systems

This exclusion is inherited from and consistent with IEC 62645. However, it does not deny that cybersecurity has clear dependencies on the security of the physical environment (e.g., physical protection, power, heating/ventilation/air-conditioning systems, etc.). It is recognized that efficient I&C programmable digital system cybersecurity can only be achieved based on a sound physical security and physical protection regime, complying with national laws and regulations. From an international perspective, the IAEA provides relevant guidance.

A.4 Exclusion of non-malevolent actions and events

In consistence with IEC 62645, cybersecurity relates to prevention of, detection of, and reaction to malicious acts by digital means (cyberattacks) on I&C programmable digital systems. It does not cover considerations related to non-malevolent actions and events such as accidental failures, natural events, or human errors (except for those degrading cybersecurity). Although such aspects are sometimes included in other normative contexts (e.g., in the ISO/IEC 27000 series, the IEC 62443 series or the NIST framework), these exclusions and the focus on the protection against cyberattacks have been decided to provide the maximum consistency and the minimum overlap with the existing nuclear standards and practices. If aspects such as accidental failures, human errors and natural events are of course of prime importance, they are already covered by other SC 45A documents and standards, and are not considered as cybersecurity related in this document (except for human errors degrading cybersecurity).

A.5 Exclusion of development tools and platforms

This document is limited to I&C programmable digital systems used in NPPs, including on-site maintenance and configuration tools. It does not apply directly to development tools and platforms, typically found at the supplier premises. However, development tools and platforms might be impacted by the present document, in order to make the developed I&C systems and architectures meet its requirements. This exclusion does not deny the importance of securing development tools and platforms from a global cybersecurity perspective; it reflects the fact that this document has not been particularly developed to treat these aspects, which deserve due care but are to be treated mostly by non-nuclear specific provisions.

Bibliography

Nuclear I&C system specific references

MDEP, Common Position No. DICWG08, *Common position on the impact of cyber security features on digital I&C safety systems*

IAEA, Nuclear Security Series No. 17, Reference Manual, *Computer security at nuclear facilities*

ORNL, report ref. ORNL/NRC/LTR-07/05, *Safety and non-safety communications and interactions in international nuclear power plants*, 2007

U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, *Cyber security programs for nuclear facilities*, January 2010

U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, Rev. 3, 2011

IEEE, Std 7-4.3.2-2010, *Standard criteria for digital computers in safety systems of nuclear power generating stations*

CSA N290.7 Standard, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities*, 2014

IAEA Safety Guide SSG-39, *Design of instrumentation and control systems in Nuclear Power Plants*

Interface between nuclear safety and nuclear security

IAEA, INSAG-24, *The interface between safety and security at nuclear power plants*

U.S. Nuclear Regulatory Commission, RG 5.74, *Managing the safety-security interface*

WINS, *An integrated approach to nuclear safety and nuclear security*, Rev. 1-1

Non-nuclear I&C system specific references

ISA TR84.00.09-2013, *Security protection layers and considerations related to SIS*

IEC 62443 (all parts), *Security for industrial automation and control systems*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

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

Non I&C-specific IAEA references

IAEA, GS-R-3:2006, *The management system for facilities and activities*

IAEA, Safety Guide No, GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA, Safety Guide No, GS-G-3.5:2009, *Management system for nuclear installations*

IAEA, Safety Standard Series No. SSR-2/1:2012, *Safety of Nuclear Power Plant: Design*

IAEA, Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants*

IAEA, Safety Guide SSG-34, *Design of electrical power systems in Nuclear Power Plants*

IAEA, Safety Glossary, *Terminology used in nuclear safety and radiation protection*

SOMMAIRE

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.

Cette version consolidée de la Norme IEC officielle et de son amendement a été préparée pour la commodité de l'utilisateur.

L'IEC 62859 édition 1.1 contient la première édition (2016-10) [documents 45A/1104/FDIS et 45A/1118/RVD] et son amendement 1 (2019-10) [documents 45A/1279/FDIS et 45A/1286/RVD].

Cette version Finale ne montre pas les modifications apportées au contenu technique par l'amendement 1. Une version Redline montrant toutes les modifications est disponible dans cette publication.

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.

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

Le comité a décidé que le contenu de la publication de base et de son amendement 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.