IEC 62645

Edition 2.0 2019-11

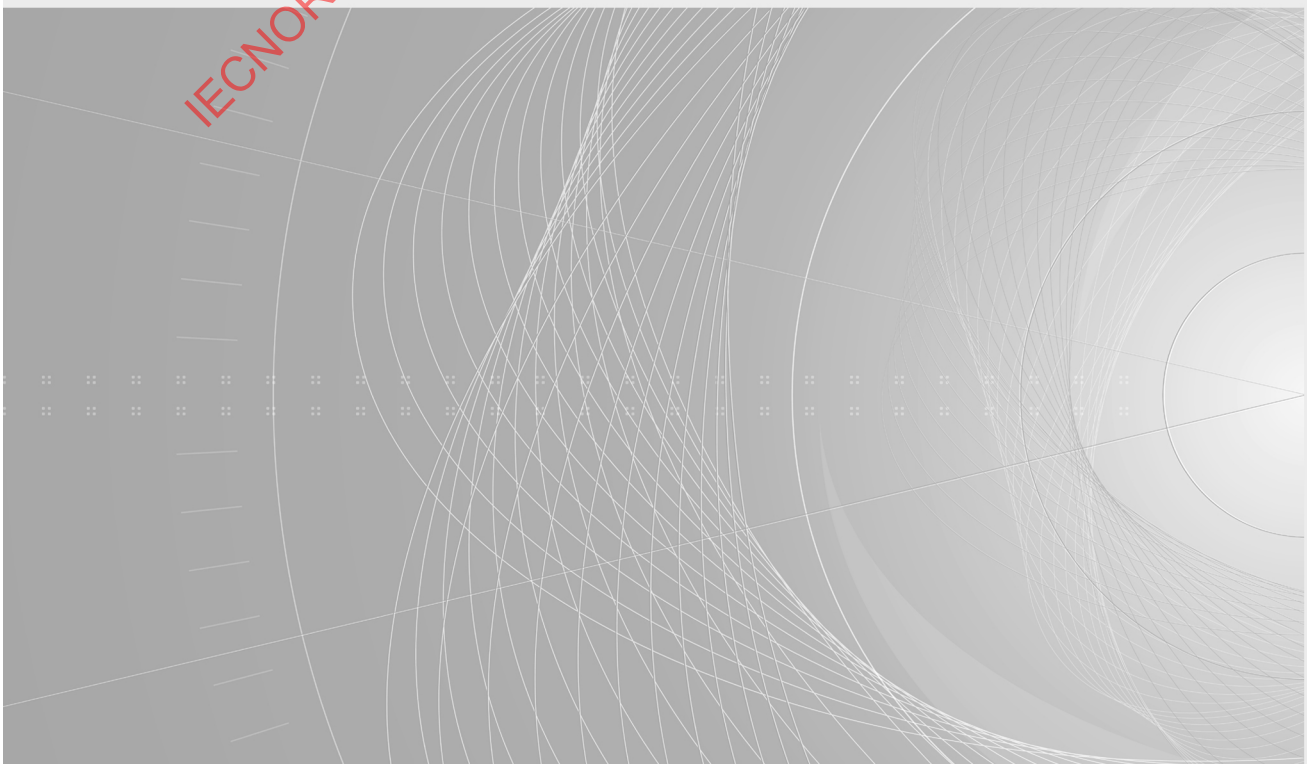
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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



IEC 62645:2019-11(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 62645

Edition 2.0 2019-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-7548-1

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 9
1.1 General 9
1.2 Application 10
1.3 Framework 10
2 Normative references 12
3 Terms and definitions 12
4 Abbreviated terms 17
5 Establishing and managing a nuclear I&C programmable digital system security programme 17
5.1 Context of the organization 17
5.1.1 Understanding the organization and its context 17
5.1.2 Understanding the needs and expectations of interested parties 17
5.1.3 Determining the scope of the I&C programmable digital system security programme 17
5.2 Programme, policy and plan 18
5.2.1 I&C digital programmable system security program 18
5.2.2 Policy 18
5.2.3 Plan 19
5.3 Leadership 19
5.3.1 Leadership and commitment 19
5.3.2 Roles, responsibilities and authorities 19
5.4 Planning of the programme 20
5.4.1 Cybersecurity objectives and planning to achieve them 20
5.4.2 Addressing risks and opportunities of the programme 20
5.4.3 Graded approach to I&C security and risk assessment 21
5.5 Support 28
5.5.1 Resources 28
5.5.2 Training, competence and awareness 28
5.5.3 Communications about cybersecurity 29
5.5.4 Documented information 29
5.6 Operation 29
5.6.1 Operation planning and control 29
5.6.2 Cybersecurity graded approach, risk assessment and risk treatment 30
5.7 Performance evaluation 30
5.7.1 Monitoring, measurement, analysis and evaluation 30
5.7.2 Internal audit 30
5.7.3 Management review 30
5.8 Improvement 31
5.8.1 General 31
5.8.2 Nonconformity and corrective action 31
5.8.3 Continual improvement 31
6 Life-cycle implementation for I&C programmable digital system security 31
6.1 General 31
6.2 System requirements specification 31

6.2.1 General 31
6.2.2 Security degree assignment 32
6.3 System specification 32
6.3.1 Selection of pre-existing components 32
6.3.2 System architecture 32
6.4 System detailed design and implementation 32
6.4.1 General 32
6.4.2 Risk assessment at the design phase 33
6.4.3 Design project security plan 33
6.4.4 Communication pathways 33
6.4.5 Security zone definition 34
6.4.6 Security assessment of the final design 34
6.4.7 Implementation activities 34
6.5 System integration 34
6.6 System validation 34
6.7 System installation 35
6.8 Operation and maintenance activities 35
6.8.1 Change control during operations and maintenance 35
6.8.2 Periodic reassessment of risks and security controls 35
6.8.3 Change management 35
6.9 Retirement activities 36
7 Security controls 36
7.1 General 36
7.2 Characterization 36
7.3 Security defence-in-depth 37
7.4 Selection and enforcement of cybersecurity controls 37
Annex A (informative) Rationale for, and notes related to, the scope of this document 38
A.1 Objective of this annex 38
A.2 Inclusion of I&C programmable digital system not important to safety 38
A.3 Exclusion of site physical security, room access control and site security surveillance systems 38
A.4 Exclusion of non-malevolent actions and events 38
A.5 Development tools and platforms 38
Annex B (informative) Generic considerations about the security degrees 39
B.1 Rationale for three security degrees 39
B.1.1 General 39
B.1.2 Safety categories as input to security degree assignment 39
B.1.3 Impact on plant availability and performance as input to security degree 39
B.1.4 Resulting security degree assignment approach 40
B.2 Considerations about tools associated to on-line systems 40
B.3 Practical design and implementation 40
Annex C (informative) Correspondence with ISO/IEC 27001:2013 41
Annex D (informative) Overall organisation of IEC SC 45A standards related to cybersecurity 43
Annex E (informative) Selection of security controls 45
Annex F (informative) Considerations about IEC 62645 applicability to non-NPP nuclear facilities 47
F.1 Applicability of IEC 62645 security graded approach to Research Reactors 47
F.1.1 General 47

F.1.2 Categorization of RRs in accordance with potential hazards 47
F.1.3 Safety categories as input to security degree assignment 48
F.1.4 Impact on operational capacity as input to security degree 49
F.1.5 Considerations on requirements associated to security degrees 49
F.2 Applicability of IEC 62645 security graded approach to fuel cycle facilities 49
F.3 Applicability of IEC 62645 security graded approach to SMR 49
F.4 Reference documents 50
Annex G (informative) High-level correspondence table between IEC 62443 series and IEC 62645 51
Bibliography 53

Figure 1 – Overall framework of IEC 62645 11
Figure 2 – E/E/PE items 14
Figure D.1 – Overview of IEC SC 45A standards with cybersecurity relation 44
Figure E.1 – Selection of security controls 46

Table C.1 – Correspondence between ISO/IEC 27001:2013 and IEC 62645 41
Table F.1 – Correspondence between safety categories and classes as per IEC 61513 48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

FOREWORD

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

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

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

c) Recommendations and limitations regarding the application of this standard

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

It is recognized that this standard addresses an evolving area of regulatory requirements, due to the changing and evolving nature of computer security threats. Therefore, the standard defines a framework within which the evolving country specific requirements may be developed and applied.

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

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

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

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

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

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

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

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

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

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

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

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

1 Scope

1.1 General

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

This document defines adequate measures for the prevention of, detection of and reaction to malicious acts by digital means (cyberattacks) on I&C programmable digital systems. This includes any unsafe situation, equipment damage or plant performance degradation that could result from such an act, such as:

– malicious modifications affecting system integrity;

– malicious interference with information, data or resources that could compromise the delivery of or performance of the required I&C programmable digital functions;

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2 Application

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

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

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

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

1.3 Framework

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

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

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

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

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

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

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

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

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

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

Figure 1 presents the overall framework of this document.

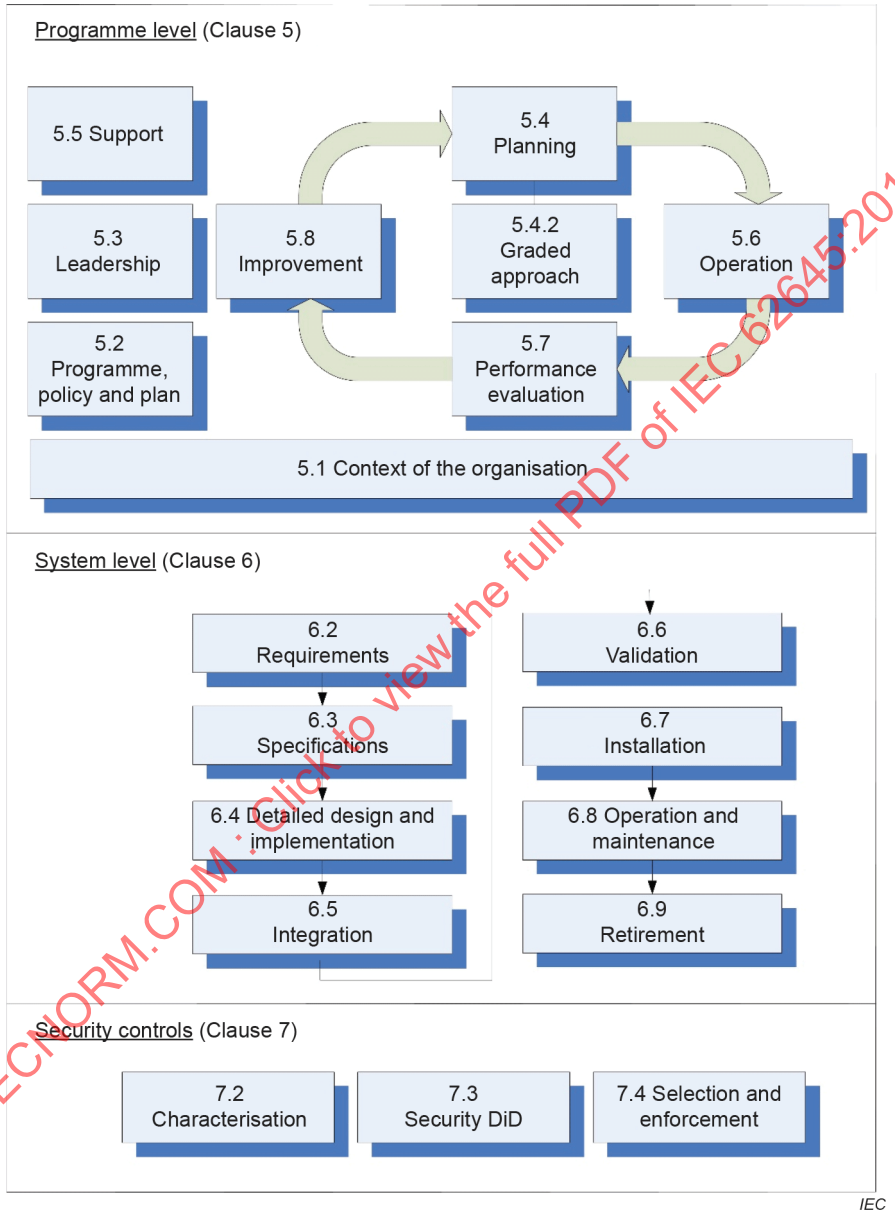


Figure 1 – Overall framework of IEC 62645

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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
attack vector
path or means by which an attacker or malicious program can gain access to a computer-based system

3.2
authorization
function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular

3.3
availability
property of being accessible and usable upon demand by an authorized entity

Note 1 to entry: This definition is different from the one used in the other IEC standards in the field of instrumentation and control of nuclear facilities which is “ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided”.

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.4
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.

[SOURCE: IEC 62138: 2018, 3.8]

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.6
cyberattack
malicious acts by digital means

3.7
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

– 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;

– 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

Note 1 to entry: This definition is tailored with respect to the IEC 62645 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 for more detail about such exclusions.

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

3.8
design
the process and the result of developing a concept, detailed plans, supporting calculations and specifications for a facility and its parts

[SOURCE: IAEA Safety glossary, 2007 edition]

3.9
Design Basis Threat
DBT
attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated

Note 1 to entry: Cyberattacks and related adversaries are not considered, in an equivalent manner in DBTs; this depends on each national approach and legal framework. Moreover, the content of a nuclear DBT is treated as highly confidential.

[SOURCE: IAEA INFCIRC/225/Rev.4:1999, modified: note 1 added]

3.10
Electrical/Electronic/Programmable Electronic item
E/E/PE item
item based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

Note 1 to entry: In this term and its definitions, the word “item” can be replaced by the words: system or equipment or device.

Note 2 to entry: The definitions of the terms related to the technology: E/E/PE item, programmable digital item, computer-based item, hardwired item, programmable logic item are totally consistent and coherent. The relationships between the terms E/E/PE item, hardwired item, programmable digital item, computer-based item, programmable logic item are given by Figure 2.

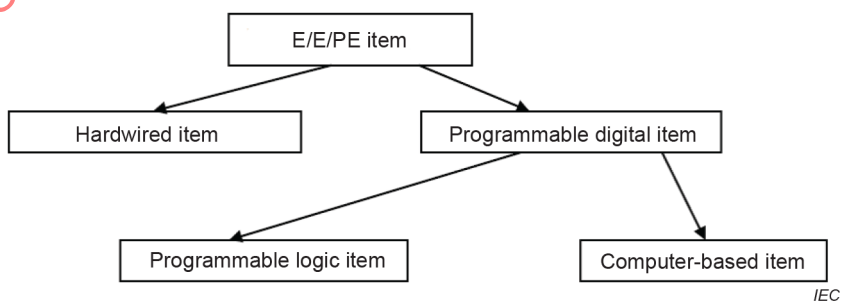


Figure 2 – E/E/PE items

[SOURCE: IEC 62138: 2018, 3.15]

3.11
HDL-Programmed Device
HPD
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 micro-electronic technologies.

Note 4 to entry: HPD is a kind of programmable logic item.

Note 5 to entry: See also the definition of E/E/PE item and the associated notes.

[SOURCE: IEC 62566: 2012, 3.7]

3.12
I&C function
function to control, operate and/or monitor a defined part of the process

[SOURCE: IEC 61513:2011, 3.28]

3.13
I&C system
system, based on E/E/PE items, performing plant I&C functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: See also “electrical power system”. The terms “electrical power system” and “I&C system” are terms related to the main functions the systems perform; respectively “electrical power generation, transmission and distribution” and “measurement, protection, control and HMI related to the NPP process”. They have to be considered in conjunction and are totally consistent and coherent with the general requirements established by IEC 61513 and IEC 63046 for instrumentation, control and electrical power systems for nuclear power plants.

Note 4 to entry: See also the definition of E/E/PE item and the associated notes.

Note 5 to entry: According to their typical functionality, IAEA distinguishes between automation / control systems, HMI systems, interlock systems and protection systems.

[SOURCE: IEC 62138: 2018, 3.26]

3.14
integrity
the property of protecting the accuracy and completeness of assets

[SOURCE: IAEA Nuclear Security Series No. 17:2011 and ISO/IEC 27000:2018, 2.40]

3.15
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment or device.

Note 2 to entry: See also the definition of E/E/PE item and the associated notes.

Note 3 to entry: The main kinds of programmable digital items are computer-based items and programmable logic items.

Note 4 to entry: This term used by IEC SC 45A is equivalent to programmable electronic item (PE item) defined accordingly to IEC 61508.

[SOURCE: IEC 62138:2018, 3.35]

3.16
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.17
risk assessment
overall process of systematically identifying, estimating, analysing and evaluating risk

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.18
security controls
means of managing security which can be technical, physical, or administrative

3.19
security degree
gradation of security protection with associated sets of requirements, assigned to a system according to the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance

Note 1 to entry: Subclause 5.2.3 of this document defines three security degrees which correspond to S1, S2 and S3. The rationale behind the use of three security degrees for I&C programmable digital systems is provided in Annex B. This document only deals with I&C programmable digital systems and does not make any assumptions on security degrees for other kinds of systems. Non-I&C systems (for instance office computers) might be assigned to supplemental/different security degrees, leading to a graded approach with more than 3 security degrees from a global plant perspective. Moreover, some national practices involve subdivision of security degree.

Note 2 to entry: The term “security degree” has been preferred to “security level” in order to avoid possible confusion with the concept of I&C levels, commonly found in other standards and industry practices.

3.20
security programme
set of interrelated or interacting elements of an organization to establish security policies and objectives, as well as processes and security plans to achieve those objectives

Note 1 to entry: Programme is a concept similar to “management system” as defined in ISO/IEC 27000:2018.

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

3.21
security zone
concept for grouping computer-based I&C systems for administration, communication and application of protective measures

Note 1 to entry: Security zones are practical and architectural implementations of a graded approach. They are not limited in number. They can be logical and/or physical. There is no direct correspondence with the concept of safety zones and the associated geographical separations.

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.22
threat
potential cause of an unwanted incident, which may result in harm to a system or organization

Note 1 to entry: In the frame of this document (see 1.1), the considered events or occurrences are limited to malicious ones and to human errors degrading cybersecurity – not to include accidental aspects (e.g., natural hazards, human errors not impacting cybersecurity), treated by other IEC documents in the field of instrumentation and control of nuclear facilities.

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

3.23
vulnerability
weakness of an asset or a security control that can be exploited by a threat

[SOURCE: IAEA Nuclear Security Series No. 17:2011]

4 Abbreviated terms

CB	Computer-Based
CERT	Computer Emergency Response Team
CSSO	Computer System Security Officer
DBT	Design Basis Threat
HDL	Hardware Description Language
HVAC	Heating, Ventilation and Air-Conditioning
ISMS	Information Security Management System
I&C	Instrumentation and Control
NPP	Nuclear Power Plant
PLC	Programmable Logic Controller
PSP	Project Security Plan
QA	Quality Assurance
V&V	Verification & Validation

5 Establishing and managing a nuclear I&C programmable digital system security programme

5.1 Context of the organization

5.1.1 Understanding the organization and its context

The content of ISO/IEC 27001:2013, 4.1 applies.

5.1.2 Understanding the needs and expectations of interested parties

The content of ISO/IEC 27001:2013, 4.2 applies.

5.1.3 Determining the scope of the I&C programmable digital system security programme

The content of ISO/IEC 27001:2013, 4.3 applies.

In particular, the scope and boundaries of the security programme shall be defined in terms of the characteristics of the nuclear power plant's organization, its location, national regulatory requirements, I&C programmable digital assets and technology, and risk of system

exploitation. It shall include details of and justification for exclusions/modifications from the scope.

5.2 Programme, policy and plan

5.2.1 I&C digital programmable system security program

5.2.1.1 The content of ISO/IEC 27001:2013, 4.4 applies.

5.2.1.2 The I&C security programme shall be developed based on risk assessment and take into account the policy and guidance established by the designer, country regulatory authority and existing plant specific policies and procedures to implement the security programme.

5.2.1.3 Security programmes shall be implemented through the use of documented policies and procedures approved by the personnel that are in charge of the security programmes.

5.2.1.4 A proper coordination between safety and cybersecurity aspects shall be ensured. Requirements and recommendations can be found in IEC 62859.

5.2.1.5 An I&C programmable digital systems security programme of a NPP shall contain the following activities:

a) definition of the computer security organization and responsibilities and the process of periodic reviews;

b) development of the process of designating assets subject to computer security protective measures including computer systems, computer system applications and network connections;

c) implementation of methods of personnel management in computer security and I&C programmable digital system security including training, qualification and termination/transfer;

d) development and performance of the process for risk assessment, taking into account the country specific design basis threat (DBT) as applicable, for the complete I&C architecture as well as for every I&C system;

e) performance of an assessment of the residual risk that is transferred/accepted from design to operation;

f) definition of the fundamental architecture and design principles and requirements for system security design and configuration management for plant systems and vendor support required to maintain the cybersecurity features incorporated in the design;

g) identification of operational security procedures for access control, data security, communication security, platform and application security, system monitoring, computer system security maintenance and modification and security incident handling;

h) in particular, definition of a process for assessment of off-the-shelf components, both hardware and software to ensure as far as reasonably possible that they are free from malicious software or functionality;

i) establishment of security requirements for the preparation and formalization of deliveries of hardware, data, software, code or information between different sites of the designers, or between a designer and a third party, or between the designer and the utility.

5.2.2 Policy

5.2.2.1 The content of ISO/IEC 27001:2013, 5.2 applies.

5.2.2.2 A computer security policy shall set the high-level computer security goals applicable for a nuclear facility.

5.2.2.3 I&C programmable digital system security policy requirements shall be factored into lower level documents, which will be used to implement and control policy.

5.2.2.4 These requirements shall be:

a) measurable,

b) enforceable,

c) and achievable.

5.2.3 Plan

The I&C programmable digital system security plan shall:

a) be the implementation of that policy in the form of organizational roles, responsibilities and procedures,

b) specify and detail the means for achieving the security goals,

c) contain the primary actions to be taken and the associated response in terms of intrusion detection and prevention, assessment of consequences, and the countermeasures necessary to mitigate consequences.

