IEC 62645

Edition 1.0 2014-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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

IEC 62645:2014-08(en-fr)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 14 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 55 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62645

Edition 1.0 2014-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX X

ICS 27.120.20

ISBN 978-2-8322-1810-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

FOREWORD

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

c) Recommendations and limitations regarding the application of this standard

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Scope

1.1 General

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2 Application

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

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

1.3 Framework

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

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

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

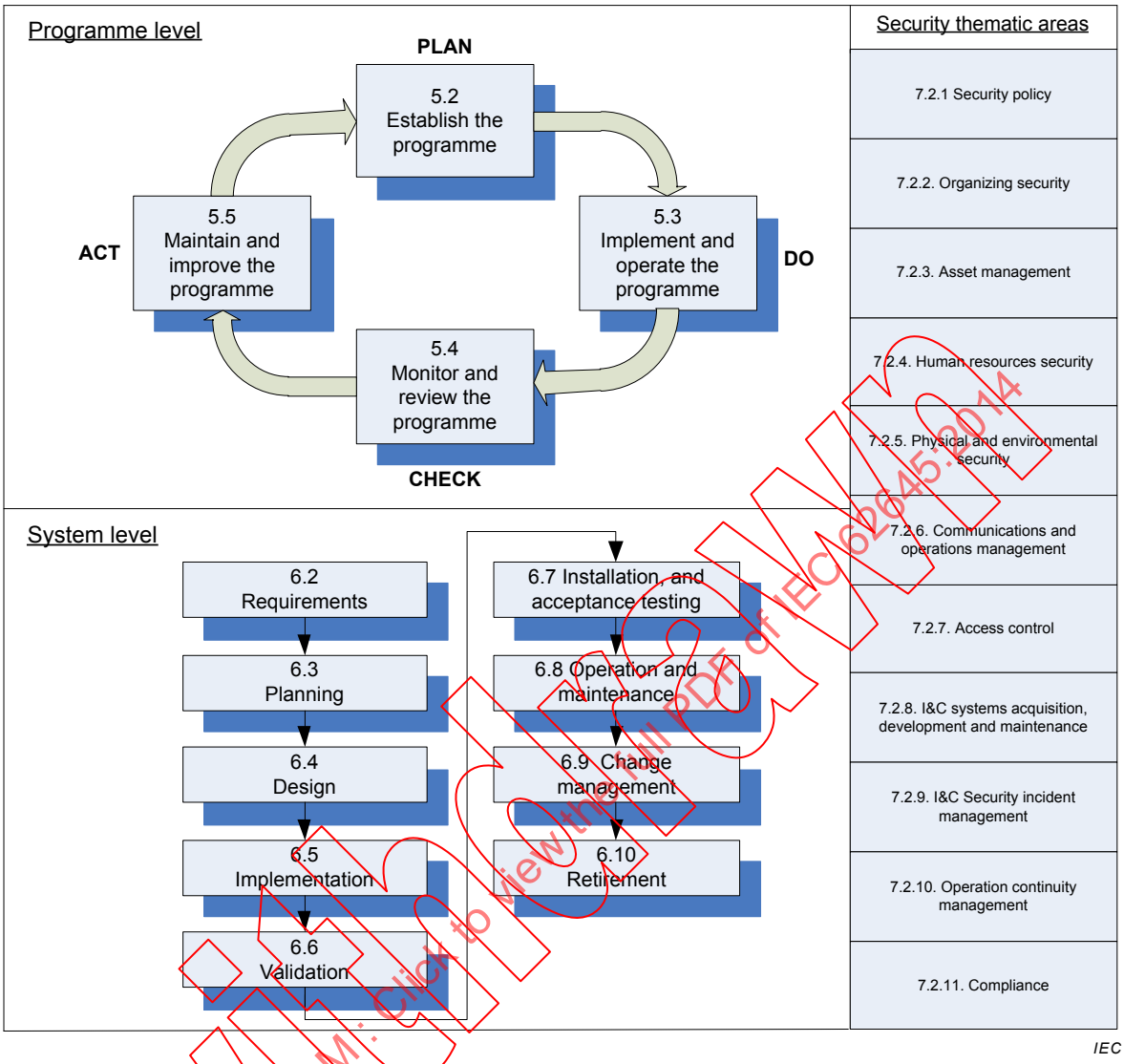

Figure 1 – Overall framework of IEC 62645

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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
the 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 system
I&C system whose functions are mostly dependent on, or completely performed by using, microprocessors, programmed electronic equipment or computers

Note 1 to entry: In the context of this standard, computer, computer-based system, digital system, digital device, software-based system, and programmed system are all synonymous.

Note 2 to entry: In the context of this standard, I&C CB&HPD systems include computer-based sub systems but also possibly HPD based sub systems and all components susceptible to electronic compromises. See also definition of HPD.

[SOURCE: IEC 60880:2006, 3.11]

3.5
confidentiality
the 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
cybersecurity
set of activities and measures whose objective is to prevent, detect, and react to digital attacks that have the intent to cause:

- disclosures that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation (confidentiality),
- malicious modifications of functions that may compromise the delivery or integrity of the required service by I&C CB&HPD systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation (integrity),
- 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 which could lead to an accident, an unsafe situation or plant performance degradation (availability).

Note 1 to entry: This definition is tailored with respect to the standard scope, focusing on the prevention of, detection of and reaction to malicious acts by digital means on I&C CB&HPD systems. 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, which are all out of the scope of this standard (see 1.1)

Note 2 to entry: In the frame of this standard, “computer security” is synonymous with “cybersecurity” and “unauthorized accesses” is synonymous with “unauthorized logical accesses”.

3.7
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]

3.8
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: Cyber attacks 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]

3.9
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, PLDs or similar micro-electronic technologies.

[SOURCE: IEC 62566:2012, 3.7]

3.10
I&C function
function to control, operate and/or monitor a defined part of the process

[SOURCE: IEC 61513:2011, 3.28]

3.11
I&C system
system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

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 1 to entry: See also "I&C function".

Note 2 to entry: Any network either is part of an I&C system or is an I&C system by itself.

[SOURCE: IEC 61513:2011, 3.29]

3.12
integrity
the property of protecting the accuracy and completeness of assets

[SOURCE: IAEA Nuclear Security Series No. 17:2011 and ISO/IEC 27000:2009]

3.13
risk
the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

It is measured in terms of a combination of the likelihood of an event and the severity of its consequences.

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

3.14
risk assessment
overall process of systematically identifying, estimating, analysing and evaluating risk

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

3.15
security controls
means of managing security which can be administrative, technical, or management

3.16
security degree
gradation of security protection with associated sets of requirements, assigned to a system according to the maximum consequences of a successful cyber attack on this system in terms of plant safety and performance

Note 1 to entry: Subclause 5.2.3 of this standard defines three security degrees which correspond to S1, S2 and S3. The rationale behind the use of three security degrees for I&C CB&HPD systems is provided in Annex A. This standard only deals with I&C CB&HPD 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.

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.

3.17
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]

3.18
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 standard (see 1.1), the considered events or occurrences are limited to malicious ones – not to include accidental aspects (e.g., natural hazards, human errors), treated by other IEC documents in the field of instrumentation and control of nuclear facilities.

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

3.19
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 Abbreviations

I&C CB&HPD	Computer-Based and HDL Programmed Device
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
PDCA	Plan Do Check Act
PLC	Programmable Logic Controller
PSP	Project Security Plan
QA	Quality Assurance
V&V	Verification & Validation

5 Establishing and managing a nuclear I&C CB&HPD system security programme

5.1 General

5.1.1 Overall concepts: programme, policies and procedures

A I&C CB&HPD system security programme (often referred to in this standard as programme) shall define the steps and actions to be undertaken in order to define and apply consistent organizational and technical measures and procedures to enforce security objectives, defined in a security policy, explicitly addressed in security plans.

This 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 computer security programme.

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

A policy shall describe the expectations and requirements for managing computer security within a NPP and allow for a consistent and manageable environment. This policy shall be created and kept with the policies and procedures developed throughout the life of this I&C CB&HPD security programme.

A I&C CB&HPD systems security programme of a NPP shall contain the following activities:

- definition of the computer security organization and responsibilities and the process of periodic reviews;
- development of the process of designating assets subject to computer security protective measures including computer systems, computer system applications and network connections;
- implementation of methods of personnel management in computer security and I&C CB&HPD system security including training, qualification and termination/transfer;
- 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;
- performance of an assessment of the residual risk that is transferred/accepted from design to operation;
- 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 cyber security features incorporated in the design;

- 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;
- 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;
- 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.