5.3 Leadership

5.3.1 Leadership and commitment

The content of ISO/IEC 27001:2013, 5.1 applies.

5.3.2 Roles, responsibilities and authorities

5.3.2.1 The first requirement of ISO/IEC 27001:2013, 5.3 applies.

5.3.2.2 The second requirement of ISO/IEC 27001:2013, 5.3 applies.

5.3.2.3 Management of the I&C programmable digital system programme shall ensure that all necessary computer security issues are addressed programmatically within the computer security plan and procedures, and that they meet regulatory and corporate requirements.

5.3.2.4 The I&C programmable digital system programme shall be coordinated with the corporate security programme and the current site's framework of policies, programmes, practices and procedures, as applicable.

5.3.2.5 The implementation of a permanent I&C programmable digital system security programme shall be integrated or closely interfaced with I&C system specialists, computer security specialists and physical security specialists.

5.3.2.6 During the design and development phase, different companies are likely to be responsible for developing different I&C systems. The designer shall clearly specify I&C supplier obligations with respect to computer security, and shall verify that they are respected.

5.3.2.7 All organisations involved in any portion of the life cycle of I&C programmable digital systems development shall document the organizational structure and associated responsibilities for each position that support the computer security programme for those systems. Communication procedures shall be documented between all involved organizations (particularly different legal entities), and also teams within an organization or company.

5.3.2.8 In order to develop, approve and implement an I&C programmable digital system security programme, plant management in cooperation with the I&C designer shall consider:

a) utility corporate security requirements;

b) internal corporate security policy;

c) national legislative material;

d) national regulatory material;

e) computer and I&C programmable digital system security industry best practices;

f) current and projected threat status in the nuclear industry and in other industries using I&C equipment used in nuclear plants;

g) to establish information channels concerning continuous update on current and projected threat status in the nuclear industry and in other industries using I&C equipment used in nuclear plants.

5.3.2.9 I&C programmable digital system security oversight shall be assigned to specific person(s)/position(s) in the organization or project with precisely defined responsibilities. This document refers to the role of Computer System Security Officer(s) (CSSO), or equivalent. The responsibilities of the CSSO shall include:

a) advise the company's and/or project's management;

b) coordinate and control the development of the computer security activities;

c) coordinate computer security with other security and safety disciplines;

d) ensure that the computer security programme takes into account plant operation or maintenance and does not inadvertently affect the systems important to safety;

e) identify and document the systems that are critical to maintaining computer security within a facility;

f) conduct computer security risk assessments;

g) conduct periodic security inspections, audits and reviews, and provide status reports to top level management;

h) develop and implement computer security training and evaluation;

i) develop a strategy, including training aspects and procedures, to identify potential cybersecurity incidents;

j) develop and lead or contribute to the response for relevant computer security events including coordination with relevant internal and external organizations;

k) investigate computer security incidents or identified vulnerabilities and recommend corrective actions.

5.3.2.10 Additional responsibilities of a CSSO may be added to the above list, which are specific to the organization of the company. A dedicated and/or multi-disciplined team, with the required resources and expertise should support the execution of these responsibilities.

5.4 Planning of the programme

5.4.1 Cybersecurity objectives and planning to achieve them

5.4.1.1 The content of ISO/IEC 27001:2013, 6.2 applies.

5.4.1.2 Cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realisation.

5.4.2 Addressing risks and opportunities of the programme

The content of ISO/IEC 27001:2013, 6.1.1 applies.

5.4.3 Graded approach to I&C security and risk assessment

5.4.3.1 Classification scheme

5.4.3.1.1 General

5.4.3.1.1.1 I&C programmable digital system security shall be based on a graded approach: all I&C programmable digital systems shall be assigned to security degrees. The security degree of a I&C programmable digital system shall be assigned based on the maximum consequences of a successful cyberattack on this system in terms of plant safety and performance (see 5.4.3.1.3 for detailed assignment criteria). Graded security requirements are defined for each security degree (in 5.4.3.2.4 to 5.4.3.2.8).

NOTE In the context of this document, plant performance is understood from a power generation perspective.

5.4.3.1.1.2 The classification scheme is based on the following principles:

a) consequences of cyberattack regarding safety shall be assumed as more serious than those regarding plant performance;

b) systems shall be considered from a functional point of view and assigned to a given security degree according to their possible direct or indirect impact on plant safety and performance. The security degree of a system is assigned based on the most sensitive function (i.e. the one which leads to the most severe impacts when maliciously manipulated or disrupted) it implements;

c) such a consequence-based assignment approach shall be rigorous and repeatable, ensuring reproducibility and consistency of the security posture. This analysis shall include the possibility that other I&C systems are subject to the same attack (e.g. similar systems in separate redundancies).

5.4.3.1.1.3 Security degree assignment should be made as early as possible in the I&C system life-cycle.

5.4.3.1.1.4 Security degree assignment shall be documented.

5.4.3.1.1.5 A graded approach to security as per this document involves that:

a) the number of interfaces between systems assigned to different security degrees shall be justified;

b) appropriate restrictions shall be enforced to interfaces between systems of different security degrees.

5.4.3.1.1.6 Risk assessment, including vulnerability assessment and threat scenario identification, shall complete the analysis and may lead to complementing the security requirements and security measures (see 5.4.3.2.2).

5.4.3.1.2 Link between safety categories, safety classes and security degrees

The security graded approach described in this document aims at defending the plant safety and performance against cyber threats, built on a consequence-based analysis.

The part related to safety-oriented consequences of such an analysis is already dealt with from a non-malicious perspective by compliance with IEC 61513 and IEC 61226. As a consequence, the safety classification as per IEC 61226 shall be used as a significant input to the security degree assignment process. Security may benefit from safety provisions implemented to comply with requirements of IEC 61513 and of other IEC standards that are safety-relevant.

However, in order to take account of plant performance and of national practices regarding implementation of functions which may jeopardize safety in case of a cyberattack, there is not

a strict one-to-one mapping for I&C systems between their safety class and their security degree.

5.4.3.1.3 Description of the security degrees and associated assignment criteria

This document defines three security degrees, S1, S2 and S3, to which graded security requirements are associated (as defined in 5.4.3.2). These three security degrees are defined as follows:

a) The functions and systems shall be analysed to determine the maximum consequences on the plant safety and performance (as defined in 5.4.3.1.1) of malicious actions or events involving them.

b) This analysis shall be documented.

c) The systems shall be assigned to degrees S1 (the most stringent) to S3 according to these maximum consequences,

d) Security degrees should be assigned to I&C programmable digital systems as follows:

   – I&C programmable digital systems processing safety category A functions to security degree S1,

   – I&C programmable digital systems processing safety category B functions, and I&C programmable digital systems with direct and immediate impact on plant safety or on the main nuclear process operation, to no lower than security degree S2,

   – I&C programmable digital systems supporting Category C functions to S1, S2 or S3 according to the maximum consequences,

   – and I&C programmable digital systems assisting plant operation and maintenance to security degree S3.

As stated in 5.4.3.1.2, there is not a one-to-one mapping between safety categorization and security degrees. For instance, I&C programmable digital systems with direct and immediate impact on plant safety or on the main nuclear process operation are recommended to a security degree S2, without mention of the safety category; moreover, it is possible to assign a stringent security degree to non-safety classified systems (although item e) would apply). In addition to safety, impact on plant performance has been considered in the security degree assignment criteria.

e) A system may be assigned to a more stringent security degree than the one recommended in d) if the maximum consequences of a malicious act or event on any of the functions it implements are deemed equivalent to the ones corresponding to the more stringent security degree.

   Annex B provides explanations about the justification for having three security degrees for I&C programmable digital systems, and other complementary information.

NOTE 1 This document only deals with I&C systems and does not make any assumptions on security degrees for other kinds of systems. Non I&C systems might be assigned to supplemental/different security degrees, leading to a graded approach with more than 3 security degrees from a plant global perspective (see for instance the 5 degree scheme of the IAEA NSS17, with which this document is consistent).

NOTE 2 Technical data management systems (e.g. work permit, work order, tag out, etc.), in particular those corresponding to the security level 4 of the IAEA NSS17 reference manual, are not considered in the scope of this standard. However, being closely tied with I&C systems, they deserve specific cybersecurity attention, which lead in some contexts to the use of a 4th security degree tailored for their protection. Another practice is to consider them as I&C system and then subdivide the security degree S3 into appropriate subdegrees.

NOTE 3 See 5.4.3.2.8 for computer–based tools of I&C systems.

5.4.3.2 Assignment of technical requirements

5.4.3.2.1 General

Security requirements valid for all I&C programmable digital systems are given in 5.4.3.2.4. To these requirements are added requirements given in 5.4.3.2.5 for S1-graded systems, requirements given in 5.4.3.2.6 for S2-graded systems and requirements given in 5.4.3.2.7 for S3-graded systems. These requirements deal with the systems themselves and the communications between systems. They restate or complement existing security requirements from IEC 61513, IEC 60880, IEC 62566 and IEC 62138.

It is important to stress that these cybersecurity requirements do not intend to, and cannot, substitute to requirements associated to other aspects, related to other relevant and applicable standards or documents, and in particular safety-related ones. They form an additional set of requirements.

For instance, if from a cybersecurity point of view, two systems are allowed to communicate, it is possible that safety-related requirements prevent such a communication. In such a case, the communication would of course be prohibited. IEC 62859 provides a framework to help in the coordination between safety and cybersecurity requirements.

Requirements applicable to computer-based tools, in particular those for I&C system maintenance and diagnostic purposes, are given in 5.4.3.2.8.

5.4.3.2.2 Link with security risk assessment activity and Design Basis Threats

5.4.3.2.2.1 The I&C programmable digital system security programme of the NPP shall include threat and vulnerability assessment.

5.4.3.2.2.2 Justification that security requirements have been correctly addressed shall be made by risk assessment analyses of the proposed solution. Such analyses take into account vulnerability assessment of the technical implementation and specific threat and attack scenario analysis (including the country-specific design basis threat (DBT), as applicable).

5.4.3.2.2.3 Threat and vulnerability assessment activities may lead to the identification and implementation of additional countermeasures required to prevent or mitigate the consequences of attacks against plant I&C systems.

5.4.3.2.2.4 Security provisions shall be compatible with safety requirements. IEC 62859 provides an adequate framework to ensure safety and cybersecurity coordination.

5.4.3.2.2.5 The plant specific risk assessment should cover at least the following steps:

– perimeter and context definition;
– threat identification and characterization;
– vulnerability assessment;
– attack scenario elaborations;
– evaluation of level of risk;
– countermeasure definition.

ISO/IEC 27005 provides a generic framework for information security risk assessment, but the specific implementation methodology is up to the organization, depending on its organizational, industrial and regulatory context.

5.4.3.2.2.6 The specific risk assessment methodologies and tools shall be identified and kept up-to-date. Risk re-assessments shall be performed periodically throughout the whole life cycle of the I&C systems, when modifications to the system occur and when changes to the threat landscape are identified, such as new threats or new vulnerabilities that can affect the installed I&C programmable digital system. The number of potential threats and vulnerabilities usually increases with progress from stand-alone to interconnected systems.

5.4.3.2.2.7 Risk assessment shall be always treated as advisory, that is not limiting the plant I&C security awareness only to identified risks. Management of I&C programmable digital systems' vulnerabilities should be carried through studies of the publications by national Computer Emergency Response Teams (CERTs), and contacts with the computer security community, focusing particular interest on I&C solutions and product weaknesses.

NOTE Security degrees are assigned to I&C programmable digital systems or subsystems from the onset of a project. They are based on the potential consequences, as defined in 5.4.3.1.1, of a security attack on I&C systems or on functions they implement. Security degrees, via associated requirements, help specify systems.

5.4.3.2.2.8 When making bids, the supplier shall justify that his solution matches security requirements by making risk assessment studies.

5.4.3.2.3 Confidentiality

In the framework of this document, it is useful to distinguish two different aspects:

– confidentiality of data exchanged, treated and/or stored by I&C digital programmable systems (measures, commands, set points, etc.), and

– confidentiality of information about I&C digital programmable systems (e.g., detailed design and specifications, status, versions, network maps, etc.).

With respect to the first aspect, although integrity and availability of I&C systems and functions are usually the prime security objectives, specific contexts and risk analyses may lead in some cases to the implementation of confidentiality-focused mechanisms to protect I&C systems. Being very context-related, they are not specifically addressed in this document. IEC 62859 provides guidance and requirements about the use of confidentiality-focused cryptographic mechanisms.

The second aspect is of paramount importance, but is out of the scope of this standard. It should be treated according to national regulations.

NOTE The IAEA implementing guide NSS 23-G provides a general framework to deal with nuclear security related information.

5.4.3.2.4 Baseline requirements

The following requirements apply to all I&C programmable digital systems, independent of their security degree assignment.

a) Design measures shall be defined to provide adequate confidence that the treatments of a system assigned to a given security degree are not degraded by systems assigned to a less stringent security degree.

b) Any I&C system should be configured and parameterized so as to minimize the vulnerability of the system.

c) Any pre-developed component should be selected, configured and parameterized so as to minimize the vulnerability of the system.

d) The system security analysis, including risk assessment, shall be taken into account in the system security plan. If the analysis shows that the planned measures are not sufficient then the security analysis shall identify the need for additional countermeasures.

e) The security policy shall be adapted to each I&C system or group of systems. A correspondence should be established between the overall security policy and its adaptation to the I&C systems or groups of systems. This can be done more or less formally.

f) Effective protection measures should be included in the design, configuration and/or parameter assignment of programmable equipment concerning:

   – user selective access control to the software functions and memory spaces,

   – data connections to systems with less stringent security degree,

   – traceability of software or parameter modifications.

g) During verification and validation of the system, the effectiveness of the security functions shall be demonstrated through suitable tests with the system in its final configuration.

h) I&C systems should support technical measures to provide an effective authentication procedure before access is permitted.

i) Human-machine-interfaces either to operate the plant or off-line dedicated functions, or used for I&C system maintenance, should restrict access to the minimally necessary extent, both in terms of authorized staff and authorized operations. When the minimally necessary extent cannot be reached, compensating security controls should be implemented.

j) A security assessment of the on-site configuration and parameter assignment should take place to verify that suitable countermeasures have been implemented against potential security threats.

k) Software modification activities shall be systematically planned for and performed and consider potential security threats.

l) Logs should be checked periodically from a security perspective for safety-classified I&C programmable digital systems and systems monitoring safety-classified I&C programmable digital systems.

m) Logs should be checked periodically for systems ensuring cybersecurity functions (e.g., filtering and/or segmentation equipment). These logs should be centrally managed and correlated where possible as long as it does not compromise security (e.g., network segmentation) or safety separations (e.g., for independence purposes).

n) The number of access points to networks shall be minimalized to the extent possible to minimize vulnerability.

o) Provisions for anomaly detection should be implemented and alarms should be analyzed with appropriate response measures taken. Implementation shall be compatible with safety requirements.

p) Physical access to I&C systems shall be strictly controlled to prevent access from unauthorized persons. This shall be enforced by physical security measures (e.g., locked cabinet, physical access control to the room or area) and covered by appropriate organizational and administrative measures. These measures shall be commensurate with the security degree of the systems considered.

q) Physical and logical access of contractors to I&C systems shall be restricted according to their mission, both in terms of duration and systems involved.

r) All temporary provisions, for example root access and supplementary connections for test devices, shall be identified and registered.

s) Software configuration and hardware implementation changes shall be forbidden when not planned, approved by the owner, and documented.

t) Arrangements shall be in place to enable a timely restoration of an acceptable level of service in the event of a successful cyberattack. Measures shall be put in place to minimize the possibility that these arrangements are themselves vulnerable to the same cyber threats.

5.4.3.2.5 Degree S1 additional requirements

The minimum set of security requirements for S1-graded I&C programmable digital systems (in addition to the baseline ones) is listed below. The required application-specific security measures shall be determined by an application-specific system security analysis, including relevant threat and attack scenario, and identification of system vulnerabilities.

a) For S1 systems, I&C programmable digital communications shall be restricted to other S1-graded I&C programmable digital systems and to S2-graded I&C programmable digital systems, and to their associated computer-based tools.

b) Communications should be oriented from S1-graded I&C programmable digital systems towards S2-graded I&C programmable digital systems.

c) Data network transmission from a S2-graded system to a S1-graded system shall be limited to unavoidable transmissions (e.g. for priority actuators control systems, permissives, resets), and shall be supported by a complete justification and security risk-analysis. Any data transmitted from a S2-graded system to a S1-graded system shall be secured by adapted static provisions (e.g., format and time-window controls).

d) Software upgrade and configuration change of S1-graded systems shall be possible only by local hardware interlock means (e.g. keys) and only for one channel at time. Bidirectional data transfer between I&C equipment of highest security degree and a dedicated service station shall be performed using a dedicated and separated data connection which is decoupled from other networks. This dedicated data connection shall be secured by technical, operational and administrative means. Access with permission for software or configuration changes shall be monitored by alarms in the control room or other appropriate place.

e) There shall be provisions against hidden functions in the system software (e.g., software code verification).

f) Compliance with 5.7 (Software security) and 12.2 (On-site software security) of IEC 60880:2006 and IEC 62566 shall be required for S1-graded systems.

g) Physical access to S1-graded I&C systems shall be monitored by alarms in the control room or other appropriate place.

5.4.3.2.6 Degree S2 additional requirements

The minimum set of security requirements for S2-graded I&C programmable digital systems (in addition to the baseline ones) is listed below. The required application-specific security measures shall be determined by an application-specific system security analysis, including relevant threat and attack scenarios, and identification of system vulnerabilities.

a) Communications should be oriented from S2-graded systems towards S3-graded systems. S2-graded systems should act as initiators of the communication. These requirements (orientation and initiation) should be enforced by appropriate security provisions (e.g. dedicated filtering equipment).

b) Data transmission from a S3-graded system to a S2-graded system shall be strongly restricted and justified on a case-by-case basis.

c) Software upgrade and configuration change of a S2-graded system shall not be possible from a S3-graded system.

d) Software upgrade and configuration change of S2-graded systems shall be done only one channel at a time, only during predefined time windows, and should be protected by appropriate interlocks. Bidirectional data transfer between S2-graded I&C equipment and a dedicated service station should be performed using a dedicated and separated data connection which is decoupled from other networks. This data connection shall be secured by technical, organizational and administrative means.

e) Entering communication into S2-graded I&C systems, either from outside the plant or from non-I&C systems, shall be prevented.

f) Design measures shall limit access to programmable zones of S2-graded systems (e.g., by efficient user authentication) and prevent any unauthorized creation of new access to these zones.

5.4.3.2.7 Degree S3 additional requirements

The minimum set of security requirements for S3-graded I&C programmable digital systems (in addition to the baseline ones) is listed below. A system-specific security analysis should complete this list.

a) Access from non-I&C systems which could influence the I&C system functions shall be justified on a case-by-case basis and shall not compromise security and safety requirements associated to the system.

b) Communications between S3-graded systems and non-I&C systems should be initiated from the S3 -graded systems. Exceptions shall be justified and the connection shall be monitored.

5.4.3.2.8 Security requirements for computer-based tools (including maintenance and diagnostic)

5.4.3.2.8.1 Computer-based tools, in particular those for I&C system maintenance and diagnostic purposes, are well-proven attack vectors and typical intermediate targets in I&C system attack scenarios. They shall be assigned to the same security degree as that of the I&C system they are associated to, when there is a direct connection (either temporary or permanent) between them.

5.4.3.2.8.2 Lower security degree may be assigned in case of indirect connection, involving procedural and/or human control. If the computer-based tools are associated to less stringent security degrees, the tools should be designed to prevent unplanned action. Logging (who/what/when) the use of tools and strong access controls shall be implemented.

5.4.3.2.8.3 Associated security requirements for computer-based tools should be adapted as follows:

– 5.4.3.2.4 (baseline requirements) holds for all computer-based tools.

– For S1 degree, 5.4.3.2.5 holds except for its item g) (dealing with alarms) which is not relevant for computer-based tools, and except for its item e) (dealing with hidden functions) which is superseded by the following: there should be provisions against hidden functions in the tool system software.

– For S2 degree, 5.4.3.2.6 holds except for its items c), d) and f) which are not relevant for computer-based tools. Its item e) is superseded by the following: entering communication into S2-graded I&C systems, either from outside the plant or from non-I&C systems, should be prevented.

– For S3 degree, 5.4.3.2.7 holds (same requirements).

NOTE These adaptations aim to take into account potentially important technological difference between the I&C programmable digital systems themselves and their computer-based tools, especially for safety systems.

5.4.3.3 Security zones

5.4.3.3.1 A possible practical implementation of the graded approach is to group I&C programmable digital systems into logical zones, where graded protective principles are applied for each security zone (see definition in Clause 3). Zones 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. Criteria for a defining security zone may include organizational issues (such as ownership/responsibility), localization, architectural or technical aspects.

NOTE In the rest of this document, the term “zone” refers to “security zone” as defined 3.21 and in this subclause. It does not refer to safety zones and the associated geographical separations (although some relations exist).

5.4.3.3.2 The delineation and implementation of security zones should comply with the following guidelines:

a) Each zone comprises systems that have the same degree of security. If for architectural or other reasons, a I&C programmable digital system has a less stringent security degree (as per 5.4.3.1.3) than the other systems grouped in the zone, its security degree should be upgraded and comply with the requirements associated to security degree of the other systems of the zone.

NOTE 1 Security degrees are assigned to I&C programmable digital systems (see 5.2.3.2). However, as a zone groups systems having the same security degree, a given zone can be considered by extension as having the security degree of the systems it groups (e.g., “security zone of degree S2”). However, security zone and security degree are intertwined but still distinct concepts.

b) Security barriers are not required between systems belonging to the same security zone. However, for zones with multiple systems and inter-zonal interfaces, barriers may be an effective means of protection.

NOTE 2 If communication between systems having a same security degree is possible from a cybersecurity graded approach point of view, it does not mean that it is not restricted or forbidden for other reasons, such as safety-related requirements (e.g., independence), architecture, or cybersecurity zoning.

c) Network equipment (switches, cables, etc.) shall be located in a security zone consistent with those of the interconnected I&C systems. In case of network equipment connected to multiple zones, if the zones have the same security degree, then, the potential security separations shall be defined by specific facility requirements (out of the scope of this document). If the zones have different security degrees, then the security requirements associated to security degrees apply (see 5.4.3.2.4 to 5.4.3.2.7). In particular those dealing with communications and interfaces between systems of different security degrees shall involve dedicated security provisions.

d) Communication should only be initiated from a higher security zone (grouping systems assigned to a given security degree) to a lower security zone (i.e., grouping systems assigned to a lower security degree).

e) Zone borders require decoupling mechanisms for data flow, consistent with the security degree of the associated I&C programmable digital systems.

5.4.3.3.3 The relationship between security zones and security degrees is not one-to-one; a degree may be assigned to multiple zones.

5.4.3.3.4 Security zones can be used to segment systems with the same security degree but with different safety classes. IEC 62859 provides more guidance on the relation between safety and cybersecurity.

NOTE Zones are a logical and/or physical grouping of computer systems, while security degrees represent the degree of protection required.

5.5 Support

5.5.1 Resources

The content of ISO/IEC 27001:2013, 7.1 applies.

5.5.2 Training, competence and awareness

5.5.2.1 Training

Education of staff, including contractors, within an organisation is necessary to achieve a secure cyber environment for I&C programmable digital equipment. It reduces the chances of security breaches and internal security occurrences. As a consequence:

a) A formal training programme for personnel designing and supporting I&C programmable digital systems shall be developed and delivered.

b) This programme shall include general training courses relevant for all users and specialized training courses, adapted to the security degree of the systems accessed by the attendees.

5.5.2.2 Competence

The content of ISO/IEC 27001:2013, 7.2 applies.

5.5.2.3 Awareness

The content of ISO/IEC 27001:2013, 7.3 applies.

5.5.2.4 Expertise in training and awareness

Awareness and training shall involve organizations or individuals who have expertise in I&C programmable digital system security, ideally in the context of nuclear power plants.

5.5.3 Communications about cybersecurity

The content of ISO/IEC 27001:2013, 7.4 applies.

5.5.4 Documented information

5.5.4.1 General

5.5.4.1.1 The content of ISO/IEC 27001:2013, 7.5.1 applies.

5.5.4.1.2 The I&C programmable digital systems security programme shall establish the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cybersecurity are developed, reviewed, approved, issued, used, and revised to reflect completed work including:

– records that are generated in the establishment, implementation and maintenance of the programme;
– records of threat assessment results that address the specific vulnerabilities with respect to the technology being used, the configuration of the I&C programmable digital systems, and the nature of their use, maintenance or test requirements;
– records of addition, modification, and removal of I&C programmable digital assets addressed by the programme;
– records and supporting technical documentation including audit data and training records, required to satisfy country specific regulatory requirements.

Documentation supports the demonstration that I&C programmable digital systems design and actual implementation meet an appropriate level of security as per this document, and that the system users have received the adequate instruction and training on operation and maintenance of the security-related elements of the system.

5.5.4.2 Creating and updating

The content of ISO/IEC 27001:2013, 7.5.2 applies.

5.5.4.3 Control of documented information

The content of ISO/IEC 27001:2013, 7.5.3 applies.

5.6 Operation

5.6.1 Operation planning and control

The content of ISO/IEC 27001:2013, 8.1 applies.

5.6.2 Cybersecurity graded approach, risk assessment and risk treatment

5.6.2.1 The organization shall implement and maintain the graded approach and perform risk assessment and risk treatment as per 5.4.3.

5.6.2.2 The organization shall retain documented information of the graded approach implementation, risk assessments and risk treatments.

5.7 Performance evaluation

5.7.1 Monitoring, measurement, analysis and evaluation

5.7.1.1 General

The content of ISO/IEC 27001:2013, 9.1 applies.

5.7.1.2 Security reviews and audits

5.7.1.2.1 A major element of maintaining an effective I&C programmable digital system security programme is to conduct periodic security reviews. The programme shall establish the necessary measures and governing procedures to implement reviews of applicable programme elements, in accordance with the national regulatory requirements.

5.7.1.2.2 As a consequence, the organization shall:

a) Establish a review programme that addresses the purpose, scope, roles, responsibilities, requirements and management commitment associated with reviewing elements of the I&C programmable digital system security programme for effectiveness.

b) Establish procedures to facilitate and maintain the review programme including required frequency of reviews, and qualifications of individuals performing the reviews.

5.7.2 Internal audit

5.7.2.1 The content of ISO/IEC 27001:2013, 9.2 applies.

5.7.2.2 IAEA TLD-006 provides an appropriate generic framework for auditing nuclear installation, including I&C systems, however, the specific audit methodology is up to the organization, depending on its organizational, industrial and regulatory context.

5.7.3 Management review

5.7.3.1 The content of ISO/IEC 27001:2013, 9.3 applies.

5.7.3.2 The output from the management review and approval shall include any decisions and actions related to the following:

a) implementation of and modifications to procedures and controls that affect the I&C programmable digital system security programme, as necessary, to respond to internal and external events that may impact on:
   - business requirements,
   - security requirements,
   - regulatory and legal requirements,
   - contractual obligations,
   - levels of risk and/or criteria for accepting risks,
   - resource needs;

b) initial criteria and improvements to how the effectiveness of controls is being measured;

c) decision process and criteria to take actions impacting plant operations (e.g., continued plant operation, plant shutdown, communication isolation, equipment maintenance).

5.7.3.3 The decisions and actions based on this management review shall be taken with an adequate decision process ensuring coordination with non-I&C system security programmes, plant physical protection regimes and plant operations and maintenance programmes.

5.8 Improvement

5.8.1 General

The I&C programmable digital system security programme shall establish the process to:

a) Implement programme improvements identified during internal and external programme reviews including corrective and preventive actions.

b) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances, and as part of the ongoing training programme.

c) Develop and implement a review programme to periodically evaluate and update the security threat assessment and information about identified vulnerabilities.

d) Establish measures to evaluate whether the improvements achieved their intended objectives.

5.8.2 Nonconformity and corrective action

The content of ISO/IEC 27001:2013, 10.1 applies.

5.8.3 Continual improvement

The content of ISO/IEC 27001:2013, 10.2 applies.

6 Life-cycle implementation for I&C programmable digital system security

6.1 General

The following subclauses provide an overview of the documents and tasks that should be included in the I&C programmable digital security life cycle process on a system level. The I&C programmable digital security life cycle is developed to address I&C programmable digital systems and components from inception to operation and ultimately retirement.

NOTE The lifecycle used in this clause corresponds to the system safety lifecycle of IEC 61513:2011, extended with two phases “Operation and maintenance activities” and “Retirement”.

A proper coordination between safety and cybersecurity aspects shall be ensured. Requirements and recommendations can be found in IEC 62859.

6.2 System requirements specification

6.2.1 General

6.2.1.1 A top-down approach, considering the global I&C architecture to the individual systems and components, shall be used.

6.2.1.2 Security specifications shall be written in order to cover the global I&C architecture from a functional and a security point of view, before addressing systems and their interfaces.

NOTE When writing specifications, systems implementing the needed functionality are not known, so that it is not possible to carry out a complete and detailed security risk assessment: in particular, only threat or high-level consequence evaluations are possible at this stage.

6.2.1.3 Individual systems or components may be supplied and secured by different suppliers, provided the security of the whole architecture is consistently maintained.

6.2.1.4 Product security specifications shall be provided by the suppliers.

6.2.2 Security degree assignment

Each individual I&C programmable digital system shall be assigned to a security degree. The security degrees shall be based on the graded approach to I&C programmable digital system security, described in 5.2.3.

NOTE The term “system” is used in the sense of an “individual I&C system” according to IEC 61513.

6.3 System specification

6.3.1 Selection of pre-existing components

6.3.1.1 The suitability of the candidate components shall be evaluated and assessed to demonstrate that their characteristics comply with the system security requirement specifications.

6.3.1.2 The security suitability evaluation and assessment of the candidate components should be based on the comparison of the security requirements specifications of the system and the security documentation related to the pre-existing components. The latter includes when available the product security specification.

6.3.1.3 If discrepancies between the security requirements specification of the system and the equipment family security specifications are identified which render the equipment unsuitable for the intended system security degree, the equipment shall be rejected.

6.3.1.4 The assessment of the suitability shall establish that the specification of the candidate equipment complies with its intended security degree and security specification.

6.3.2 System architecture

The system architecture is partitioned into a number of interconnected subsystems and components. The arrangement of system subsystems shall comply with security requirements related to the overall security degree of the system.

6.4 System detailed design and implementation

6.4.1 General

6.4.1.1 The design phase shall incorporate the objectives of the plant design as a whole and on the individual system security degree basis (assigned as per 5.2.3) to address security controls over:

a) physical and logical access to the I&C system function,

b) use of the I&C system, and

c) data communication with other I&C systems.

6.4.1.2 The designer should ensure that the software code design complies with secure coding practices, to address potential vulnerabilities that can be introduced as part of the design process. A specific interest should be given to configuration management.

6.4.1.3 The requirements shall be translated into specific design criteria.

6.4.1.4 Access to all software entities placed under configuration control shall be subject to adequate controls to ensure that software is not modified by unauthorized persons and that the security of the software is maintained.

6.4.1.5 The designer shall make a complete inventory of all I&C systems and of their interfaces considering all devices used within the plant, including diagnostic, maintenance or test devices.

6.4.2 Risk assessment at the design phase

6.4.2.1 Justification that security requirements have been correctly addressed should be completed by risk assessment. Such analyses take into account vulnerability analyses of the technical implementation and specific threat and attack scenario analysis, (including country-specific design basis threats (DBT), as applicable).

6.4.2.2 Risk assessments may lead to change the security measures or the security architecture. Threat and vulnerability assessment activities may lead to the identification and implementation of complementary countermeasures required to prevent or mitigate the consequences of attacks against plant I&C systems.

6.4.3 Design project security plan

6.4.3.1 The I&C security plan shall apply to the primary design organization and all third party or subcontractor organizations working on the project.

6.4.3.2 A design project security plan, covering the licensee/operator but also third-parties and external entities involved in the project, shall be established.

6.4.3.3 In particular, the designer shall show that:

a) a security policy is in place;

b) such a policy applies for each of its development sites;

c) it is completed along local aspects;

d) it ensures that its own third-parties meet an adequate security level.

6.4.4 Communication pathways

6.4.4.1 Communication pathways shall be evaluated in the design of the system and components. As part of this process, the system boundaries should be defined and a system map established.

6.4.4.2 Cybersecurity controls shall be established to:

a) Enforce and document assigned authorizations for controlling the flow of information, within and between interconnected systems in accordance with their assigned security degrees (see 5.4.3.1).

NOTE This is the case for systems assigned to different security degrees or to different security zones.

b) Maintain documentation that demonstrates the analysis and addressing of permissible and impermissible flow of information between systems and devices addressed in the I&C programmable digital system security programme, consistently with the risk assessment and graded approach described in 5.4.3.

6.4.4.3 Wireless devices shall comply with 4.3, 5.6 and Clause 8 of IEC 62988:2018, involving prohibition for S1 and S2 graded systems, and conditions for S3-graded systems.

NOTE As per the assignment criteria of security degrees, wireless is excluded for systems supporting Category A or B functions.

6.4.5 Security zone definition

6.4.5.1 Security zones (see 3.21 and 5.4.3.3) should be defined during the design phase. They may alternatively be defined in the implementation phase (see 6.5).

6.4.5.2 Assignment of I&C programmable digital systems to security zones shall take into account, as per 5.4.3.3, the security degree assigned previously to each I&C programmable digital system during the planning phase, and identified communication pathways (see 6.4.4).

6.4.6 Security assessment of the final design

Security assessments shall cover the overall I&C architecture at the final design stage.

6.4.7 Implementation activities

6.4.7.1 In the implementation phase, hardware and software shall be implemented per the system design including all defined security requirements.

6.4.7.2 If changes from the intended design or substantial new technical information are available, threat and vulnerability assessment activities shall be updated which may lead to complementary countermeasures.

6.5 System integration

As per IEC 61513, the objective of this phase is to assemble the hardware and software modules and to verify compatibility of the software loaded into the hardware. During this phase:

a) the integrated security features should be in place and configured as per specification prior to integration testing and system validation (see 6.6).

b) integration testing should confirm that the integrated security controls perform as required and do not adversely affect the system's ability to perform its required functions (see IEC 62859 for more inputs on the coordination between safety and cybersecurity).

c) A phase-specific system integration security plan shall be developed either as a stand-alone document or as a part of an overall security plan.

6.6 System validation

6.6.1 Verification and Validation (V&V) testing per required standards shall be performed for the specified security requirements of I&C programmable digital systems.

6.6.2 Additionally, testing shall verify the I&C security design of the hardware architecture, external communication devices and configurations for unauthorized pathways and system integrity.

6.6.3 The security requirements and configuration items shall be part of validation of the overall system requirements and design configuration items.

6.6.4 Each system security feature shall be validated to ensure that the implemented system does not increase the risk of security vulnerabilities and does not reduce the reliability of safety functions (see IEC 62859 for more inputs on the coordination between safety and cybersecurity).

6.6.5 A phase specific system validation security plan shall be developed either as a stand-alone document or as a part of the overall security plan.

6.7 System installation

6.7.1 The installation and acceptance testing for specified security requirements shall comply with the plant-specific policy and procedures, as well as the plant I&C programmable digital system security programme, as applicable.

6.7.2 At the end of the installation, the system shall be tested in the operational environment to verify and validate the correctness of the I&C system security features and the incorporation into the system in accordance with the design.

6.7.3 A phase specific system installation security plan shall be developed either as a stand-alone document or as a part of the overall security plan.

6.8 Operation and maintenance activities

6.8.1 Change control during operations and maintenance

6.8.1.1 During the operational and maintenance phase, the periodic security audits of security features shall be performed.

6.8.1.2 Prior to any system modification or maintenance, the affected components shall be evaluated to confirm that all protective feature and design elements will remain functional.

6.8.1.3 After such modifications or maintenance activities are performed, any temporarily disabled security protective features and controls shall be restored and security functionality verified. Security requirements for computer-based tools are addressed in 5.4.3.2.8.

6.8.2 Periodic reassessment of risks and security controls

6.8.2.1 The effectiveness of the security controls implemented into the system shall be reassessed on a periodic basis.

6.8.2.2 Testing of security controls shall also be conducted if necessary to verify the effectiveness of controls following specific events.

6.8.2.3 Risk assessment shall be updated periodically.

6.8.2.4 Risk assessment shall be updated in case of identification of a new major security vulnerability, or in case of major modification in the I&C architecture (e.g. addition of a system, new network link, etc.).

6.8.2.5 Risks that emerge or become apparent during operations shall be managed in a timely manner and in accordance with defined procedures and regulatory requirements.

6.8.3 Change management

6.8.3.1 Change management processes shall follow plant procedural, regulatory and/or licensing commitments, as applicable, for maintaining both compliance basis and configuration control.

6.8.3.2 A risk assessment shall be performed before any modifications are made that could affect a security feature. The approval process should be adapted to the considered change.

6.8.3.3 At a minimum, the impact to security shall be considered based on risk assessment and documented prior to any change. Justification shall be provided to demonstrate appropriate measures are already in place or will be implemented to address any identified new risks in an appropriate manner.

6.8.3.4 Unauthorized or undocumented changes to network configuration or characteristics by the plant personal or a third-party can weaken or void security measures in place. Therefore, careful control of design and maintenance practices shall be provided to prevent violations of this type.

6.9 Retirement activities

6.9.1 The I&C system retirement phase shall be primarily the responsibility of the plant management.

6.9.2 An effective continuing programme shall address the retirement lifecycle phase. Procedure(s) shall be in place to address proper retirement of I&C programmable digital devices and disposal of media and resident software in a controlled manner, to avoid disclosure of sensitive information.

6.9.3 In addition, security aspects for the preparation of a system for retirement such as the dual operation of both the current and new system – if needed – should be addressed.

7 Security controls

7.1 General

This clause provides generic considerations to take into account in nuclear I&C environments when selecting and enforcing cybersecurity controls in the framework of a programme elaborated according to Clause 5 and Clause 6 requirements.

NOTE 1 Cybersecurity controls, security controls and security measures are considered synonymous.

ISO/IEC 27002:2013 provides a catalog of security controls, grouped under 14 clauses and 35 categories. ISO/IEC 27002:2013 is information security-oriented, and does not take into account nuclear I&C specific aspects and is not directly applicable in such contexts.

NOTE 2 A dedicated international standard dealing with cybersecurity controls is under development within IEC SC 45A at the time of the writing of IEC 62645 ed. 2. It will provide more detailed content on this subject.

7.2 Characterization

7.2.1 Three types of cybersecurity controls can be distinguished:

– technical controls: hardware and/or software solutions for the protection, detection and mitigation of and recovery from intrusion or other malicious acts;

– physical controls: physical barriers for the protection of computer and supporting assets from physical damage and unauthorized physical access. The physical controls include barriers such as locks, physical encasements, tamper seals, isolation rooms, gates and guards;

– administrative controls: policies, procedures and practices designed to protect computer systems by controlling personnel actions and behaviors. The administrative controls are directive in nature, specifying what employees and third party personnel should and should not do. In the nuclear environment, administrative controls are understood to include operational and management controls.

7.2.2 Cybersecurity programme shall involve the use of the three types of cybersecurity controls (with proper coordination with the site physical protection aspect, out of the scope of this document).

7.2.3 Cybersecurity controls may contribute in different manners to cybersecurity, mostly by contributing to:

– prevention of cybersecurity events;

– their detection;

– correction, reaction and/or response.

7.2.4 Cybersecurity programme and the resulting cybersecurity controls put in place shall cover these three aspects.

7.3 Security defence-in-depth

Security defence-in-depth is an approach to security in which multiple and independent security controls, covering organizational, technical and operational aspects, are deployed in an architecture, as no individual security control can provide the expected security. In such an approach, it is the set of diversified and independent security controls which is able to bring the needed prevention, detection and response capabilities.

The security defence-in-depth principle shall guide the selection of security controls.

NOTE The terms “safety defence-in-depth” and “security defence in depth” are used in this document. The former refers to defence in depth as defined in the IAEA Safety Glossary, whereas the latter refers to a similar, but security-focused concept of defence in depth defined in the Nuclear Security Fundamentals, IAEA NSS20) in implementing computer security controls.

7.4 Selection and enforcement of cybersecurity controls

7.4.1 Selection and enforcement of security controls shall be based on the approach described in 5.4.3.

NOTE The informative Annex D and Annex E provide graphical representations on how IEC 62645 interacts with the international standards, and in particular IEC 63096 dedicated to cybersecurity controls for I&C digital systems.

7.4.2 High-level requirements attached to security degrees (i.e. as per 5.4.3.2.4 and 5.4.3.2.5, 5.4.3.2.6 or 5.4.3.2.7 depending on the security degree) shall result into the selection and application of security controls, documented, enforced and monitored in the framework of a security programme compliant with Clause 5.

7.4.3 Complementary security controls may result from other risk analysis activities, taking into account specifics of the project, the context and the system considered, and from application of country-specific laws and regulations.

7.4.4 The applicability of cybersecurity controls, and in some cases its implementation, should be differentiated depending on the lifecycle phase of the system to protect. One possible way is to distinguish between:

– development phase (project independent development of a generic I&C system),

– project engineering (site-dependent project, including when relevant conceptual design, basic and detailed Design, FAT, shipping to site);

– operation and maintenance.

An alternative is to use the system lifecycle of Clause 6.

7.4.5 Legacy systems should be treated with a particular attention, with an adapted selection process of cybersecurity controls.

NOTE Detailed recommendations will be brought in the future international standard dealing with cybersecurity controls, mentioned in the first note of 7.1 (under development with IEC SC 45A at the time of the writing of IEC 62645 ed. 2.).

Annex A
(informative)

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

A.1 Objective of this annex

This annex presents the reasons and rationale which have led 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 standard development have finally decided to include in the scope I&C programmable digital systems not important to safety because assessing the impacts of cyberattacks, including in terms of plant safety, involves a global perspective (for instance, the effects of multiple coordinated attacks cannot be properly taken into account by an analysis limited to systems important to safety only).

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

This 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 site 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 framework (except for human errors degrading cybersecurity).

A.5 Development tools and platforms

This document is limited to I&C programmable digital systems used in a NPP, including on-site maintenance and configuration tools. It does not directly target 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 meeting its requirements. Securing development tools and platforms is crucial from a global cybersecurity perspective; however this document has not been particularly developed to treat these aspects globally, as they deserve due care but mainly non-nuclear I&C specific considerations.

Annex B
(informative)

Generic considerations about the security degrees

B.1 Rationale for three security degrees

B.1.1 General

Experts have considered in IEC 61226 that 3 safety categories were necessary and sufficient to grade all safety functions. Similarly, it has been considered in IEC 62645 that 3 security degrees were necessary and sufficient to grade security measures for all I&C programmable digital systems. However, if this eases linkage between the two scales, there is not a one-to-one mapping between safety categories and security degrees.

Indeed, in the context of this document, both plant safety (for obvious reasons) and plant availability (as energy is vital for countries) are considered as fundamental objectives and constitute the basis for security degree assignment.

NOTE 1 This document only deals with I&C programmable digital systems and does not make any assumptions on security degrees for other kinds of systems. Non-I&C systems might be assigned to supplemental/different security degrees, leading to a graded approach with more than 3 security degrees from a global NPP perspective (see for instance the 5 degree scheme of the IAEA NSS17, with which this document is consistent).

NOTE 2 Technical data management systems (e.g. work permit, work order, tag out, etc.), in particular those corresponding to the security level 4 of the IAEA NSS17 reference manual, are not considered in the scope of this document. However, being closely tied with I&C systems, they deserve specific cybersecurity attention, which lead in some contexts to the use of a 4th security degree tailored for their protection. Another practice is to consider them as I&C system and then subdivide the security degree S3 into appropriate subdegrees.