A computer security policy shall set the high-level computer security goals applicable for a nuclear facility. I&C CB&HPD system security policy requirements shall be factored into lower level documents, which will be used to implement and control policy, and shall be measurable, enforceable and achievable.

The I&C CB&HPD system security plan shall be the implementation of that policy in the form of organizational roles, responsibilities and procedures. The plan shall specify and detail the means for achieving the security goals. The plan shall 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.

5.1.2 Roles and responsibilities

Management of the computer security programme shall ensure that all necessary computer security issues are addressed programmatically within the nuclear programme's policy and procedures to meet regulatory and corporate requirements. It shall be coordinated with the corporate security programme and the current site's framework of policies, programmes, practices and procedures, as applicable.

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

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

All organisations involved in any portion of the life cycle of I&C CB&HPD 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.

In order to develop, approve and implement a I&C CB&HPD system security programme, plant management in cooperation with the I&C designer shall consider:

- utility corporate security requirements;
- internal corporate security policy;
- national legislative material;
- national regulatory material;
- computer and I&C CB&HPD system security industry best practices;
- current and projected threat status in the nuclear industry and in other industries using I&C equipment used in nuclear plants;
- 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.

On the plant specific level, the utility shall:

- assume overall responsibility for all aspects of computer security to ensure the facility is safe and secure;
- take into account applicable regulatory requirements to define the nuclear plant computer security objectives;
- ensure appropriate coordination with the non I&C system security programme and physical protection regime;
- ensure compliance with laws and regulations;
- establish a continuous process security risk assessment for the plant I&C CB&HPD systems;
- set the risk acceptance level for the facility in compliance with regulatory requirements;
- assign organizational I&C CB&HPD system security responsibilities;
- ensure an enforceable I&C CB&HPD system security policy is established;
- provide adequate resources to implement a robust I&C CB&HPD system security programme;
- ensure periodic audits and updates of I&C CB&HPD system security policy and procedures.

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

- advise the company's and/or project's management;
- coordinate and control the development of the computer security activities;
- coordinate computer security with other security and safety disciplines;
- ensure that the computer security programme takes into account plant operation or maintenance and does not inadvertently affect the systems important to safety;
- identify and document the systems that are critical to maintaining computer security within a facility;
- conduct computer security risk assessments;
- conduct periodic security inspections, audits and reviews, and provide status reports to top level management;
- develop and implement computer security training and evaluation;
- develop a strategy, including training aspects and procedures, to identify potential cyber security incidents;
- develop and lead or contribute to the response for relevant computer security events including coordination with relevant internal and external organizations;
- investigate computer security incidents or identified vulnerabilities and recommend corrective actions.

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.

5.1.3 Documentation requirements

The I&C CB&HPD systems security programme shall establish the necessary measures and governing procedures to ensure that sufficient records of items and activities affecting cyber security 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 CB&HPD systems, and the nature of their use, maintenance or test requirements;
- records of addition, modification, and removal of I&C CB&HPD 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 CB&HPD systems design and actual implementation meet an appropriate level of security as per this standard, and that the system users have received the adequate instruction and training on operation and maintenance of the security-related elements of the system.

5.2 Establish the programme

5.2.1 Defining security policy

Those responsible for the security programme (as defined in 5.1.2) shall generate a written top-level security policy for the programme. This policy shall:

- include a framework for setting objectives and establish an overall sense of direction and principles for action with regard to I&C CB&HPD system security;
- take into account legal and regulatory requirements, as well as contractual security obligations;
- ensure security requirements are applied through all levels of the supply chain for all life cycle activities;
- align with the nuclear facility's strategic risk management context in which the establishment and maintenance of the I&C CB&HPD system security programme will take place;
- establish criteria against which risk will be evaluated (see 5.2.2) including consideration of the outcomes from I&C CB&HPD system exploitation; and
- be approved by management.

5.2.2 Defining the programme scope and boundaries

The scope and boundaries of the I&C CB&HPD system security programme shall be defined in terms of the characteristics of the nuclear power plant's organization, its location, national regulatory requirements, I&C CB&HPD assets and technology, and risk of system exploitation. It shall include details of and justification for exclusions/modifications from the scope (see 1.1).

5.2.3 Graded approach to I&C security and risk assessment

5.2.3.1 Classification scheme

5.2.3.1.1 General

I&C CB&HPD system security shall be based on a graded approach: all I&C CB&HPD systems shall be assigned to security degrees. The security degree of a I&C CB&HPD system shall be assigned based on the maximum consequences of a successful cyber attack on this system in terms of plant safety and performance (see 5.2.3.1.3 for detailed assignment criteria). Graded security requirements are defined for each security degree (in 5.2.3.2.3 to 5.2.3.2.7).

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

The classification scheme is based on the following principles:

- consequences of cyber attack regarding safety shall be assumed as more serious than those regarding plant performance;
- 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;
- 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).

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

A graded approach to security as per this standard provides that:

- the number of interfaces between systems assigned to different security degrees shall be justified;
- appropriate restrictions shall be enforced to interfaces between systems of different security degrees.

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 5.2.3.2.2).

5.2.3.1.2 Link between safety categories, safety classes and security degrees

The security graded approach described in this standard 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 cyber attack, there is not a strict one-to-one mapping for I&C systems between their safety class and their security degree.

5.2.3.1.3 Description of the security degrees and associated assignment criteria

This standard defines three security degrees, S1, S2 and S3, to which graded security requirements are associated (as defined in 5.2.3.2). 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 5.2.3.1.1) 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 CB&HPD systems as follows:

   – I&C CB&HPD systems processing safety category A functions to security degree S1,

- I&C CB&HPD systems needed for real-time operation and I&C CB&HPD systems processing safety category B functions to no lower than security degree S2,
- I&C CB&HPD systems for Category C according to the maximum consequences, and I&C CB&HPD systems assisting plant operation and maintenance to security degree S3.

NOTE 1 As stated in 5.2.3.1.2, there is not a one-to-one mapping between safety categorization and security degrees. For instance, I&C CB&HPD systems needed for real-time 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 A provides explanations about the justification for having three security degrees for I&C CB&HPD systems, and other complementary information.

NOTE 2 This standard 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.

NOTE 3 See 5.2.3.2.7 for computer tools.

5.2.3.2 Assignment of technical requirements

5.2.3.2.1 General

Security requirements valid for all I&C CB&HPD systems are given in 5.2.3.2.3. To these requirements shall be added requirements given in 5.2.3.2.4 for S1-graded systems, requirements given in 5.2.3.2.5 for S2-graded systems and requirements given in 5.2.3.2.6 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.

Requirements applicable to computer based tools, in particular those for I&C system maintenance and diagnostic purposes, are given in 5.2.3.2.7.

5.2.3.2.2 Link with security risk assessment activity and Design Basis Threats

The I&C CB&HPD system security programme of the NPP shall include threat and vulnerability assessment. 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).

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. Security provisions shall be compatible with designed functional performance of the solution.

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;
- likelihood of successful exploitation;

- 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.

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 CB&HPD system. The number of potential threats and vulnerabilities usually increases with progress from stand-alone to interconnected systems.

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 CB&HPD 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 CB&HPD systems or subsystems from the onset of a project. They are based on the potential consequences, as defined in 5.2.3.1.1, of a security attack on I&C systems or on functions they implement. Security degrees, via associated requirements, help specify systems.

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

5.2.3.2.3 Generic requirements

The following requirements apply to all I&C CB&HPD 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 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 requirements for additional countermeasures.

e) The security policy shall be adapted to each I&C system or group of systems. An informal or formal correspondence should be established between the overall security policy and its adaptation to the I&C systems or groups of systems.

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, shall restrict access to the minimally necessary extent, both in terms of authorized staff and authorized operations.

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 CB&HPD systems and systems monitoring safety-classified I&C CB&HPD 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 cyber attack. Measures shall be put in place to minimize the possibility that these arrangements are themselves vulnerable to the same cyber threats.

5.2.3.2.4 Degree S1 additional requirements

The minimum set of security requirements for S1-graded I&C CB&HPD systems (in addition to the generic 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 CB&HPD communications shall be restricted to other S1-graded I&C CB&HPD systems and to S2-graded I&C CB&HPD systems, and to their associated tools.