B.1.2 Safety categories as input to security degree assignment

Safety is the first aspect to deal with since, if it is not ensured, the plant cannot be licensed. From this perspective, the 3 safety categories defined in IEC 61226 are obviously to be taken into account to define the security degrees. Noting that the more necessary to safety an I&C programmable digital system is, the more stringent its security degree has to be, the following has been proposed:

– I&C programmable digital systems processing safety category A functions involve the most stringent security degree (S1),
– I&C programmable digital systems processing safety category B functions involve at least an intermediate security degree (S2),
– I&C programmable digital systems processing safety category C functions imply an analysis of the worst consequences on plant safety of a cyberattack targeting these systems, as it may lead to weaken safety category A or B functions (e.g., values not maintained within assigned safety limits, safety probabilistic goals not matched, prevention of internal hazards not ensured, etc.),
– I&C programmable digital systems not processing safety functions can be assigned to a less stringent and third security degree (S3), notwithstanding their potential impact on plant availability, or even plant safety when manipulated by an attacker (i.e. outside the assumptions adopted for safety categorization of IEC 61226), which can lead to assign them a stronger security degree.

B.1.3 Impact on plant availability and performance as input to security degree

The security classification of I&C programmable digital systems necessary to plant availability and performance is then to be considered. Consequences of a cyberattack on I&C programmable digital systems necessary to operate the plant cannot reach those of security degree S1 systems, but may be, regarding plant performance, equivalent in the worst case to those of a successful cyberattack on a S2 security classified I&C system.

B.1.4 Resulting security degree assignment approach

To sum up, only 3 security degrees are necessary to grade the impact of cyber-attacks on I&C programmable digital systems, integrating plant safety and availability dimensions:

– S1 for I&C programmable digital systems processing safety category A functions, and functions which could have the same impact on safety when manipulated maliciously (whatever their safety category),

– S2 for I&C programmable digital systems processing safety categories B functions or functions which could have the same impact on safety when manipulated maliciously (including potentially specific category C or non-classified functions) and systems with direct and immediate impact on plant safety or on the main nuclear process operation,

– S3 for I&C programmable digital systems which cannot have when attacked a direct and immediate impact on plant safety or on the main nuclear process operation.

Regarding plant safety or availability, the security degree of an I&C programmable digital system may be upgraded to the degree corresponding to consequences of a successful cyberattack on the most sensitive function it processes.

B.2 Considerations about tools associated to on-line systems

Tools associated to on-line systems, for example to configure, monitor or maintain them, do not need to comply with the same safety requirements, but considering that when connected to on-line systems they are potential attack vectors, they shall be assigned to the same security degree, involving comparable security (not safety) requirements.

B.3 Practical design and implementation

As a first step, possible impact on plant safety and performance of functions which are not processed by security degree S1 systems are analysed in order to assign them an adequate security degree. The second step is the assignment of security controls according to the security degree of the I&C system, and associated requirements. A third step consists in security analyses for each system. The third step aims at designing proper cyber-protection for each I&C system taking account of the baseline requirements associated to its degree and the results of its security analysis.

Annex E provides an overall view of the process to select security controls, and how the different SC 45A standards interact with each other.

Annex C
(informative)

Correspondence with ISO/IEC 27001:2013

Table C.1 shows the correspondence between ISO/IEC 27001:2013 and IEC 62645 (this mainly concerns Clause 5, dealing with programmes). All the clauses and associated requirements of ISO/IEC 27001 have been considered; they are either:

– "identical", meaning that the requirements are exactly the same (with the terminological differences discussed in 1.3), or

– "augmented", meaning that in addition to the same requiring the same thing as ISO/IEC 27001, specific requirements have been added for IEC 62645 (mainly coming from ed. 1.0), completing ISO/IEC 27001, or

– "adapted" meaning that IEC 62645 covers the thematic with some common elements, but also with specifically tailored content, taking into account the specificities of NPPs and I&C contexts.

Table C.1 – Correspondence between ISO/IEC 27001:2013 and IEC 62645

ISO/IEC 27001:2013		IEC 62645		Content
4	**Context of the organization**	5.1 and 5.2.1	Same title (for 5.1)	Augmented
4.1	Understanding the organization and its context	5.1.1	Same title	Identical
4.2	Understanding the needs and expectations of interested parties	5.1.2	Same title	Identical
4.3	Determining the scope of the ISMS	5.1.3	Same title	Augmented
4.4	Information security managament system	5.2.1	I&C digital programmable system security program	Augmented
5	**Leadership**	5.3	Same title	Augmented
5.1	Leadership and commitment	5.3.1	Same title	Identical
5.2	Policy	5.2.2	Same title	Augmented
5.3	Organizational roles, responsibilities and authorities	5.3.2	Roles, responsibilities and authorities	Augmented
6	**Planning**	5.4	Planning of the programme	(detail below)
6.1	Actions to address risks and opportunities	5.4.3	Graded approach to I&C security and risk assessment	Adapted
6.1.1	General	5.4.2	Addressing risks and opportunities of the programme	Identical
6.1.2	Information security assessment	5.4.3(.2.2)	Graded approach to I&C security and risk assessment	Adapted
6.1.3	Information security risk treatment	5.4.3	Graded approach to I&C security and risk assessment	Adapted
6.2	Information security objectives and planning to achieve them	5.4.1	Cybersecurity objectives and planning to achieve them	Identical
7	**Support**	5.5	Same title	Augmented
7.1	Ressources	5.5.1	Same title	Identical
7.2	Competence	5.5.2.2	Same title	Identical
7.3	Awareness	5.5.2.3	Same title	Identical
7.4	Communications	5.5.3	Same title	Identical
7.5	Documented information	5.5.4	Same title	Augmented
7.5.1	General	5.5.4.1	Same title	Augmented

ISO/IEC 27001:2013		IEC 62645		Content
7.5.2	Creating and updating	5.5.4.2	Same title	Identical
7.5.3	Control of documented information	5.5.4.3	Same title	Identical
8	**Operation**	5.6	Same title	(detail below)
8.1	Operation planning and control	5.6.1	Same title	Identical
8.2	Information security risk assessment	5.6.2	Cybersecurity graded approach, risk assessment and risk treatment	Adapted
8.3	Information security risk treatment	5.6.2	Cybersecurity graded approach, risk assessment and risk treatment	Adapted
9	**Performance evaluation**	5.7	Same title	Augmented
9.1	Monitoring, measurement, analysis and evaluation	5.7.1	Same title	Identical
9.2	Internal audit	5.7.2	Same title	Augmented
9.3	Management review	5.7.3	Same title	Augmented
10	**Improvement**	5.8	Same title	Augmented
10.1	Non conformity and corrective action	5.8.2	Same title	Identical
10.2	Continual improvement	5.8.3	Same title	Identical
Annex A	**Reference control objectives and controls**	7	Cybersecurity controls	Adapted

Annex D
(informative)

Overall organisation of IEC SC 45A standards related to cybersecurity

Figure D.1 provides an overview of IEC SC 45A standards with cybersecurity relation. Only the relevant digital I&C system-related standards are represented. The right-hand side groups the cybersecurity-focused documents, whereas the left-hand side mentions the relevant safety-focused documents, which include or link towards cybersecurity related aspects.

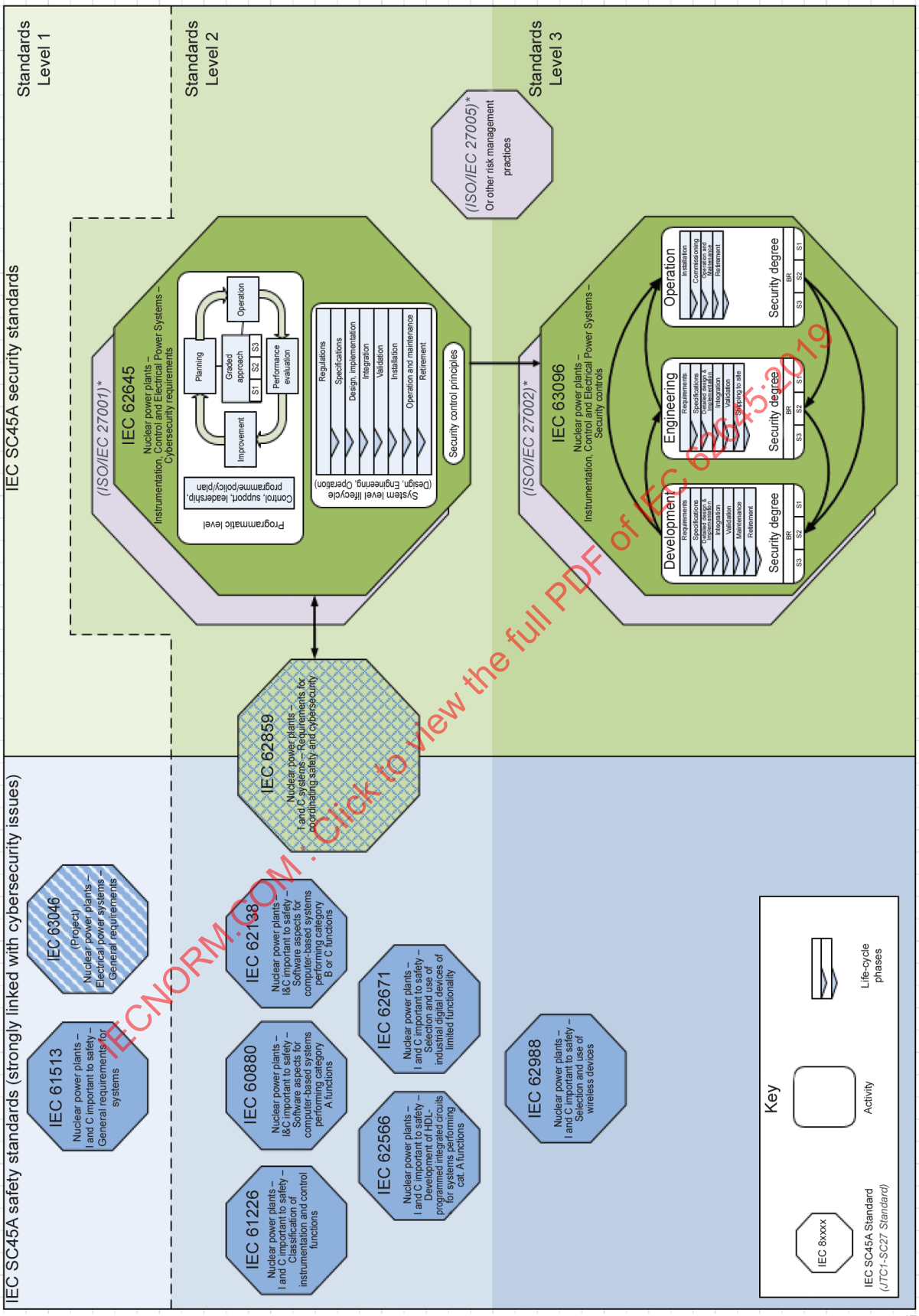


Figure D.1 – Overview of IEC SC 45A standards with cybersecurity relation

Annex E
(informative)

Selection of security controls

Figure E.1 provides a macroscopic view on how cybersecurity controls are selected according to IEC 62645 and to the future standard on cybersecurity controls (IEC 63096, currently under development). Some steps are described in this document, others are out of the scope of IEC 62645. This figure is provided on a strict indicative basis.

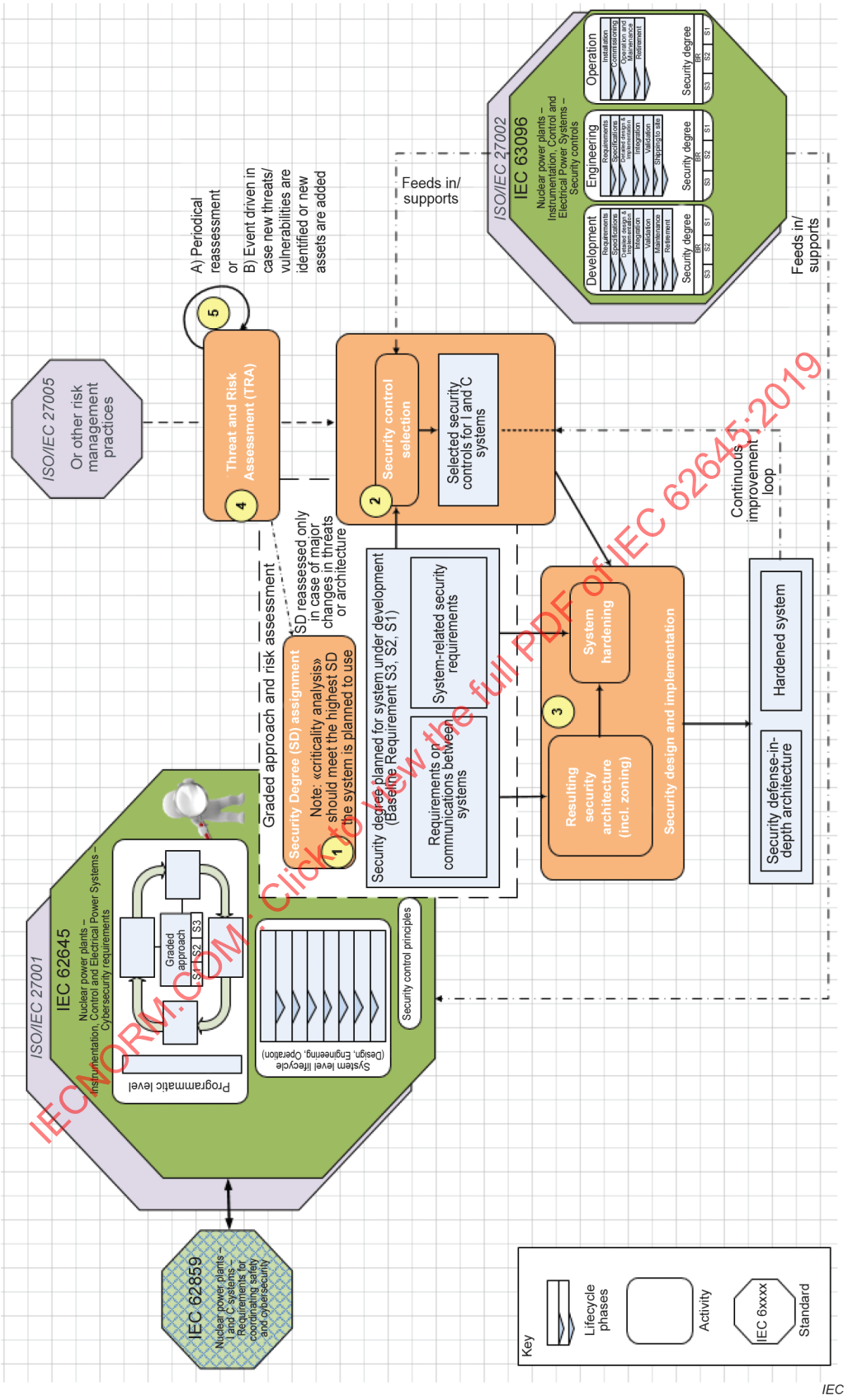


Figure E.1 – Selection of security controls

Annex F
(informative)

Considerations about IEC 62645 applicability to non-NPP nuclear facilities

F.1 Applicability of IEC 62645 security graded approach to Research Reactors

F.1.1 General

Para 1.2 of IAEA SSG-22 [1, see Clause F.4] states “Research reactors […] employ a variety of designs. Utilization of research reactors covers a wide range of activities such as: core physics experiments, training, target material irradiation for materials science, transmutation studies, commercial production of radioisotopes, neutron activation analysis, experiments involving high pressure and temperature loops for fuel and material testing, cold and hot neutron sources, neutron scattering research, and neutron and gamma radiography. These uses call for a variety of different design features and operational regimes. Therefore, site evaluation, design and operating characteristics of research reactors vary significantly.”

In addition, Research Reactors (RR) may also be classified as a multi-purpose reactor and perform a number of secondary operational objectives for example a reactor used primarily for the production of radioisotopes but also containing apertures for neutron scattering experiments as a secondary purpose.

This diversity complicates any effort to impart a standard approach to computer security when compared to approaches used for Nuclear Power Plants (NPPs).

However, NPPs and RRs are both required to comply with categorization of I&C functions important to safety, and the corresponding classification of I&C systems important to safety. This structuring common point provides a valuable basis to use IEC 62645 security graded approach for RR, as described in this annex.

F.1.2 Categorization of RRs in accordance with potential hazards

IAEA SSG-22 [1] provides guidance on application of a graded approach. Each RR is categorized based on the potential radiological hazard. These categories, arranged from most consequential to the least, are:

(1) Facilities with off-site radiological hazard potential;

(2) Facilities with on-site radiological hazard potential only;

(3) Facilities with no radiological hazard potential beyond the research reactor hall and associated beam tubes or connected experimental facility areas.

Typically, these consequences are strongly correlated with the Reactor Thermal Power. For example, in Canada, RRs with a gross thermal power greater than 30 MW are considered as facilities that have the potential to be associated with off-site radiological hazards (see (1) above). In China, the HTR-10 is a high temperature gas cooled reactor with 10 MW thermal power. The HTR-10 design considers the potential for off-site radiological hazards and has implemented safety features that have been evaluated to reduce the likelihood of occurrence to required regulatory limits [2].

However, in Austria [3], the 250 kW TRIGA reactor at the Atominstitut is considered to have no radiological hazard potential beyond the research hall and associated beam tubes or connected experimental facility areas (see (3) above). Owing to the lower thermal energy and fission product inventory, TRIGA reactors similar to the Austrian RR typically present a much smaller hazard than NPP reactors and as such need much less elaborate safety features to comply with safety requirements.

Although gross thermal power is a prime consideration, there are other individual characteristics, or attributes, that may impact the categorization of the RR into (1), (2) or (3) above. SSG-22 [1] identifies eleven attributes to be considered in deriving the category of the facility in accordance with its hazard (see 2.7 of SSG-22:2012).

Once the category of the facility is determined, safety classification of functions, and system categorization can occur using a similar process as to NPPs, based on IEC 61513.

RRs categorized as (1) above, would rely on a safety classification scheme similar to IEC 61513 (i.e. same as NPPs): these RRs would be expected to have 3 categories of safety functions ‘A’, ‘B’, and ‘C’.

RRs categorized as (2) or (3) would not require safety category ‘A’ functions.

Once the RR category is determined along with the categorization of safety functions, the corresponding I&C system safety class can be determined using IEC 61513 (See Table F.1).

Table F.1 – Correspondence between safety categories and classes as per IEC 61513

Categories of I&C functions important to safety (IEC 61513)			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3

F.1.3 Safety categories as input to security degree assignment

I&C functions important to safety for RRs must still be categorised. Once categorisation has been completed, the I&C programmable digital systems which directly provide for the safety function, can be classified. Using the safety classes defined in the IEC 61513, or their equivalent, the security degree can be defined based on importance.

Once the I&C safety class is known, a possible scheme for security degree assignment, consistent with IEC 62645, is as follows.

– I&C programmable digital systems that have been classified at the equivalent of safety class 1 require the most stringent security degree (S1),

– I&C programmable digital systems that have been classified at the equivalent of safety class 2 involve at least an intermediate security degree (S2),

– I&C programmable digital systems that have been classified at the equivalent of safety class 3 imply an analysis of the worst consequences on RR of an extended cyberattack targeting these systems. As result of the analysis:

  - For I&C programmable digital systems with the most severe consequences when attacked, including from a duration of impact perspective, at least an intermediate security degree (S2) is to be assigned;
  - For the others, a less stringent and third security degree (S3) is to be assigned.

– I&C programmable digital systems not processing safety functions or processing safety functions that have been classified as the equivalent of safety class 3 and are supported by other safety processes through defence in depth, involve a less stringent and third security degree (S3).

F.1.4 Impact on operational capacity as input to security degree

After the functional requirements for both the research reactor and the important I&C systems have been identified, the security classification for the I&C programmable digital systems that have an impact on nuclear safety can be defined. Consequences of a cyberattack on I&C programmable digital systems necessary to operate the plant cannot reach those of security degree S1 systems.

– I&C programmable digital systems where the consequence of a cyberattack could cause a severe degradation in, or loss of capability to an extent and duration that the research reactor cannot perform one of more of its primary objectives, or a number of secondary objectives, for an extended time may involve at least an intermediate security degree (S2),

– I&C programmable digital systems, where the consequence of a cyberattack could cause a degradation in, or loss of capability to an extent and duration that while the research reactor can perform its primary objective the operational capacity of the primary objective is reduced, or an inability to perform entirely a secondary objective, may be assigned to a less stringent and third security degree (S3).

F.1.5 Considerations on requirements associated to security degrees

As indicated research reactors have a wide variety of operational objectives. Some of these objectives may complicate the application of security requirements to I&C programmable digital systems as their addition might inhibit the research reactors ability to achieve their objectives.

For example, the research reactor may be collocated with other facilities and instruments that require a level of signalling between digital systems assigned to different security degrees to ensure there are no adverse impacts to radiation safety. Other research reactors might provide a less restricted access to digital I&C programmable systems to achieve their operational objective of education and training.

Note that this is only the case for systems classified at an intermediate (S2) or less stringent security degree (S3). I&C programmable systems that have been classified at most stringent security degree (S1) should not diverge from the security requirements.

Moreover, generic security requirements (valid for all security degrees, see 5.4.3.2.4) are relevant for all systems.

It is important that in each of these cases a graded approach is taken and level of defence in depth is applied to ensure that the possible impacts of diverging from the security requirements are minimised.

F.2 Applicability of IEC 62645 security graded approach to fuel cycle facilities

Text to be inserted if relevant content provided.

F.3 Applicability of IEC 62645 security graded approach to SMR

Text to be inserted if relevant content provided.

F.4 Reference documents

[1] IAEA Safety Standards, *Use of a Graded approach in the Application of the Safety Requirements for Research Reactors*, SSG-22, Vienna, Austria, 2012

[2] G. Zuying, L. Baoyan, "Safety Analysis of Accident Scenarios for the HTR-10", *Tsinghu Science and Technology*, March 1996, Vol. 1 , pp. 27—3
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6078139

[3] H. Böck, A. Musilek, M. Villa , *Research Reactors in Austria – Present Situation*, IAEA, 2005,
http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/36/069/36069526.pdf

Annex G
(informative)

High-level correspondence table between IEC 62443 series and IEC 62645

IEC 62645		IEC 62443		
Subclause		**Part**	**Subclause**	
5.1	**Context of the organization**			
5.1.1	Understanding the organization and its context	2-1	4.1.2.2	Security program implementation
5.1.2	Understanding the needs and expectations of interested parties	2-1	4.1.2.3	Organizational Interfaces
5.1.3	Determining the scope of the I&C programmable digital system security programme	2-1	4.1.2.1	Determining the scope of the ISMS
5.2.1	I&C digital programmable system security program	2-1	5.2.1	Security management system
5.2.2	Policy	2-1	5.2	Security related organization and policies
5.3	**Leadership**			
5.3.1	Leadership and commitment	2-1	4.1.2.2	Security program implementation
5.3.2	Roles, responsibilities and authorities	2-1	5.2.3	Security roles and responsibilities
5.4.1	Cybersecurity objectives and planning to achieve them	2-1	4.1.2.2	Security program implementation
5.4.2	Addressing risks and opportunities of the programme	2-1	4.2	Maturity model
5.4.3(.2.2)	Graded approach to I&C security and risk assessment	2-1	4.3	Security levels
5.5	Planning of the programme	2-1	4.2	Maturity model
5.5.2 & .3	Graded approach to I&C security and risk assessment	2-1	4.1.2.1	Risk mitigation
5.5	**Support**			
5.5.1	Resources	2-1	5.2.3	Security roles and responsibilities
5.5.2.2	Competence	1-1 1-5	4.7.1 4.2	People People, technology, and process
5.5.2.3	Awareness	1-1	4.7.1	People
5.5.3	Communications	1-1	4.7.2	Processes
5.5.4	Documented information	1-3	4.3.2	Collect, analyze and report metrics
5.6	**Operation**			
5.6.1	Operation planning and control	1-1	8.3.4.3	Operations and maintenance phase
5.6.2	Cybersecurity graded approach, risk assessment and risk treatment	4-2	3.3	Conventions
5.7	**Performance evaluation**			
5.7.1	Monitoring, measurement, analysis and evaluation	1-3	4.3.2	Collect, analyze and report metrics
5.7.2.2	Internal audit	1-1	A, 8.3.4.3	Annex A- Policies and procedures, Operations and maintenance phase
5.8	**Improvement**			
5.8.2	Non conformity and corrective action	1-1	7.6	Timely response to events
5.8.3	Continual improvement	1-3	4.3.3	Continuously improve measures

IEC 62645		IEC 62443		
Subclause		**Part**	**Subclause**	
Clause 6	**Lifecycle Implementation for I&C programmable digital system security**	1-1	8.3	Lifecycles
6.1	General	1-1	8.3.1	Introduction
6.2	System requirements specification	1-1	8.3.2	Requirements and design
6.3	System specification	1-1	8.3.4.1	Specification phase
6.4	System detailed design and implementation	1-1	8.3.2	Requirements and design
6.5	System integration	1-1	8.3.4.2	Integration and commissioning phase
6.6	System validation	1-1	8.3.4.2	Integration and commissioning phase
6.7	System installation	1-1	8.3.4.2	Integration and commissioning phase
6.8	Operation and maintenance activities	1-1	8.3.4.3	Operations and maintenance phase
6.9	Retirement activities	1-1	8.3.4.4	Decommissioning phase
Clause 7	**Security controls**	3-3		**System security requirements and security levels**

Bibliography

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

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

IAEA (International Atomic Energy Agency), Nuclear Security Series No. 23-G (NSS 23-G), *Security of nuclear information*, Vienna, 2015

IAEA (International Atomic Energy Agency), Safety Standards Series No. SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, Vienna, 2016

IAEA (International Atomic Energy Agency), Nuclear Security Series No. 33-T (NSS 23-G), *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, Vienna, 2018

IAEA NSS 17, Reference Manual, *Computer Security at Nuclear Facilities,* 2011

NIST SP 800-53, Rev. 4, *Recommended Security Controls for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, MD, 2013

NIST SP 800-82, Rev. 2, *Guide to Industrial Control Systems (ICS) Security – Computer security,* National Institute of Standards and Technology, Gaithersburg, MD, 2015

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

U.S. Nuclear Regulatory Commission Interim Staff Guidance DI&C-ISG-04, *Task Working Group #04 – Highly Integrated Control Rooms – Communications Issues (HICRc)*

Nuclear Energy Institute, NEI 08-09, R6, *Cyber Security Plan for Nuclear Power Reactors*

Swedish Emergency Management Agency, nr 0451/2008, *Guide to Increased Security in Process Control Systems for Critical Societal Functions*

CPNI (Centre for the Protection of National Infrastructure), *Process control and SCADA security – Good practice guidelines*, 2008

SOMMAIRE

AVANT-PROPOS 57
INTRODUCTION 59
1 Domaine d'application 62
1.1 Généralités 62
1.2 Application 63
1.3 Cadre général 63
2 Références normatives 66
3 Termes et définitions 66
4 Termes abrégés 71
5 Établissement et gestion d'un programme de sécurité des systèmes numériques programmables d'I&C 72
5.1 Contexte de l'organisation 72
5.1.1 Compréhension de l'organisation et de son contexte 72
5.1.2 Compréhension des besoins et des attentes des parties intéressées 72
5.1.3 Détermination du domaine d'application du programme de sécurité du système numérique programmable d'I&C 72
5.2 Programme, politique et plan 72
5.2.1 Programme de sécurité des systèmes numériques programmables d'I&C 72
5.2.2 Politique 73
5.2.3 Plan 73
5.3 Leadership 73
5.3.1 Leadership et engagement 73
5.3.2 Rôles, responsabilités et autorités 74
5.4 Planification du programme 75
5.4.1 Objectifs de cybersécurité et plans pour les atteindre 75
5.4.2 Traitement des risques et opportunités du programme 75
5.4.3 Approche graduée de la sécurité de l'I&C et de l'évaluation des risques 75
5.5 Support 84
5.5.1 Ressources 84
5.5.2 Formation, compétences et sensibilisation 84
5.5.3 Communication relative à la cybersécurité 84
5.5.4 Informations documentées 84
5.6 Exploitation 85
5.6.1 Planification et contrôle opérationnels 85
5.6.2 Approche graduée de la cybersécurité, évaluation des risques et traitement des risques 85
5.7 Évaluation des performances 85
5.7.1 Surveillance, mesurages, analyse et évaluation 85
5.7.2 Audit interne 86
5.7.3 Revue de direction 86
5.8 Amélioration 86
5.8.1 Généralités 86
5.8.2 Non-conformité et actions correctives 86
5.8.3 Amélioration continue 87
6 Mise en œuvre du cycle de vie pour la sécurité des systèmes numériques programmables d'I&C 87

6.1 Généralités 87
6.2 Spécification des exigences relatives au système 87
6.2.1 Généralités 87
6.2.2 Attribution du degré de sécurité 87
6.3 Spécification du système 87
6.3.1 Sélection des composants préexistants 87
6.3.2 Architecture du système 88
6.4 Conception détaillée et mise en œuvre du système 88
6.4.1 Généralités 88
6.4.2 Évaluation des risques au niveau de la phase de conception 88
6.4.3 Plan de sécurité du projet de conception 89
6.4.4 Chemins de communication 89
6.4.5 Définition des zones de sécurité 89
6.4.6 Évaluation de la sécurité de la conception finale 90
6.4.7 Activités de mise en œuvre 90
6.5 Intégration du système 90
6.6 Validation du système 90
6.7 Installation du système 91
6.8 Activités d'exploitation et de maintenance 91
6.8.1 Contrôle des modifications durant l'exploitation et la maintenance 91
6.8.2 Réévaluations périodiques des risques et des mesures de sécurité 91
6.8.3 Gestion des modifications 91
6.9 Activités liées au retrait d'exploitation 92
7 Mesures de sécurité 92
7.1 Généralités 92
7.2 Caractérisation 92
7.3 Défense en profondeur de la sécurité 93
7.4 Choix et mise en exécution des mesures de cybersécurité 93
Annexe A (informative) Justifications et notes relatives au domaine d'application du présent document 95
A.1 Objet de la présente Annexe 95
A.2 Inclusion des systèmes numériques programmables d'I&C non importants pour la sûreté 95
A.3 Exclusion des systèmes de sécurité physique, de contrôle d'accès aux salles de commande et de surveillance sécuritaire du site 95
A.4 Exclusion des actions et événements non malveillants 95
A.5 Outils et plateformes de développement 96
Annexe B (informative) Considérations générales par rapport aux degrés de sécurité 97
B.1 Raisons sous-jacentes au choix de trois degrés de sécurité 97
B.1.1 Généralités 97
B.1.2 Catégories de sûreté prises comme données d'entrée pour l'attribution du degré de sécurité 97
B.1.3 Dégradation de la disponibilité et des performances de la centrale prise comme donnée d'entrée pour l'attribution des degrés de sécurité 98
B.1.4 Approche d'attribution du degré de sécurité en résultant 98
B.2 Considération sur les outils associés aux systèmes en ligne 98
B.3 Conception pratique et mise en œuvre 98
Annexe C (informative) Correspondance avec l'ISO/IEC 27001:2013 100
Annexe D (informative) Organisation d'ensemble des normes du SC 45A de l'IEC liées à la cybersécurité 102

Annexe E (informative) Choix des mesures de sécurité 104
Annexe F (informative) Considérations concernant l'applicabilité de l'IEC 62645 aux installations nucléaires hors centrales nucléaires de puissance 106
F.1 Applicabilité de l'approche graduée de sécurité de l'IEC 62645 aux réacteurs de recherche 106
F.1.1 Généralités 106
F.1.2 Catégorisation des réacteurs de recherche conformément aux dangers potentiels 106
F.1.3 Catégories de sûreté prises comme données d'entrée pour l'attribution du degré de sécurité 107
F.1.4 Impact sur la capacité opérationnelle pris comme donnée d'entrée pour l'attribution du degré de sécurité 108
F.1.5 Considérations relatives aux exigences associées aux degrés de sécurité 108
F.2 Applicabilité de l'approche graduée de sécurité de l'IEC 62645 pour les installations du cycle du combustible 109
F.3 Applicabilité de l'approche graduée de sécurité de l'IEC 62645 pour les petits réacteurs modulaires 109
F.4 Documents de référence 109
Annexe G (informative) Tableau de correspondances de haut niveau entre la série IEC 62443 et l'IEC 62645 110
Bibliographie 112

Figure 1 – Cadre général de l'IEC 62645 65
Figure 2 – Elément E/E/PE 69
Figure D.1 – Vue d'ensemble des normes du SC 45A de l'IEC liées à la cybersécurité 103
Figure E.1 – Choix des mesures de sécurité 105

Tableau C.1 – Correspondance entre l'ISO/IEC 27001:2013 et l'IEC 62645 100
Tableau F.1 – Correspondance entre les catégories de sûreté et les classes selon l'IEC 61513 107

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

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

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

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

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

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

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

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

FDIS	Rapport de vote
45A/1289/FDIS	45A/1295/RVD

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

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

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

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

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

INTRODUCTION

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

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

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

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

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

L'IEC 62645 est le document de deuxième niveau du SC 45A de l'IEC qui traite de la question générale de la cybersécurité des systèmes d'I&C utilisés dans des centrales nucléaires de puissance.

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

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

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

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

Il est reconnu que la présente norme couvre le domaine des exigences réglementaires en la matière qui est en pleine évolution, ceci étant dû à la nature changeante et évolutive des menaces liées à la sécurité informatique. Ainsi, la présente norme définit un cadre de travail dans lequel les exigences nationales particulières susceptibles d'évoluer peuvent être élaborées et appliquées.

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

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

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

L'IEC 61513 et l'IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation, la défense contre les défaillances de cause commune, la conception des salles de commande, la compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec l'IEC 61513 et l'IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont pas référencées directement par l'IEC 61513 ou l'IEC 63046, sont relatives à des matériels particuliers, à des méthodes techniques ou à des activités spécifiques. Généralement, ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

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

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

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

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

NOTE 1 Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les dangers chimiques et la prévention contre les dangers liés au procédé énergétique) des normes nationales ou internationales sont appliquées.

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

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

1 Domaine d'application

1.1 Généralités

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

Le présent document définit les mesures adéquates pour ce qui concerne la prévention, la détection et la réaction à des actes malveillants, réalisés en utilisant des moyens informatiques (cyberattaques), portant atteinte aux systèmes numériques programmables d'I&C. Ceci comprend les situations non sûres, les endommagements d'équipements ou la dégradation des performances de la centrale qui pourraient résulter d'une telle action, par exemple:

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

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

Le présent document décrit un schéma d'approche graduée pour les actifs susceptibles d'être compromis sur le plan numérique, prenant en compte leur importance au niveau de la sûreté de l'ensemble de l'installation, de sa disponibilité et de la protection des équipements.

Les considérations suivantes sont exclues du domaine du présent document:

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

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

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

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

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

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

Les normes telles que l'ISO/IEC 27001 et l'ISO/IEC 27002 ne sont pas directement applicables pour la cyberprotection des systèmes numériques programmables d'I&C du nucléaire. Ceci est principalement dû à l'existence de spécificités propres à ces systèmes, qui comprennent les exigences de sûreté et réglementaires inhérentes aux installations nucléaires. Cependant, le présent document, construit sur les principes pertinents de haut niveau et les principaux concepts de l'ISO/IEC 27001:2013, les adapte et les complète pour qu'ils s'accordent au contexte nucléaire.

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

1.2 Application

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

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

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

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

1.3 Cadre général

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

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

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

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

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

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

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

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

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

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

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

La Figure 1 représente le cadre général du présent document.

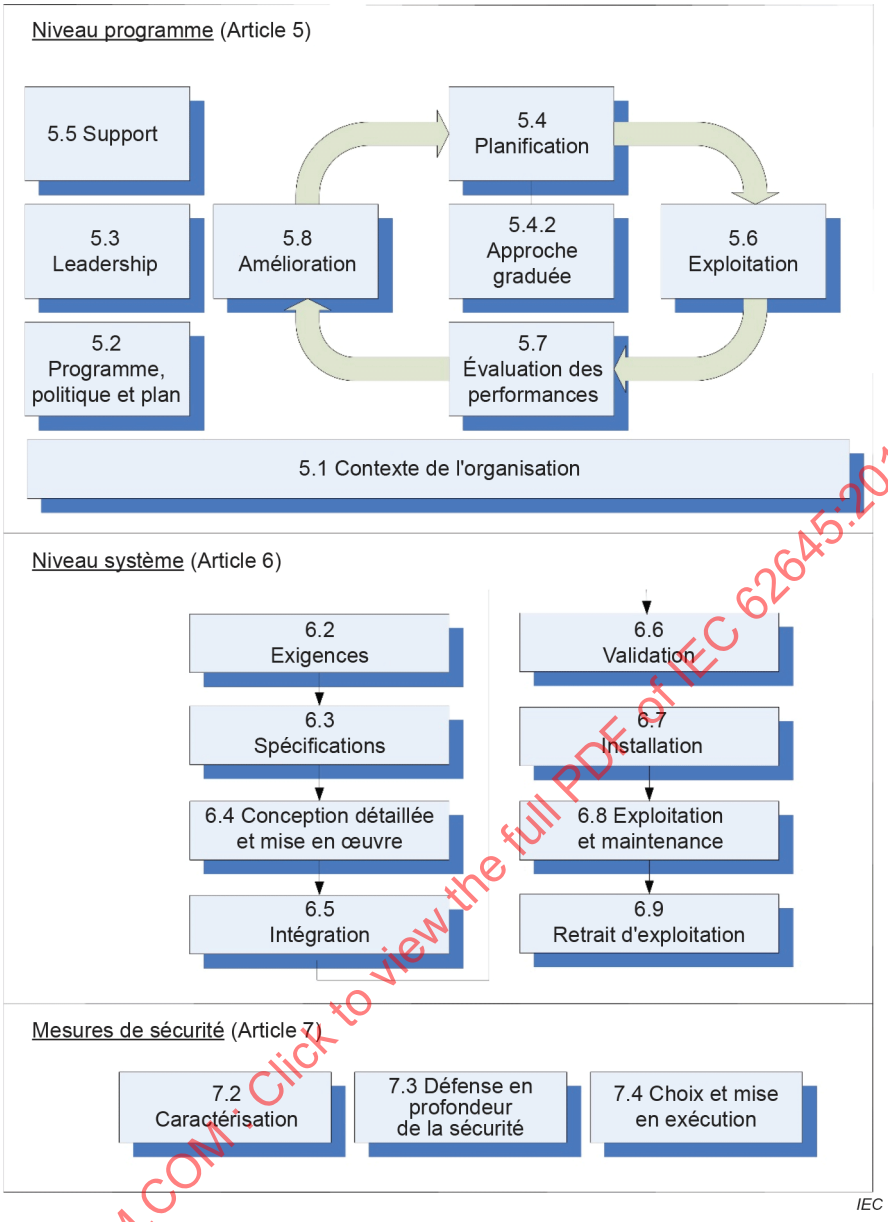


Figure 1 – Cadre général de l'IEC 62645

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

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

Le présent document traite aussi des exigences de sécurité portant sur les systèmes numériques programmables d'I&C qui sont hors des domaines d'application des normes IEC 61513, IEC 60880, IEC 62138 et IEC 62566, mais qui peuvent avoir un impact possible sur les équipements de la centrale, sa disponibilité et ses performances.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

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

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

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

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

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

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

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

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

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

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

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
vecteur d'attaque
chemin ou moyen par lequel un programme malveillant ou attaquant peut avoir accès à un système informatisé

3.2
autorisation
fonction de spécification des droits d'accès aux ressources, qui est liée en général à la sécurité de l'information et à la sécurité informatique, et en particulier au contrôle d'accès

3.3
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

Note 1 à l'article: Cette définition est différente de celle utilisée dans les autres normes de l'IEC dans le domaine des systèmes d'instrumentation et de contrôle-commande des installations nucléaires, qui est la suivante:"Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné en supposant que la fourniture des moyens nécessaires est assurée".

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

3.4
élément informatisé
élément qui s'appuie sur des instructions logicielles s'exécutant sur des microprocesseurs ou des microcontrôleurs

Note 1 à l'article: Dans ce terme et sa définition le mot "élément" peut être remplacé par les mots "système", "équipement" ou "dispositif".

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

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

Note 4 à l'article: Dans la traduction française des normes du SC 45A, les termes "informatique" et "informatisé" sont équivalents.

[SOURCE: IEC 62138:2018, 3.8]

3.5
confidentialité
propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes ou à des entités ou des processus non autorisés

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

3.6
cyberattaque
actes malveillants réalisés par des moyens numériques

3.7
cybersécurité
ensemble d'activités et de mesures dont l'objectif est d'empêcher, de détecter et de réagir aux attaques digitales dont l'intention est d'entraîner:

– les modifications malveillantes (intégrité) de fonctions pouvant porter atteinte à la fourniture ou à l'intégrité d'un service exigé par des systèmes numériques programmables d'I&C (y compris la perte de contrôle) qui pourraient avoir pour conséquence un accident, l'apparition d'une situation non sûre ou une dégradation des performances de la centrale;

– la rétention ou la prévention malveillante pour l'accès à ou la communication d'informations, de données ou de ressources (y compris la perte de visibilité) qui pourraient compromettre la fourniture par un système d'I&C (disponibilité) d'un service demandé qui pourrait avoir pour conséquence un accident, l'apparition d'une situation non sûre ou une dégradation des performances de la centrale;

– la divulgation malveillante d'informations (confidentialité) qui pourraient être utilisées pour réaliser des actes malveillants qui pourraient amener à un accident, une situation non sûre ou dégrader les performances de la centrale.

Note 1 à l'article: Cette définition est établie par rapport au domaine d'application de l'IEC 62645 et à la structure d'ensemble des documents du SC 45A. Il est reconnu que le terme "cybersécurité" a un sens plus large au niveau des autres normes et recommandations, qui couvre souvent les menaces non malveillantes, les erreurs humaines et la protection contre les risques naturels. Ces aspects – à l'exception des erreurs humaines qui dégradent la cybersécurité – ne sont pas couverts par le concept de cybersécurité défini par la série de normes du SC 45A. Voir l'Annexe A pour plus de détails sur ces exclusions.

Note 2 à l'article: Sécurité informatique, sécurité et cybersécurité sont considérées comme synonymes dans le présent document.

3.8
conception
processus consistant à élaborer le projet et les plans détaillés, exécuter les calculs préparatoires et établir les spécifications d'une installation et de ses parties, et résultat de ce processus

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2007]

3.9
menace de référence
DBT
attributs et caractéristiques d'attaquants internes et/ou externes qui peuvent tenter de subtiliser des matériaux nucléaires de façon non autorisée ou un sabotage, et contre lesquels un système de protection physique a été conçu et évalué

Note 1 à l'article: Les cyberattaques et les attaquants associés ne sont pas considérés d'une façon équivalente dans les menaces de référence, cela dépend des approches nationales et des cadres légaux. De plus, le contenu des menaces de référence pour le nucléaire est traité comme très confidentiel.

Note 2 à l'article: L'abréviation "DBT" est dérivée du terme anglais développé correspondant "Design Basis Threat".

[SOURCE: AIEA INFCIRC/225/Rév.4:1999, modifié: notes 1 et 2 ajoutées]

3.10
élément électrique/électronique/électronique programmable
élément E/E/PE
élément réalisé à base de technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (PE)

Note 1 à l'article: Dans ce terme et sa définition, le mot "élément" peut être remplacé par les mots "système", "équipement" ou "dispositif".

Note 2 à l'article: Les définitions des termes liés à la technologie: élément E/E/PE, élément numérique programmable, élément câblé, élément à logique programmable sont totalement coordonnées et cohérentes. Les relations entre les termes élément E/E/PE, élément câblé, élément numérique programmable, élément informatisé, élément à logique programmable sont indiquées par la Figure 2.