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

5.2.3.2.5 Degree S2 additional requirements

The minimum set of security requirements for S2-graded I&C CB&HPD systems (in addition to the generic 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.

5.2.3.2.6 Degree S3 additional requirements

The minimum set of security requirements for S3-graded I&C CB&HPD systems (in addition to the generic 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 duly justified and the connection shall be monitored.

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

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.

Lower security degree may be assigned in case of indirect connection, involving procedural and/or human control. If the 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.

Associated security requirements for computer tools should be adapted as follows.

- 5.2.3.2.3 (generic requirements) holds for all computer tools.
- For S1 degree, 5.2.3.2.4 holds except for its item g) (dealing with alarms) which is not relevant for 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, 5.2.3.2.5 holds except for its items c), d) and f) which are not relevant for 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, 5.2.3.2.6 holds (same requirements).

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

5.2.3.3 Security zones

A possible practical implementation of the graded approach is to group I&C CB&HPD systems into logical zones, where graded protective principles are applied for each security zone (see definition in 3.17). 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), localisation, architectural or technical aspects.

NOTE 1 In the rest of this standard, the term "zone" refers to "security zone" as defined in 3.17 and in this subclause. It does not refer to safety zones and the associated geographical separations (although some relations exist).

The application of a zone model should comply with the following guidelines:

- Each zone comprises systems that have the same degree of security. If for architectural or other reasons, a I&C CB&HPD system has a less stringent security degree (as per 5.2.3.1.3) 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 2 Security degrees are formally assigned to I&C CB&HPD 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.

- 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.
- 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 standard). If the zones have different security degrees, then the security requirements associated to security degrees apply (see 5.2.3.2.3 to 5.2.3.2.6). In particular those dealing with communications and interfaces between systems of different security degrees shall involve dedicated security provisions.

- 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).
- Zone borders require decoupling mechanisms for data flow, consistent with the security degree of the associated I&C CB&HPD systems.

The relationship between security zones and security degrees is not one-to-one; a degree may be assigned to multiple zones when multiple zones may require the same security degree. Zones are a logical and/or physical grouping of computer systems, while security degrees represent the degree of protection required.

5.2.4 Management approval

A management review of the overall I&C CB&HPD system security programme shall be undertaken on a regular basis. The output from the management review and approval shall include any decisions and actions related to the following:

- implementation of and modifications to procedures and controls that affect the I&C CB&HPD 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;
- initial criteria and improvements to how the effectiveness of controls is being measured;
- decision process and criteria to take actions impacting plant operations (e.g., continued plant operation, plant shutdown, communication isolation, equipment maintenance).

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.

5.3 Implement and operate the programme

5.3.1 Implementation of general requirements

The organization shall do the following:

- develop a I&C CB&HPD system security programme that satisfies the general security requirements of this standard;
- develop an implementation plan that identifies management action, resources and priorities for managing I&C CB&HPD systems risks;
- implement a I&C CB&HPD system security programme utilizing identified operational, management and technical controls and/or mitigating actions to adequately manage risks;
- implement continuing maintenance, update and security incident response efforts to ensure continued protection for I&C CB&HPD systems against cyber attack;
- implement all plans with consideration of funding, allocation of roles and responsibilities and management support.

5.3.2 Effectiveness measurement definition

Successful implementation and operation of a I&C CB&HPD system security programme requires that metrics be in place to measure the effectiveness of the utilized security controls

or groups of controls. These metrics allow the organization to assess how well the controls achieve planned objectives.

During the I&C CB&HPD system security programme development phase, the organization should:

- Define effectiveness metrics for each individual control utilized in the programme.
- Define effectiveness metrics for groupings of controls that are considered a distinct entity and credited as such in the security plan.
- Determine implementation specific variations for controls and groups of controls that require variations in measurement metrics.
- Define metrics to quantify effectiveness of mitigating actions which justify continued absence of security controls.
- Prepare a consolidated set of detailed information on identified metrics linked to the specific control to support efficiency and standardization of the control effectiveness monitoring effort.