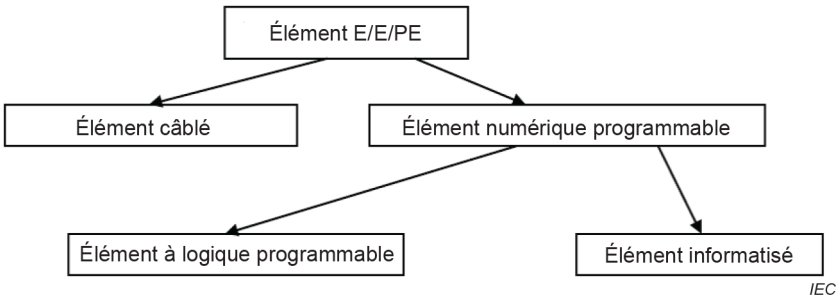


Figure 2 – Elément E/E/PE

[SOURCE: IEC 62138:2018, 3.15]

3.11
circuit intégré programmé en HDL
HPD
circuit intégré configuré (pour des systèmes d'I&C de centrales nucléaires de puissance) avec des HDL 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 (réseaux de portes programmables sur site) ou des technologies microélectroniques similaires.

Note 4 à l'article: Les HPD sont des types d'éléments à logique programmable.

Note 5 à l'article: Voir aussi la définition d'élément E/E/PE et les notes associées.

Note 6 à l'article: L'abréviation "HPD" est dérivée du terme anglais développé correspondant "HDL-Programmed Device".

[SOURCE: IEC 62566:2012, 3.7]

3.12
fonction d'I&C
fonction permettant de commander, exploiter et/ou surveiller une partie définie du procédé

[SOURCE: IEC 61513:2011, 3.28]

3.13
système d'I&C
système réalisé sur la base d'éléments E/E/PE, exécutant des fonctions d'I&C de la centrale ainsi que des fonctions de service et de surveillance liées au fonctionnement du système lui-même

Note 1 à l'article: Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les interfaces vers les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

Note 2 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 3 à l'article: Voir aussi "système d'alimentation électrique". Les termes "système d'alimentation électrique" et "système d'I&C" sont liés à la fonction principale réalisée par chacun de ces systèmes; respectivement, "la production, la transmission et la distribution électriques" et "le mesurage, la protection, la régulation et l'IHM liés au procédé de la centrale nucléaire de puissance". Ces termes doivent être considérés ensemble, ils sont totalement consistants et cohérents avec les exigences générales établies par l'IEC 61513 et l'IEC 63046 pour les systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des centrales nucléaires de puissance.

Note 4 à l'article: Voir aussi la définition d'élément E/E/PE et les notes associées.

Note 5 à l'article: Selon leurs fonctionnalités propres, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection.

[SOURCE: IEC 62138:2018, 3.26]

3.14
intégrité
propriété de protection de l'exactitude et de la complétude des actifs

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013 et ISO/IEC 27000:2018, 2.40]

3.15
élément 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: Voir aussi la définition d'élément E/E/PE et les notes associées.

Note 3 à l'article: Les principaux éléments numériques programmables sont les éléments informatisés et les éléments à logique programmable.

Note 4 à l'article: Ce terme utilisé par l'IEC SC 45A équivaut au terme "élément électronique programmable" (élément PE) utilisé dans l'IEC 61508.

[SOURCE: IEC 62138:2018, 3.35]

3.16
risque
possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un dommage à l'organisation

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

3.17
évaluation des risques
processus général de détermination, d'estimation, d'analyse et d'évaluation systématiques des risques

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

3.18
mesure de sécurité
moyen de gestion de sécurité qui peut être administratif, technique ou physique

3.19
degré de sécurité
niveau de protection de sécurité correspondant à un ensemble d'exigences, attribué à un système en prenant en compte les conséquences maximales que pourrait avoir sur le système une cyberattaque qui aboutirait, au niveau des performances et de la sûreté de l'installation

Note 1 à l'article: Trois degrés de sécurité sont définis en 5.2.3 et correspondent à S1, S2 et S3. Le comportement conduisant à l'utilisation de trois degrés de sécurité pour les systèmes numériques programmables d'I&C est présenté à l'Annexe B. Le présent document traite seulement des systèmes numériques programmables d'I&C et ne fait pas d'hypothèses supplémentaires concernant les degrés de sécurité pour les autres types de systèmes. Les systèmes qui ne font pas partie de l'I&C (par exemple les ordinateurs de bureau) peuvent être assignés à des degrés de sécurité différents/complémentaires, amenant à une approche graduée présentant plus

de trois degrés de sécurité lorsque la centrale est considérée de manière globale. De plus, certaines pratiques nationales impliquent la sous-division du degré de sécurité.

Note 2 à l'article: Le terme "degré de sécurité" a été préféré à "niveau de sécurité" pour éviter des confusions possibles avec les niveaux d'I&C, concept communément utilisé dans d'autres normes et dans les pratiques industrielles.

3.20
programme de sécurité
ensemble d'éléments liés ou en interaction d'une organisation visant à établir des politiques et objectifs de sécurité, ainsi que des processus et des plans de sécurité visant à atteindre ces objectifs

Note 1 à l'article: Le programme est un concept similaire à celui de "système de management" défini dans l'ISO/IEC 27000:2018.

Note 2 à l'article: Le programme de sécurité informatique, le programme de cybersécurité et le programme de sécurité sont considérés comme synonymes dans le présent document.

3.21
zone de sécurité
concept permettant de regrouper des systèmes informatisés d'I&C à des fins de gestion, de communication et d'application de mesures de protection

Note 1 à l'article: Les zones de sécurité correspondent à la mise en œuvre pratique et architecturale d'une approche graduée. Leur nombre n'est pas limité. Elles peuvent être logiques et/ou physiques. Il n'y a pas de correspondance directe avec le concept de zone de sûreté et des séparations géographiques associées.

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

3.22
menace
cause potentielle d'un incident indésirable, qui peut nuire à un système ou à une organisation

Note 1 à l'article: Dans le cadre du présent document (voir 1.1), les événements ou la survenance d'événements sont limités à ceux qui sont malveillants et aux erreurs humaines compromettant la cybersécurité – ce qui ne couvre pas les aspects accidentels (par exemple les risques naturels, les erreurs humaines n'affectant pas la cybersécurité), couverts par d'autres documents de l'IEC dans le domaine des systèmes d'instrumentation et de contrôle-commande des installations nucléaires.

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

3.23
vulnérabilité
faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une menace

[SOURCE: Collection de sécurité nucléaire de l'AIEA No. 17:2013]

4 Termes abrégés

CB	Computer-Based (informatique)
EIUI	Équipe d'intervention en cas d'urgence informatique
RSSI	Responsable sécurité des systèmes d'information
DBT	Design Basis Threat (Menace de référence)
HDL	Hardware Description Language (Langage de description de matériel)
CVC	Chauffage, ventilation et conditionnement de l'air
SMSI	Système de management de la sécurité de l'information
I&C	Instrumentation et contrôle-commande
CNP	Centrale nucléaire de puissance

PLC Programmable logic controller (Automate programmable)

PSP Plan de sécurité du projet

AQ Assurance qualité

V&V Vérification et validation

5 Établissement et gestion d'un programme de sécurité des systèmes numériques programmables d'I&C

5.1 Contexte de l'organisation

5.1.1 Compréhension de l'organisation et de son contexte

Le contenu du 4.1 de l'ISO/IEC 27001:2013 s'applique.

5.1.2 Compréhension des besoins et des attentes des parties intéressées

Le contenu du 4.2 de l'ISO/IEC 27001:2013 s'applique

5.1.3 Détermination du domaine d'application du programme de sécurité du système numérique programmable d'I&C

Le contenu du 4.3 de l'ISO/IEC 27001:2013 s'applique.

Le domaine d'application et les limites du programme de sécurité doivent notamment être définis en fonction des caractéristiques de l'organisation de la centrale nucléaire de puissance, son emplacement, ses exigences réglementaires nationales, ses actifs numériques programmables d'I&C et sa technologie, et des risques engendrés par l'exploitation du système. Le programme de sécurité doit comprendre des détails et justifications concernant les exclusions/modifications par rapport au domaine d'application.

5.2 Programme, politique et plan

5.2.1 Programme de sécurité des systèmes numériques programmables d'I&C

5.2.1.1 Le contenu du 4.4 de l'ISO/IEC 27001:2013 s'applique.

5.2.1.2 Le programme de sécurité d'I&C doit être développé sur la base d'une évaluation des risques et prendre en compte la politique et les recommandations établies par les concepteurs, les autorités réglementaires nationales et les politiques et procédures propres à la centrale pour mettre en œuvre le programme de sécurité.

5.2.1.3 Des programmes de sécurité doivent être mis en œuvre par l'utilisation de politiques et procédures documentées approuvées par le personnel en charge des programmes de sécurité.

5.2.1.4 Une coordination correcte entre les aspects de sûreté et de cybersécurité doit être assurée. Des exigences et recommandations à cet égard se trouvent dans l'IEC 62859.

5.2.1.5 Un programme de sécurité des systèmes numériques programmables d'I&C d'une centrale nucléaire de puissance doit comprendre les activités suivantes:

a) définition des responsabilités et de l'organisation liées à la sécurité informatique et du processus d'examens périodiques;

b) développement du processus de désignation des actifs sujets aux mesures de protection de sécurité informatique comprenant les systèmes informatisés, les applications des systèmes informatisés et les connexions réseaux;

c) mise en œuvre des méthodes de gestion du personnel pour les aspects liés à la sécurité informatique et à la sécurité des systèmes numériques programmables d'I&C, ceci comprenant la formation, la qualification des personnes et leur départ ou leur transfert;

d) développement et conduite du processus d'évaluation des risques, prenant en compte les menaces de référence (DBT) particulières au pays telles qu'applicables, pour l'architecture d'I&C dans son ensemble comme pour chaque système d'I&C;

e) conduite de l'évaluation du risque résiduel qui est transféré/accepté, de la conception à l'exploitation;

f) définition des principes fondamentaux d'architecture et de conception et des exigences pour la conception de la sécurité des systèmes et la gestion des configurations pour les systèmes de la centrale et du support fournisseur exigés pour maintenir les fonctionnalités de cybersécurité prévues à la conception;

g) identification des procédures de sécurité en exploitation pour le contrôle d'accès, la sécurité des données, la sécurité des communications, la sécurité des applications et des plateformes, la surveillance système, la maintenance et les modifications de la sécurité des systèmes informatisés et la prise en charge des incidents relatifs à la sécurité;

h) en particulier, la définition du processus d'évaluation des composants sur étagère, au niveau matériel comme logiciel pour garantir autant qu'il est raisonnablement possible qu'ils ne contiennent pas de fonctionnalité ou de logiciel malveillant;

i) élaboration des exigences portant sur la préparation et la formalisation, du point de vue de la sécurité, pour la remise du matériel, des données, du logiciel, des codes ou des informations entre les différents sites de conception, ou entre un concepteur et une tierce partie, ou entre le concepteur et l'entreprise productrice d'électricité.

5.2.2 Politique

5.2.2.1 Le contenu du 5.2 de l'ISO/IEC 27001:2013 s'applique.

5.2.2.2 Une politique de sécurité informatique doit définir les objectifs de sécurité informatique de haut niveau applicables pour l'installation nucléaire.

5.2.2.3 Les exigences de la politique de sécurité pour les systèmes numériques programmables d'I&C doivent être déclinées dans des documents de niveau inférieur, qui sont utilisés pour mettre en œuvre cette politique et la contrôler.

5.2.2.4 Ces exigences doivent être:

a) mesurables,

b) réalisables,

c) atteignables.

5.2.3 Plan

Le plan de sécurité des systèmes numériques programmables d'I&C doit:

a) être la mise en œuvre de cette politique sous la forme de procédures, de responsabilités et de rôles organisationnels,

b) définir et détailler les moyens permettant d'atteindre les objectifs de sécurité,

c) contenir les actions principales à entreprendre et les réponses associées en matière de détection et de prévention d'intrusion, d'évaluation des conséquences et de contre-mesures nécessaires pour atténuer les conséquences.

5.3 Leadership

5.3.1 Leadership et engagement

Le contenu du 5.1 de l'ISO/IEC 27001:2013 s'applique.

5.3.2 Rôles, responsabilités et autorités

5.3.2.1 La première exigence du 5.3 de l'ISO/IEC 27001:2013 s'applique.

5.3.2.2 La deuxième exigence du 5.3 de l'ISO/IEC 27001:2013 s'applique.

5.3.2.3 La gestion du programme des systèmes numériques programmables d'I&C doit garantir que toutes les questions nécessaires de sécurité informatique sont prises en compte de façon programmée dans le plan et les procédures de sécurité informatique et qu'elles satisfont aux exigences réglementaires et à celles de l'entreprise.

5.3.2.4 Le programme des systèmes numériques programmables d'I&C doit être coordonné avec le programme de sécurité de l'entreprise et le cadre de la politique en vigueur pour le site, ses programmes, ses pratiques et ses procédures, le cas échéant.

5.3.2.5 La mise en œuvre d'un programme de sécurité pour les systèmes numériques programmables d'I&C permanent doit se faire en intégrant ou interfaçant étroitement des spécialistes des systèmes d'I&C, des spécialistes de la sécurité informatique et des spécialistes de la sécurité physique.

5.3.2.6 Durant les phases de conception et de développement, il est probable que différentes entreprises soient responsables du développement de différents systèmes d'I&C. Le concepteur doit clairement définir les obligations des fournisseurs d'I&C en ce qui concerne la sécurité informatique et il doit vérifier que celles-ci sont respectées.

5.3.2.7 Toutes les organisations impliquées à quelque niveau que ce soit du cycle de vie du développement des systèmes numériques programmables d'I&C doivent documenter les structures organisationnelles et les responsabilités associées à chaque emploi venant soutenir le programme de sécurité informatique pour ces systèmes. Les procédures de communication entre toutes les organisations impliquées doivent être documentées (en particulier entre les différentes entités juridiques), et aussi celles entre les équipes à l'intérieur des organisations et des entreprises.

5.3.2.8 Pour développer, approuver et mettre en œuvre un programme de sécurité pour les systèmes numériques programmables d'I&C, le personnel de direction de la centrale doit, en coopération avec le concepteur d'I&C, imposer:

a) les exigences de sécurité de l'entreprise productrice d'électricité,

b) la politique de sécurité interne de l'entreprise,

c) le cadre juridique national,

d) le cadre réglementaire national,

e) les meilleures pratiques industrielles en matière de sécurité informatique et de sécurité pour les systèmes numériques programmables d'I&C,

f) l'état des menaces actuelles et de celles prédictibles liées au secteur de l'industrie nucléaire et aux autres secteurs industriels utilisant les équipements d'I&C utilisés dans les centrales nucléaires,

g) l'élaboration de canaux d'information pour mettre à jour en permanence l'état des menaces actuelles et de celles prédictibles liées au secteur de l'industrie nucléaire et aux autres secteurs industriels utilisant les équipements d'I&C utilisés dans les centrales nucléaires.

5.3.2.9 La surveillance générale de la sécurité des systèmes numériques programmables d'I&C doit être affectée à une ou des personnes par rapport à un ou des emplois dans l'organisation avec des responsabilités définies précisément. Le présent document fait référence au rôle du ou des Responsables sécurité des systèmes d'information (RSSI), ou équivalent. La responsabilité du RSSI doit couvrir:

a) le conseil à l'équipe de direction de l'entreprise et/ou du projet;

b) la coordination et le contrôle du développement des activités de sécurité informatique;

c) la coordination de la sécurité informatique avec les autres aspects de la sécurité et de la sûreté;

d) la garantie que le programme de sécurité informatique prend en compte l'exploitation et la maintenance de la centrale et ne porte pas atteinte par inadvertance aux systèmes importants pour la sûreté;

e) l'identification et la documentation des systèmes qui sont critiques pour le maintien de la sécurité informatique de l'installation;

f) la conduite d'évaluations des risques liés à la sécurité informatique;

g) la conduite d'inspections, d'audits et de revues périodiques de sécurité, et la fourniture de rapports d'état à l'équipe de direction;

h) le développement et la mise en œuvre d'un processus d'évaluation et de formation à la sécurité informatique;

i) le développement d'une stratégie, couvrant les procédures et les aspects formation, pour identifier les incidents relevant potentiellement de la cybersécurité;

j) l'élaboration, le pilotage et la contribution aux réponses aux événements pertinents concernant la sécurité informatique, y compris la coordination avec les organisations internes et externes;

k) les investigations à mener par suite de la survenance d'incidents ou de l'identification de vulnérabilités et la définition de recommandations concernant les actions correctives.

5.3.2.10 Le RSSI peut être chargé de responsabilités supplémentaires particulières à l'organisation de l'entreprise, en plus de celles apparaissant dans la liste précédente. Il convient qu'une équipe multidisciplinaire disposant des ressources et de l'expertise exigées soit en charge de l'exécution des activités liées à ces responsabilités.

5.4 Planification du programme

5.4.1 Objectifs de cybersécurité et plans pour les atteindre

5.4.1.1 Le contenu du 6.2 de l'ISO/IEC 27001:2013 s'applique.

5.4.1.2 La cybersécurité ne doit pas interférer avec les objectifs de sûreté de la centrale et doit protéger leur accomplissement.

5.4.2 Traitement des risques et opportunités du programme

Le contenu du 6.1.1 de l'ISO/IEC 27001:2013 s'applique.

5.4.3 Approche graduée de la sécurité de l'I&C et de l'évaluation des risques

5.4.3.1 Schéma de classement

5.4.3.1.1 Généralités

5.4.3.1.1.1 La sécurité des systèmes numériques programmables d'I&C doit reposer sur une approche graduée. Un degré de sécurité doit être attribué à chaque système numérique programmable d'I&C. Le degré de sécurité d'un système numérique programmable d'I&C doit être attribué sur la base de l'évaluation des conséquences maximales d'une cyberattaque réussie sur ce système en matière de sûreté et de performances de la centrale (voir 5.4.3.1.3 pour les critères d'attribution détaillés). Des exigences graduées de sécurité sont définies pour chaque degré de sécurité (voir 5.4.3.2.4 à 5.4.3.2.8).

NOTE Dans le contexte du présent document, les performances de la centrale sont abordées depuis l'angle de la production d'électricité.

5.4.3.1.1.2 Le schéma de classement repose sur les principes suivants:

a) les conséquences d'une cyberattaque sur la sûreté doivent être considérées comme plus importantes que celles portant sur les performances de la centrale;

b) les systèmes doivent être pris en compte du point de vue fonctionnel et assignés à un degré de sécurité en fonction de l'impact potentiel direct ou indirect sur la sûreté de la centrale et ses performances. L'attribution d'un degré de sécurité à un système dépend de la fonction la plus sensible qu'il met en œuvre (c'est-à-dire la fonction qui conduit à l'impact le plus grave lorsqu'elle est manipulée ou perturbée de façon malveillante);

c) une telle approche d'attribution reposant sur les conséquences doit être rigoureuse et répétable, garantissant la reproductibilité et la cohérence de l'approche sécurité. Cette analyse doit prendre en compte la possibilité que d'autres systèmes d'I&C subissent la même attaque (par exemple des systèmes similaires situés dans des voies redondantes séparées).

5.4.3.1.1.3 Il convient que l'attribution du degré de sécurité soit faite le plus tôt possible dans le cycle de vie du système d'I&C.

5.4.3.1.1.4 L'attribution du degré de sécurité doit être documentée.

5.4.3.1.1.5 Une approche graduée de la sécurité telle que décrite par le présent document implique que:

a) le nombre d'interfaces entre systèmes assignés à différents degrés de sécurité doit être justifié;

b) des restrictions adaptées doivent être mises en œuvre aux interfaces entre systèmes appartenant à des degrés de sécurité différents.

5.4.3.1.1.6 L'évaluation des risques, comprenant une évaluation des vulnérabilités et des scénarios de menace, doit compléter l'analyse et peut amener à compléter les exigences de sécurité et à mettre en place des dispositions de sécurité complémentaires (voir 5.4.3.2.2).

5.4.3.1.2 Lien entre catégories de sûreté, classes de sûreté et degrés de sécurité

L'approche graduée de sécurité décrite dans le présent document a pour objectif de défendre la sûreté de la centrale et ses performances contre les cybermenaces, sur la base d'une analyse basée sur les conséquences.

La partie relative aux conséquences liées à la sûreté d'une telle analyse est déjà couverte du point de vue non malveillant par la conformité à l'IEC 61513 et à l'IEC 61226. Ainsi, le classement de sûreté découlant de l'application de l'IEC 61226 doit être utilisé comme une donnée d'entrée importante du processus d'attribution du degré de sécurité. La sécurité peut tirer profit des dispositions de sûreté mises en œuvre conformément aux exigences de l'IEC 61513 et des autres normes IEC pertinentes pour la sûreté.

Cependant, afin de prendre en compte les performances de la centrale et les pratiques nationales concernant la mise en œuvre de fonctions qui peuvent mettre en péril la sûreté en cas de cyberattaque, il n'y a pas de relation bijective entre les classes de sûreté et les degrés de sécurité des systèmes d'I&C.

5.4.3.1.3 Description des degrés de sécurité et des critères associés d'attribution

Le présent document définit trois degrés de sécurité, S1, S2 et S3, auxquels des exigences graduées de sécurité sont associées (comme cela est défini en 5.4.3.2). Ces trois degrés de sécurité sont définis comme suit:

a) Les fonctions et les systèmes doivent être analysés pour déterminer les conséquences maximales sur la sûreté de la centrale et ses performances (telles que définies en 5.4.3.1.1) en provenance d'actions ou d'événements malveillants les impliquant.

b) Cette analyse doit être documentée.

c) Les systèmes doivent être affectés aux degrés S1 (le plus strict) à S3 suivant ces conséquences maximales.

d) Il convient que les degrés de sécurité soient affectés aux systèmes numériques programmables d'I&C de la façon suivante:

   – les systèmes numériques programmables d'I&C réalisant des fonctions de catégorie A de sûreté sont de degré de sécurité S1,

   – les systèmes numériques programmables d'I&C réalisant des fonctions de catégorie B de sûreté et les systèmes numériques programmables d'I&C ayant un impact direct et immédiat sur la sûreté de la centrale ou sur l'exploitation principale du processus nucléaire sont d'un degré de sécurité qui n'est pas inférieur à S2,

   – les systèmes numériques programmables d'I&C réalisant des fonctions de catégorie C sont assignés au degré de sécurité S1, S2 ou S3 suivant le principe des conséquences maximales,

   – et les systèmes numériques programmables d'I&C d'aide à l'exploitation et à la maintenance de la centrale sont de degré de sécurité S3.

Comme indiqué en 5.4.3.1.2, il n'y a pas de relation bijective entre les catégories de sûreté et les degrés de sécurité. Par exemple, il est recommandé de classer les systèmes numériques programmables d'I&C ayant un impact direct et immédiat sur la sûreté de la centrale ou sur l'exploitation principale du processus nucléaire au degré de sécurité S2 sans prendre en compte leur catégorie de sûreté; de plus, il est possible d'assigner à un degré de sécurité supérieur des systèmes non classés de sûreté (même si le point e) s'applique). En plus de la sûreté, l'impact sur les performances de la centrale est un critère pris en compte pour l'attribution du degré de sécurité.

e) Un système peut être surclassé dans un degré de sécurité plus strict que celui recommandé au point d) si les conséquences d'un acte ou d'un événement malveillant portant sur n'importe laquelle des fonctions qu'il réalise sont estimées équivalentes à celles correspondant au degré de sécurité plus strict.

   L'Annexe B fournit des explications à propos des raisons sous-jacentes au choix de retenir trois degrés de sécurité pour les systèmes numériques programmables d'I&C, ainsi que d'autres informations complémentaires.

   NOTE 1 Le présent document traite seulement des systèmes d'I&C et ne fait pas d'hypothèses supplémentaires concernant les degrés de sécurité pour les autres types de systèmes. Les systèmes qui ne font pas partie de l'I&C peuvent être assignés à des degrés de sécurité différents/complémentaires, amenant à une approche graduée présentant plus de trois degrés de sécurité lorsque la centrale est considérée de manière globale (par exemple, voir le modèle à 5 degrés du manuel de référence NSS 17 de l'AIEA, avec lequel le présent document est cohérent).

   NOTE 2 Les systèmes de gestion de données techniques (par exemple, permis de travail, bon de travail, étiquetage, etc.), en particulier ceux qui correspondent au niveau de sécurité 4 du manuel de référence NSS 17 de l'AIEA, ne sont pas pris en considération dans le domaine d'application du présent document. Cependant, étant donné qu'ils sont étroitement liés aux systèmes d'I&C, ils méritent une attention spécifique en matière de cybersécurité, conduisant, dans certains cas, à l'utilisation d'un 4e degré de sécurité conçu pour leur protection. Une autre pratique consiste à les considérer comme des systèmes d'I&C, puis à subdiviser le degré de sécurité S3 en sous-degrés appropriés.

   NOTE 3 Voir 5.4.3.2.8 pour les outils logiciel des systèmes d'I&C.

5.4.3.2 Attribution des exigences techniques

5.4.3.2.1 Généralités

Les exigences de sécurité pertinentes sont données pour tous les systèmes numériques programmables d'I&C en 5.4.3.2.4. À ces exigences sont ajoutées les exigences de 5.4.3.2.5 pour les systèmes de degré S1, les exigences de 5.4.3.2.6 pour les systèmes de degré S2 et les exigences de 5.4.3.2.7 pour les systèmes de degré S3. Ces exigences traitent des systèmes eux-mêmes et des communications entre systèmes. Elles reprennent et complètent les exigences de sécurité existant dans l'IEC 61513, l'IEC 60880, l'IEC 62566 et l'IEC 62138.

Il est important de souligner que ces exigences de cybersécurité ne sont pas destinées à, et ne peuvent pas, remplacer les exigences associées aux autres aspects, liés à d'autres normes ou documents pertinents et applicables, et en particulier celles liées à la sûreté. Elles constituent un ensemble supplémentaire d'exigences.

Par exemple, si, d'un point de vue de la cybersécurité, la communication est admise entre deux systèmes, il est possible que les exigences liées à la sûreté empêchent cette communication. Dans ce cas, la communication est évidemment interdite. L'IEC 62859 fournit un cadre permettant de faciliter la coordination entre les exigences de sûreté et les exigences de cybersécurité.

Les exigences applicables aux outils logiciel, en particulier à ceux de maintenance et de diagnostic utilisés pour les systèmes d'I&C sont fournies en 5.4.3.2.8.

5.4.3.2.2 Lien entre l'activité d'évaluation des risques pour la sécurité et les menaces de référence (DBT)

5.4.3.2.2.1 Le programme de sécurité des systèmes numériques programmables d'I&C d'une centrale nucléaire de puissance doit couvrir l'évaluation des menaces et des vulnérabilités.

5.4.3.2.2.2 La justification que les exigences de sécurité ont été correctement prises en considération doit être faite par les analyses de l'évaluation des risques associées à la solution proposée. De telles analyses prennent en compte l'évaluation des vulnérabilités de la solution technique et l'analyse des menaces particulières et des scénarios d'attaque, (y compris les menaces de références (DBT) spécifiques au pays, le cas échéant).

5.4.3.2.2.3 Les activités d'évaluation des vulnérabilités et des menaces peuvent avoir pour conséquence l'identification et la mise en œuvre de contre-mesures complémentaires exigées pour empêcher ou limiter les conséquences d'attaques contre les systèmes d'I&C de la centrale.

5.4.3.2.2.4 Les dispositions prises pour la sécurité doivent être compatibles avec les exigences de sûreté. L'IEC 62859 fournit un cadre adapté permettant de faciliter la coordination entre la sûreté et la cybersécurité.

5.4.3.2.2.5 Il convient que l'évaluation des risques spécifiques à la centrale comprenne au moins les étapes suivantes:

– définition du périmètre et du contexte;
– identification et caractérisation des menaces;
– évaluation des vulnérabilités;
– élaboration des scénarios d'attaque;
– évaluation du niveau de risque;
– définition de contre-mesures.

L'ISO/IEC 27005 fournit un cadre générique portant sur l'information relative à l'évaluation des risques de sécurité, mais le choix de mise en œuvre particulière de la méthodologie appartient à l'organisation, en fonction de son contexte organisationnel, industriel et réglementaire.

5.4.3.2.2.6 Les méthodologies et outils particuliers pour l'évaluation des risques doivent être identifiés et maintenus à jour. Des réévaluations des risques doivent être réalisées périodiquement tout au long de l'ensemble du cycle de vie des systèmes d'I&C, lorsque des modifications sont faites sur le système et lorsque des changements sont identifiés au niveau du contexte de menace, tels que de nouvelles menaces ou de nouvelles vulnérabilités qui peuvent porter atteinte aux systèmes numériques programmables d'I&C installés. Le nombre

de menaces potentielles et de vulnérabilités augmente habituellement quand un système autonome devient interconnecté.

5.4.3.2.2.7 L'évaluation des risques doit toujours être considérée à titre consultatif, c'est-à-dire qu'elle ne doit pas limiter la vigilance de la centrale vis-à-vis de la sécurité d'I&C aux seuls risques identifiés. Il convient que la gestion des vulnérabilités associées aux systèmes numériques programmables d'I&C se fasse au travers des études des publications faites par les EIUI (Équipe d'Intervention en cas d'Urgence Informatique), des contacts avec la communauté de la sécurité informatique, avec une attention particulière portée aux faiblesses des produits et des solutions d'I&C.

NOTE Les degrés de sécurité sont affectés aux systèmes ou aux sous-systèmes numériques programmables d'I&C dès le départ du projet. Ils reposent sur les conséquences potentielles, telles que définies en 5.4.3.1.1, d'une attaque des systèmes d'I&C liée à la sécurité ou d'une des fonctions qu'ils mettent en œuvre. Les degrés de sécurité, au travers des exigences associées, aident à spécifier les systèmes.

5.4.3.2.2.8 Répondant à des appels d'offres, le fournisseur doit justifier que sa solution satisfait aux exigences de sécurité en réalisant des études d'évaluation des risques.

5.4.3.2.3 Confidentialité

Dans le cadre du présent document, il est utile de distinguer deux aspects différents:

– la confidentialité des données échangées, traitées et/ou stockées par les systèmes numériques programmables d'I&C (mesures, commandes, points de consigne, etc.), et
– la confidentialité des informations relatives aux systèmes numériques programmables d'I&C (par exemple, conception détaillée et spécifications, état, versions, images de réseaux, etc.).

Concernant le premier aspect, bien que l'intégrité et la disponibilité des systèmes et des fonctions d'I&C constituent généralement les principaux objectifs de sécurité, des analyses spécifiques aux contextes et risques peuvent se traduire, dans certains cas, par la mise en œuvre de mécanismes centrés sur la confidentialité pour protéger les systèmes d'I&C. Ces mécanismes dépendant fortement du contexte, ils ne sont pas traités de manière spécifique dans le présent document. L'IEC 62859 fournit des recommandations et des exigences concernant l'utilisation de mécanismes cryptographiques centrés sur la confidentialité.

Le deuxième aspect est d'une importance capitale, mais ne relève pas du domaine d'application du présent document. Il convient de le traiter selon les réglementations nationales.

NOTE Le guide de mise en œuvre NSS 23-G de l'AIEA fournit un cadre général pour le traitement des informations relatives à la sécurité nucléaire.

5.4.3.2.4 Exigences de base

Les exigences suivantes sont applicables à tous les systèmes numériques programmables d'I&C, indépendamment du degré de sécurité qui leur est attribué.

a) Les mesures de conception doivent être définies afin d'établir un niveau approprié de confiance dans le fait que les traitements d'un système affecté à un degré donné de sécurité ne sont pas dégradés par des systèmes affectés à des degrés moins stricts.
b) Il convient que tout système d'I&C soit configuré et paramétré de façon à réduire le plus possible les vulnérabilités du système.
c) Il convient que tout composant prédéveloppé soit choisi, configuré et paramétré de façon à réduire le plus possible les vulnérabilités du système.
d) L'analyse de sécurité d'un système, y compris l'évaluation des risques, doit être prise en compte dans le plan de sécurité du système. Si l'analyse indique que les mesures prévues ne sont pas suffisantes, alors l'analyse de sécurité doit identifier le besoin portant sur des contre-mesures supplémentaires.

e) La politique de sécurité doit être adaptée à chaque système ou groupe de systèmes d'I&C. Il convient d'établir une correspondance entre la politique de sécurité d'ensemble et son adaptation pour les systèmes ou les groupes de systèmes d'I&C. Cette correspondance peut être effectuée de manière plus ou moins formelle.

f) Il convient d'intégrer dans la conception, la configuration et/ou l'attribution des paramètres des équipements programmables des mesures de protection efficaces pour:

   – le contrôle d'accès sélectif des utilisateurs aux fonctions logiciel et aux espaces mémoire,

   – les connexions de données à des systèmes ayant un degré de sécurité moins important,

   – la capacité à tracer les modifications du logiciel ou de paramètres.

g) Durant la vérification et la validation du système, l'efficacité des fonctions de sécurité doit être démontrée par des essais pertinents sur le système dans sa configuration finale.

h) Il convient que les systèmes d'I&C présentent des fonctionnalités techniques fournissant des procédures efficaces d'authentification avant qu'un accès soit autorisé.

i) Il convient que les interfaces homme-machine, pour conduire la centrale ou bien les fonctions dédiées utilisées en temps différé, ou pour la maintenance des systèmes d'I&C, limitent au minimum nécessaire les accès, aussi bien en matière de personnel autorisé que d'opérations autorisées. Lorsque le minimum nécessaire ne peut pas être atteint, il convient de mettre en œuvre des mesures compensatoires de sécurité.

j) Il convient qu'une évaluation de sécurité de la configuration sur site et de l'attribution des paramètres soit réalisée pour vérifier que les contre-mesures appropriées ont été mises en œuvre contre les menaces potentielles de sécurité.

k) Les activités de modification logicielle doivent systématiquement être planifiées et réalisées en prenant en compte les menaces potentielles de sécurité.

l) Il convient que les journaux d'enregistrement soient vérifiés de façon périodique d'un point de vue de la sécurité pour les systèmes numériques programmables d'I&C classés de sûreté et pour les systèmes de surveillance des systèmes numériques programmables d'I&C classés de sûreté.

m) Il convient que les journaux d'enregistrement soient vérifiés périodiquement pour les systèmes assurant la réalisation de fonctions de cybersécurité (par exemple les filtrages et/ou sélections par matériel). Il convient que ces journaux soient gérés de façon centralisée et corrélés autant que possible tant que cela ne compromet pas la sécurité (par exemple, segmentation réseau) ou la séparation de sûreté (par exemple pour raison d'indépendance).

n) Le nombre de points d'accès aux réseaux doit être limité autant que possible pour réduire le plus possible les vulnérabilités.

o) Il convient que les dispositions relatives à la détection des anomalies soient mises en œuvre, que les alarmes soient analysées et que des mesures appropriées soient mises en œuvre. La mise en œuvre doit être compatible avec les exigences de sûreté.

p) L'accès physique aux systèmes d'I&C doit être strictement contrôlé pour empêcher l'accès de personnes non autorisées. Ceci doit être mis en œuvre par des dispositions de sécurité physique (par exemple armoire verrouillée, contrôle physique de l'accès à la salle ou à la zone) et couvert par des mesures organisationnelles et administratives appropriées. Ces mesures doivent être adaptées au degré de sécurité des systèmes concernés.

q) Les accès physiques et logiques des contractants aux systèmes d'I&C doivent être limités en fonction de leurs missions, aussi bien en matière de durée que de systèmes concernés.

r) Toutes les dispositions temporaires, par exemple les "accès root" et les connexions supplémentaires d'appareils d'essai, doivent être identifiées et enregistrées.

s) Les modifications de la mise en œuvre du matériel et de la configuration du logiciel doivent être interdites lorsqu'elles ne sont pas prévues, approuvées par le propriétaire et documentées.

t) Des dispositions doivent être en place pour permettre une restauration rapide d'un niveau de service acceptable dans l'éventualité d'une cyberattaque qui aboutirait. Des mesures doivent être mises en place pour réduire le plus possible la possibilité que ces dispositions soient elles-mêmes vulnérables aux mêmes cybermenaces.

5.4.3.2.5 Exigences supplémentaires pour le degré S1

La liste minimale des exigences de sécurité pour les systèmes numériques programmables d'I&C classés de degré S1 (en plus des exigences de base) est fournie ci-dessous. Les dispositions nécessaires de sécurité spécifiques à l'application doivent être déterminées par une analyse de sécurité du système spécifique à l'application, incluant les menaces et les scénarios d'attaque pertinents, et l'identification des vulnérabilités du système.

a) Pour les systèmes de degré S1, les communications des systèmes numériques programmables d'I&C doivent être limitées aux autres systèmes numériques programmables d'I&C de degré S1 et de degré S2 et à leurs outils logiciels associés.

b) Il convient que les communications partent des systèmes numériques programmables d'I&C de degré S1 vers les systèmes numériques programmables d'I&C de degré S2.

c) La transmission réseau de données d'un système de degré S2 vers un système de degré S1 doit être limitée aux transmissions inévitables (par exemple les ordres prioritaires des systèmes de commande actionneurs, les permissifs, les réinitialisations) et doit reposer sur une justification complète et sur une analyse des risques pour la sécurité. Toute donnée transmise d'un système de degré S2 vers un système de degré S1 doit être sécurisée par des dispositions statiques adaptées (par exemple, contrôle du format et de la fenêtre temporelle de transmission).

d) La mise à jour logiciel et le changement de configuration pour les systèmes de degré S1 doivent être possibles seulement au moyen de verrouillage matériel local (par exemple de clefs) et seulement sur un canal à la fois. Le transfert de données bidirectionnel entre équipements d'I&C du plus haut degré de sécurité et une station de service dédiée doit être réalisé en utilisant une connexion de données séparée et dédiée, découplée des autres réseaux. Cette connexion de données dédiée doit être sécurisée par des moyens techniques, organisationnels et administratifs. L'accès par permission pour modifications logiciel ou de configuration doit être surveillé par alarme en salle de commande ou dans un autre endroit approprié.

e) Des dispositions doivent être mises en place contre les fonctions cachées dans le logiciel du système (par exemple la vérification du code du logiciel).

f) La conformité aux 5.7 (Sécurité du logiciel) et 12.2 (Sécurité informatique sur site) de l'IEC 60880:2006 et à l'IEC 62566 doit être exigée pour les systèmes de degré S1.

g) L'accès physique aux systèmes d'I&C de degré S1 doit être surveillé par alarme en salle de commande ou dans un autre endroit approprié.

5.4.3.2.6 Exigences supplémentaires pour le degré S2

La liste de l'ensemble minimal des exigences de sécurité pour les systèmes numériques programmables classés de degré S2 (en plus des exigences de base) est fournie ci-dessous. Les dispositions exigées de sécurité spécifiques à l'application doivent être déterminées par une analyse de sécurité spécifique à l'application du système, incluant les menaces et les scénarios d'attaque pertinents, et l'identification des vulnérabilités système.

a) Il convient que les communications partent des systèmes de degré S2 vers les systèmes de degré S3. Il convient que les systèmes de degré S2 aient l'initiative de la communication. Il convient que ces exigences (orientation et initiative) soient rendues exécutoires par des dispositions appropriées de sécurité (par exemple équipement de filtrage dédié).

b) La transmission de données d'un système de degré S3 vers un système de degré S2 doit être strictement limitée et justifiée au cas par cas.

c) Les modifications logicielles et de configuration de systèmes de degré S2 ne doivent pas être possibles à partir d'un système de degré S3.

d) Les modifications logicielles et de configuration de systèmes de degré S2 doivent être faites seulement sur un canal à la fois, et seulement durant des fenêtres temporelles prédéfinies et il convient d'assurer une protection par des verrouillages appropriés. Il convient de réaliser le transfert bidirectionnel de données entre des équipements d'I&C de degré S2 et une station de service dédiée en utilisant une connexion de données séparée et dédiée qui est découplée des autres réseaux. Cette connexion de données doit être sécurisée par des moyens techniques, organisationnels et administratifs.

e) L'établissement de communication avec des systèmes d'I&C de degré S2, que ce soit à partir de l'extérieur de la centrale ou à partir de systèmes qui ne sont pas d'I&C, doit être empêché.

f) Des mesures de conception doivent limiter l'accès aux zones programmables des systèmes de degré S2 (par authentification efficace de l'utilisateur, par exemple) et empêcher toute création non autorisée d'un nouvel accès à ces zones.

5.4.3.2.7 Exigences supplémentaires pour le degré S3

La liste de l'ensemble minimal des exigences de sécurité pour les systèmes numériques programmables d'I&C classés de degré S3 (en plus des exigences de base) est fournie ci-dessous. Il convient qu'une analyse sécurité spécifique au système complète cette liste.

a) L'accès à partir de systèmes ne faisant pas partie de l'I&C qui peuvent avoir une influence sur les fonctions des systèmes d'I&C doit être justifié au cas par cas et ne doit pas compromettre les exigences de sûreté et de sécurité associées au système.

b) Il convient que la communication entre les systèmes numériques programmables d'I&C de degré S3 et les systèmes de faisant pas partie de l'I&C se fasse sur l'initiative des systèmes de degré S3. Les exceptions doivent être justifiées et les connexions doivent être surveillées.

5.4.3.2.8 Exigences de sécurité pour les outils logiciels, y compris de maintenance et de diagnostic

5.4.3.2.8.1 Les outils logiciel, en particulier ceux utilisés à des fins de maintenance système et de diagnostic d'I&C sont des vecteurs d'attaque avérés et classiquement des cibles intermédiaires dans les scénarios d'attaque des systèmes d'I&C. Ils doivent être affectés au même degré de sécurité que celui du système d'I&C auquel ils sont associés, lorsqu'il y a une connexion directe (temporaire ou permanente) entre eux.

5.4.3.2.8.2 Un degré de sécurité inférieur peut être attribué dans le cas d'une connexion indirecte mettant en jeu des contrôles humains et/ou procéduraux. Dans le cas où les outils logiciels sont assignés à des degrés de sécurité moins stricts, il convient que les outils soient conçus pour empêcher les actions non prévues. L'enregistrement (Qui/Quoi/Quand) de l'utilisation des outils et des contrôles d'accès renforcés doivent être mis en œuvre.

5.4.3.2.8.3 Il convient d'adapter comme suit les exigences de sécurité associées pour les outils logiciels:

– 5.4.3.2.4 (Exigences de base) est applicable pour tous les outils logiciels.

– Pour le degré S1, 5.4.3.2.5 est applicable à l'exception du point g) (traitant des alarmes) qui n'est pas pertinent pour les outils logiciels, et à l'exception du point e) (traitant des fonctions cachées) qui est remplacé par le suivant: il convient de prendre des dispositions contre les fonctions cachées dans le logiciel système de l'outil.

– Pour le degré S2, 5.4.3.2.6 est applicable à l'exception des points c), d) et f) qui ne sont pas pertinents pour les outils logiciel. Le point e) est remplacé par le suivant: il convient d'empêcher l'entrée en communication avec les systèmes d'I&C de degré S2, que ce soit de l'extérieur de la centrale ou à partir de systèmes ne faisant pas partie de l'I&C.

– Pour le degré S3, 5.4.3.2.7 est applicable (mêmes exigences).

NOTE Ces adaptations ont pour but de prendre en compte la différence technologique potentiellement importante entre les systèmes numériques programmables d'I&C et les outils logiciel, en particulier pour les systèmes de sûreté.

5.4.3.3 Zones de sécurité

5.4.3.3.1 Une possible mise en œuvre pratique de l'approche graduée correspond à un regroupement des systèmes numériques programmables d'I&C dans des zones logiques, pour lesquelles des principes de protection graduée sont appliqués pour chaque zone de sécurité (voir la définition dans l'Article 3). Ces zones 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 l'application et l'administration des mesures de protection. Les critères de définition des zones de sécurité peuvent prendre en compte les questions d'organisation (telles que la propriété, la responsabilité), la localisation, les aspects d'architecture ou techniques.

NOTE Dans le reste du présent document, le terme "zone" désigne une "zone de sécurité" telle que définie en 3.21 et dans le présent paragraphe. Ce terme ne fait pas référence aux zones de sûreté et aux séparations géographiques associées (bien que certaines relations existent).

5.4.3.3.2 Il convient que la délimitation et la mise en œuvre de zones de sécurité soient conformes aux lignes directrices suivantes:

a) Chacune des zones comprend des systèmes qui ont le même degré de sécurité. Si pour des raisons liées à l'architecture ou autre, un système numérique programmable d'I&C est assigné à un degré de sécurité moins strict (voir 5.4.3.1.3) que les autres systèmes regroupés dans la zone, il convient de remonter son degré de sécurité et qu'il satisfasse aux exigences associées au degré de sécurité des autres systèmes de la zone.

   NOTE 1 Les degrés de sécurité sont formellement associés aux systèmes numériques programmables d'I&C (voir 5.2.3.2). Cependant, comme les systèmes d'un groupe d'une zone ont le même degré de sécurité, une zone donnée peut être considérée par extension comme ayant le degré de sécurité des systèmes qu'elle regroupe (par exemple une zone de sécurité de degré S2). Cependant, même si les zones de sécurité et les degrés de sécurité s'entremêlent, ils sont encore des concepts différents.

b) La présence de barrières de sécurité n'est pas exigée entre les systèmes appartenant à la même zone de sécurité. Cependant, pour les zones contenant des systèmes multiples et des interfaces entre zones, des barrières peuvent être un moyen efficace de protection.

   NOTE 2 Si la communication entre des systèmes ayant le même degré de sécurité est possible du point de vue de l'approche graduée de cybersécurité, cela ne signifie pas qu'elle n'est pas limitée ou qu'elle est interdite pour d'autres raisons, comme des exigences liées à la sûreté (par exemple, indépendance), l'architecture, ou le zonage de cybersécurité.

c) Les équipements réseau (commutateurs, câbles, etc.) doivent être situés dans une zone de sécurité en cohérence avec les systèmes d'I&C interconnectés. Dans le cas d'équipements réseau connectés à de multiples zones, si les zones ont le même degré de sécurité, alors les possibles séparations de sécurité doivent être définies sur la base des exigences particulières de l'installation (qui sont hors du domaine d'application du présent document). Si les zones ont des degrés de sécurité différents, alors les exigences de sécurité associées aux degrés de sécurité s'appliquent (voir 5.4.3.2.4 à 5.4.3.2.7). En particulier, celles applicables aux communications et aux interfaces entre systèmes appartenant à des degrés de sécurité différents doivent entraîner la mise en place de dispositions dédiées de sécurité.

d) Il convient que l'initialisation des communications ne soit faite que d'une zone de sécurité supérieure (regroupant des systèmes assignés à un degré de sécurité donné) vers une zone de sécurité inférieure (c'est-à-dire regroupant des systèmes assignés à un degré de sécurité inférieur).

e) Les frontières de zones exigent la mise en œuvre de mécanismes de découplage pour le flux de données cohérents avec le degré de sécurité des systèmes numériques programmables d'I&C associés.

5.4.3.3.3 La relation entre zones de sécurité et degrés de sécurité n'est pas bijective, un degré de sécurité peut être attribué à plusieurs zones.

5.4.3.3.4 Les zones de sécurité peuvent être utilisées pour segmenter des systèmes ayant le même degré de sécurité, mais avec différentes classes de sûreté. L'IEC 62859 fournit davantage de recommandations sur la relation entre sûreté et cybersécurité.

NOTE Les zones correspondent à des regroupements logiques et/ou physiques de systèmes informatisés, alors que les degrés de sécurité représentent les degrés de protection exigés.

5.5 Support

5.5.1 Ressources

Le contenu du 7.1 de l'ISO/IEC 27001:2013 s'applique.

5.5.2 Formation, compétences et sensibilisation

5.5.2.1 Formation

La formation du personnel, y compris les contractants, au sein d'une organisation, est nécessaire pour garantir la sécurité d'un cyber environnement pour les équipements numériques programmables d'I&C. Elle limite la probabilité d'avoir des failles de sécurité et l'apparition de problèmes internes liés à la sécurité. En conséquence:

a) Un programme formalisé de formation pour le personnel concevant et exploitant les systèmes numériques programmables d'I&C doit être développé et mis en place.

b) Ce programme doit comprendre des programmes de formation destinés à des utilisateurs en général et des formations spécialisées adaptées aux degrés de sécurité des systèmes auxquels accèdent les participants à ces formations.

5.5.2.2 Compétence

Le contenu du 7.2 de l'ISO/IEC 27001:2013 s'applique.

5.5.2.3 Sensibilisation

Le contenu du 7.3 de l'ISO/IEC 27001:2013 s'applique.

5.5.2.4 Expertise relative aux formations et à la sensibilisation

Les organisations et les individus qui ont de l'expérience au niveau des systèmes numériques programmables d'I&C doivent être dans l'absolu impliqués dans la sensibilisation et la formation, idéalement dans le contexte des centrales nucléaires de puissance.

5.5.3 Communication relative à la cybersécurité

Le contenu du 7.4 de l'ISO/IEC 27001:2013 s'applique.

5.5.4 Informations documentées

5.5.4.1 Généralités

5.5.4.1.1 Le contenu du 7.5.1 de l'ISO/IEC 27001:2013 s'applique.

5.5.4.1.2 Le programme de sécurité des systèmes numériques programmables d'I&C doit définir les mesures nécessaires et les procédures de gouvernance afin d'assurer que des enregistrements suffisants de données relatives aux éléments et activités affectant la cybersécurité sont effectués, examinés, approuvés, publiés, utilisés et révisés pour refléter les travaux effectués, y compris:

– enregistrements effectués lors de l'élaboration, la mise en œuvre et la maintenance du programme;

– enregistrements des résultats d'évaluations de menaces qui traitent des vulnérabilités spécifiques concernant la technologie utilisée, la configuration des systèmes numériques programmables d'I&C, et la nature de leur utilisation, maintenance ou exigences d'essai;

– enregistrements de l'ajout, la modification et le retrait d'actifs numériques programmables d'I&C traités par le programme;

– enregistrements et documentation technique d'appui, y compris les données d'audit et les registres de formation, exigés pour satisfaire aux exigences réglementaires nationales.

La documentation prouve que la conception et la mise en œuvre réelle des systèmes numériques programmables d'I&C ont un niveau approprié de sécurité conformément au présent document, et que les utilisateurs des systèmes ont reçu des instructions et une formation adéquates concernant l'exploitation et la maintenance des éléments du système liés à la sécurité.

5.5.4.2 Création et mise à jour

Le contenu du 7.5.2 de l'ISO/IEC 27001:2013 s'applique.

5.5.4.3 Maîtrise des informations documentées

Le contenu du 7.5.3 de l'ISO/IEC 27001:2013 s'applique.

5.6 Exploitation

5.6.1 Planification et contrôle opérationnels

Le contenu du 8.1 de l'ISO/IEC 27001:2013 s'applique.

5.6.2 Approche graduée de la cybersécurité, évaluation des risques et traitement des risques

5.6.2.1 L'organisation doit mettre en œuvre et maintenir l'approche graduée et effectuer une évaluation des risques et un traitement des risques, conformément à 5.4.3.

5.6.2.2 L'organisation doit conserver des informations documentées de la mise en œuvre de l'approche graduée, des évaluations des risques et des traitements des risques.

5.7 Évaluation des performances

5.7.1 Surveillance, mesurages, analyse et évaluation

5.7.1.1 Généralités

Le contenu du 9.1 de l'ISO/IEC 27001:2013 s'applique.

5.7.1.2 Examens et audits de la sécurité

5.7.1.2.1 Un des principaux facteurs contribuant au maintien de l'efficacité du programme de sécurité des systèmes numériques programmables d'I&C est la réalisation périodique de réexamens du programme de sécurité. Le programme doit définir les mesures nécessaires et les procédures de gouvernance pour mettre en place des revues applicables aux éléments du programme, conformément aux exigences réglementaires nationales.

5.7.1.2.2 En conséquence, l'organisation doit:

a) élaborer un programme de réexamen qui traite de l'objectif, du domaine d'application, des rôles, des responsabilités, des exigences et de l'engagement hiérarchique associés aux éléments à passer en revue du programme de sécurité des systèmes numériques programmables d'I&C pour en garantir l'efficacité;

b) élaborer des procédures pour faciliter et maintenir à jour le programme de réexamen, y compris en ce qui concerne la fréquence des revues et la qualification des personnels en charge de la réalisation des revues.

5.7.2 Audit interne

5.7.2.1 Le contenu du 9.2 de l'ISO/IEC 27001:2013 s'applique.

5.7.2.2 Le document TLD-006 de l'AIEA fournit un cadre générique approprié pour l'audit des installations nucléaires, y compris les systèmes d'I&C. Cependant, il incombe à l'organisation, selon son contexte organisationnel, industriel et réglementaire, de choisir la méthodologie spécifique d'audit.

5.7.3 Revue de direction

5.7.3.1 Le contenu du 9.3 de l'ISO/IEC 27001:2013 s'applique.

5.7.3.2 Le résultat de la revue et de l'approbation de direction doit comprendre toutes décisions et actions relatives aux points suivants:

a) mise en œuvre et modifications des procédures et des mesures qui ont un effet sur le programme de sécurité des systèmes numériques programmables d'I&C, telles que nécessaires, pour répondre aux événements internes et externes qui peuvent avoir un impact sur:
   - les exigences liées aux activités industrielles et commerciales,
   - les exigences de sécurité,
   - les exigences légales et réglementaires,
   - les obligations contractuelles,
   - les niveaux de risque et/ou les critères pour accepter les risques,
   - les besoins en ressources;

b) critères originaux et amélioration des mesures mises en place concernant l'efficacité des mesures;

c) processus de décision et critères de déclenchement d'action ayant un impact sur l'exploitation de la centrale (par exemple poursuite de l'exploitation de la centrale, arrêt de la centrale, isolement des communications, maintenance des matériels).

5.7.3.3 Les décisions et les actions reposant sur cette revue de direction doivent être prises à l'aide d'un processus décisionnel adéquat garantissant la coordination avec les programmes de sécurité des systèmes ne faisant pas partie de l'I&C, les régimes de protection physique et les programmes d'exploitation et de maintenance de la centrale.

5.8 Amélioration

5.8.1 Généralités

Le programme de sécurité des systèmes numériques programmables d'I&C doit définir le processus pour:

a) mettre en œuvre les améliorations concernant le programme identifiées durant les revues internes ou externes de programme, y compris les actions prédictives ou correctives;

b) informer toutes les parties intéressées des actions et des améliorations réalisées avec un niveau de détail adapté aux circonstances, ceci faisant partie du programme de formation en continu;

c) développer et mettre en œuvre un programme de revue pour évaluer périodiquement et mettre à jour l'évaluation des menaces pour la sécurité et les informations relatives aux vulnérabilités identifiées;

d) définir les métriques pour évaluer si les améliorations ont atteint leurs objectifs.

5.8.2 Non-conformité et actions correctives

Le contenu du 10.1 de l'ISO/IEC 27001:2013 s'applique.

5.8.3 Amélioration continue

Le contenu du 10.2 de l'ISO/IEC 27001:2013 s'applique.

6 Mise en œuvre du cycle de vie pour la sécurité des systèmes numériques programmables d'I&C

6.1 Généralités

Les paragraphes suivants donnent une vue d'ensemble des documents et des tâches qu'il convient d'intégrer dans le processus du cycle de vie pour la sécurité des systèmes numériques programmables d'I&C. Le cycle de vie pour la sécurité des systèmes numériques programmables d'I&C est développé pour couvrir les systèmes numériques programmables d'I&C et leurs composants de leur conception à leur retrait d'exploitation en passant par leur vie en service.

NOTE Le cycle de vie utilisé dans le présent article correspond au cycle de vie de sûreté du système décrit dans l'IEC 61513:2011, étendu par les deux phases "Activités d'exploitation et de maintenance" et "Retrait d'exploitation".

Une bonne coordination doit être assurée entre les aspects de sûreté et ceux de cybersécurité. Des exigences et recommandations peuvent être consultées dans l'IEC 62859.

6.2 Spécification des exigences relatives au système

6.2.1 Généralités

6.2.1.1 Une approche descendante, tenant compte de l'architecture d'ensemble de l'I&C et les systèmes et composants individuels, doit être utilisée.

6.2.1.2 Les spécifications de sécurité doivent être écrites pour couvrir l'architecture d'ensemble de l'I&C d'un point de vue fonctionnel et de sécurité, avant de traiter les systèmes et leurs interfaces.

NOTE Lors de l'écriture de spécifications, les systèmes nécessaires pour réaliser une fonctionnalité donnée ne sont pas connus, ainsi il n'est pas possible de réaliser une évaluation des risques de sécurité exhaustive et détaillée, seule l'évaluation des vulnérabilités ou des conséquences de haut niveau est possible à ce stade.

6.2.1.3 Les composants et systèmes individuels peuvent être fournis et sécurisés par différents fournisseurs, à condition que la sécurité au niveau de l'ensemble de la structure soit maintenue de façon consistante.

6.2.1.4 Les spécifications relatives à la sécurité des produits doivent être fournies par les fournisseurs.

6.2.2 Attribution du degré de sécurité

Chaque système numérique programmable individuel d'I&C doit être assigné à un degré de sécurité. Les degrés de sécurité doivent être basés sur une approche graduée de la sécurité des systèmes numériques programmables d'I&C telle que décrite en 5.2.3.

NOTE Le terme "système" est utilisé pour décrire un "système individuel d'I&C" conformément à l'IEC 61513.

6.3 Spécification du système

6.3.1 Sélection des composants préexistants

6.3.1.1 L'aptitude à l'emploi des composants candidats doit être évaluée et estimée afin de démontrer que leurs caractéristiques sont conformes aux spécifications des exigences de sécurité du système.

6.3.1.2 Il convient que l'évaluation et l'estimation de sécurité de l'aptitude à l'emploi des composants candidats reposent sur la comparaison des spécifications des exigences de sécurité du système et de la documentation de sécurité relative aux composants préexistants. Cette dernière inclut les spécifications produit de sécurité (si disponible).

6.3.1.3 Si des différences sont identifiées entre la spécification des exigences de sécurité du système et la spécification de sécurité des composants candidats et que celles-ci rendent les composants inadaptés au degré prévu de sécurité du système, ceux-ci doivent être rejetés.

6.3.1.4 L'estimation de l'aptitude à l'emploi doit établir que la spécification des composants candidats est conforme au degré et à la spécification de sécurité prévus pour ces composants.

6.3.2 Architecture du système

L'architecture divise le système en sous-systèmes et composants interconnectés. L'organisation des sous-systèmes doit satisfaire aux exigences de sécurité relatives au degré de sécurité d'ensemble du système.

6.4 Conception détaillée et mise en œuvre du système

6.4.1 Généralités

6.4.1.1 La phase de conception doit prendre en compte les objectifs de conception de la centrale pour l'ensemble de l'I&C et pour les systèmes individuels en ce qui concerne la question du degré de sécurité (affecté conformément à 5.2.3 du présent document) pour traiter des mesures de sécurité pour:

a) les accès physiques et logiques à la fonction des systèmes d'I&C,

b) l'utilisation des systèmes d'I&C, et

c) la communication de données avec d'autres systèmes d'I&C.

6.4.1.2 Il convient que le concepteur garantisse que la conception du code logiciel est conforme pratiques de codage sécurisé, pour traiter de la question des vulnérabilités potentielles qui peuvent avoir été introduites au niveau du processus de conception. Il convient de porter une attention particulière à la gestion de configuration.

6.4.1.3 Les exigences doivent être traduites en critères particuliers de conception.

6.4.1.4 L'accès à toute unité logicielle placée sous contrôle de configuration doit être soumis à des dispositions de sécurité appropriées pour garantir que le logiciel n'est pas modifié par une personne non autorisée et que la sécurité du logiciel est maintenue.

6.4.1.5 Le concepteur doit faire l'inventaire complet de tous les systèmes d'I&C et de leurs interfaces en tenant compte de tous les appareils utilisés dans la centrale, y compris les appareils d'essai, de maintenance et de diagnostic.

6.4.2 Évaluation des risques au niveau de la phase de conception

6.4.2.1 Il convient que les justifications démontrant que les exigences de sécurité ont été correctement prises en compte soient complétées par une évaluation des risques. De telles analyses prennent en compte les analyses de vulnérabilités de la solution technique et l'analyse des menaces et des scénarios d'attaques particuliers, (y compris les menaces de référence particulières au pays, le cas échéant).

6.4.2.2 Les évaluations des risques peuvent conduire à modifier les mesures de sécurité ou l'architecture de sécurité. Les activités d'évaluation des menaces et des vulnérabilités peuvent entraîner l'identification et la mise en œuvre de contre-mesures supplémentaires exigées pour empêcher ou limiter les conséquences d'attaques contre les systèmes d'I&C de la centrale.

6.4.3 Plan de sécurité du projet de conception

6.4.3.1 Le plan de sécurité pour l'I&C doit être appliqué au niveau de l'organisation principale en charge de la conception et de toutes les tierces parties ou organisations sous-contractantes travaillant sur le projet.

6.4.3.2 Un plan de sécurité de projet de conception, couvrant l'exploitant mais aussi les tierces parties et les entités externes impliquées dans le projet, doit être établi.

6.4.3.3 En particulier le concepteur doit prouver que:

a) il a en place une politique de sécurité;

b) une telle politique s'applique pour chacun de ses sites de développement;

c) elle est complétée au niveau des aspects locaux;

d) elle garantit que ses propres tierces parties sont à un niveau satisfaisant de sécurité.

6.4.4 Chemins de communication

6.4.4.1 Les chemins de communication doivent faire l'objet d'évaluations au niveau de la conception du système et de ses composants. Dans le cadre de ce processus, il convient de définir les limites du système et d'en établir une cartographie.

6.4.4.2 Des mesures de cybersécurité doivent être établies pour:

a) rendre exécutoire et documenter les autorisations données pour contrôler le flux d'informations dans et entre les systèmes interconnectés conformément aux degrés de sécurité attribués (voir 5.4.3.1);

   NOTE C'est le cas pour les systèmes assignés à différents degrés de sécurité ou à différentes zones de sécurité.

b) maintenir à jour la documentation qui justifie les analyses et décrit les flux d'informations autorisés et interdits entre les systèmes et les appareils couverts par le programme de sécurité des systèmes numériques programmables d'I&C, en cohérence avec l'évaluation des risques et l'approche graduée décrite en 5.4.3.

6.4.4.3 Les appareils sans fil doivent être conformes aux 4.3 et 5.6 et à l'Article 8 de l'IEC 62988:2018, impliquant l'interdiction des systèmes de degré S1 et S2, et une utilisation conditionnelle pour les systèmes de degré S3.

NOTE Conformément aux critères d'attribution des degrés de sécurité, la technologie sans fil est exclue pour les systèmes prenant en charge les fonctions de Catégorie A ou B.

6.4.5 Définition des zones de sécurité

6.4.5.1 Il convient de définir les zones de sécurité durant la phase de conception (voir 3.21 et 5.4.3.3). Elles peuvent aussi être définies durant la phase de mise en œuvre (voir 6.5).

6.4.5.2 L'assignation des systèmes numériques programmables d'I&C aux zones de sécurité doit prendre en compte, comme indiqué en 5.4.3.3, le degré de sécurité précédemment attribué durant la phase de planification à chaque système numérique programmable d'I&C, et les chemins de communication identifiés (voir 6.4.4).

6.4.6 Évaluation de la sécurité de la conception finale

Des évaluations de la sécurité doivent couvrir l'architecture d'I&C d'ensemble à l'étape finale de la conception.

6.4.7 Activités de mise en œuvre

6.4.7.1 Dans la phase de mise en œuvre, le logiciel et le matériel doivent être mis en oeuvre en fonction de la conception système en prenant en compte toutes les exigences définies de sécurité.

6.4.7.2 S'il y a des modifications par rapport à la conception prévue ou si de nouvelles informations techniques substantielles sont disponibles, les activités d'évaluation des vulnérabilités et des menaces doivent faire l'objet de mises à jour, ce qui peut conduire à mettre en place des contre-mesures supplémentaires.

6.5 Intégration du système

Conformément à l'IEC 61513, l'objectif de cette phase est d'assembler les modules matériels et logiciels et de vérifier la compatibilité du logiciel chargé dans le matériel. Au cours de cette phase:

a) Il convient de mettre en place les caractéristiques intégrées de sécurité et de les configurer conformément à la spécification avant les essais d'intégration et la validation du système (voir 6.6).

b) Il convient que les essais d'intégration confirment que les mesures intégrées de sécurité sont effectuées comme exigé et ne compromettent pas la capacité du système à effectuer ses fonctions exigées (voir l'IEC 62859 pour obtenir plus d'informations sur la coordination entre sûreté et cybersécurité).

c) Un plan de sécurité d'intégration de système spécifique à une phase doit être élaboré sous la forme de document autonome ou dans le cadre d'un plan de sécurité d'ensemble.

6.6 Validation du système

6.6.1 Les essais traditionnels de Vérification et Validation (V&V) conformes aux normes exigées doivent être effectués en fonction des exigences de sécurité spécifiées pour les systèmes numériques programmables d'I&C.

6.6.2 De plus, les essais doivent permettre de vérifier les aspects sécurité au niveau de la conception de l'I&C pour l'architecture matérielle, les dispositifs externes de communication et les configurations pour ce qui est des chemins de communication non autorisés et de l'intégrité système.

6.6.3 Les exigences de sécurité et les éléments de configuration doivent faire partie de la validation des exigences systèmes d'ensemble et des éléments de configuration de conception.

6.6.4 Chaque caractéristique du système relative à la sécurité doit être validée pour garantir que le système mis en œuvre n'augmente pas le risque de vulnérabilité de sécurité et ne réduit pas la fiabilité des fonctions de sûreté (voir l'IEC 62859 pour obtenir plus d'informations sur la coordination entre sûreté et cybersécurité).

6.6.5 Un plan de sécurité de validation de système spécifique à une phase doit être élaboré sous la forme de document autonome ou dans le cadre d'un plan de sécurité d'ensemble.