5.3.3 Training and awareness

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

- A formal training programme for personnel designing and supporting I&C systems shall be developed and delivered.
- 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.
- Awareness and training shall involve organizations or individuals who have expertise in I&C CB&HPD system security, ideally in the context of nuclear power plants.

5.4 Monitor and review the programme

A major element of maintaining an effective I&C CB&HPD 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. As a consequence, the organization shall:

- Establish a review programme that addresses the purpose, scope, roles, responsibilities, requirements and management commitment associated with reviewing elements of the I&C CB&HPD system security programme for effectiveness.
- Establish procedures to facilitate and maintain the review programme including required frequency of reviews, and qualifications of individuals performing the reviews.

5.5 Maintain and improve the programme

The I&C CB&HPD system security programme shall establish the process to:

- Implement programme improvements identified during internal and external programme reviews including corrective and preventive actions.
- 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.
- Develop and implement a review programme to periodically evaluate and update the security threat assessment.
- Establish measures to evaluate whether the improvements achieved their intended objectives.

6 Life-cycle implementation for I&C CB&HPD system security

6.1 General

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

6.2 Requirements activities

A top-down approach, considering the global I&C architecture to the individual systems and components, shall be used. 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 design vulnerabilities evaluations are possible at this stage.

Individual systems or components may be supplied and secured by different suppliers, provided the security of the whole architecture is consistently maintained. A security degree, as defined in 5.2.3.1, and associated security requirements shall be assigned to each system. These systems may be assigned to security zones with additional security requirements.

6.3 Planning activities

6.3.1 Identification of I&C CB&HPD systems

Each I&C CB&HPD system within the plant or facility design shall be identified. At this point in the process, it is a list of I&C CB&HPD systems without the detailed design or component selections completed, which are part of the plant design.

6.3.2 Security degree assignment

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

6.4 Design activities

6.4.1 General

Subclause 6.4 describes the specific design configuration items of a I&C CB&HPD system designed to the requirements defined in 6.2 above.

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 control over (a) physical and logical access to the I&C system functions, (b) use of the I&C system, and (c) data communication with other I&C systems. The designer should ensure that the software code design complies with appropriate design standards, to address potential vulnerabilities that can be introduced as part of the design process. A specific interest should be given to configuration management. The requirements shall be translated into specific design criteria. 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.

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

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). Risk assessments may lead to improve the security measures. 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

The I&C security plan shall apply to the primary design organization and all third party or subcontractor organizations working on the project. A design project security plan, covering the licensee/operator but also third-parties and external entities involved in the project, shall be established. In particular, the designer shall show that:

- he has a security policy in place;
- such a policy applies for each of its development sites;
- it is completed along local aspects;
- it ensures that its own third-parties meet an adequate security level.

6.4.4 Communication pathways

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. Cyber security controls shall be established to:

- Enforce and document assigned authorizations for controlling the flow of information, within and between interconnected systems in accordance with their assigned security degrees (see 5.2.3.3).

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

- Maintain documentation that demonstrates the analysis and addressing of permissible and impermissible flow of information between systems and devices addressed in the I&C CB&HPD system security programme, consistently with the risk assessment and graded approach described in 5.2.2.

6.4.5 Security zone definition

Security zones (see 3.17 and 5.2.3.3) should be defined during the design phase. They may alternatively be defined in the implementation phase (see 6.5). Assignment of I&C CB&HPD systems to security zones shall take into account, as per 5.2.3.1.2, the security degree assigned previously to each I&C CB&HPD system during the planning phase.

6.4.6 Security assessment of the final design

Security assessments shall ensure a complete coverage of the complete I&C architecture at the final design stage.

6.5 Implementation activities

This subclause is focused on implementation of the secure design for creation of secure hardware and software. In the implementation phase, hardware and software shall be integrated per the system design including all defined security requirements.

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.

6.6 Validation activities

Verification and Validation (V&V) testing per required standards shall be performed for the specified security requirements of I&C CB&HPD systems. Additionally, testing shall verify the I&C security design of the hardware architecture, external communication devices and configurations for unauthorized pathways and system integrity. The security requirements and configuration items shall be part of validation of the overall system requirements and design configuration items. 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.

6.7 Installation and acceptance testing activities

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 CB&HPD system security programme, as applicable. 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.

6.8 Operation and maintenance activities

6.8.1 Change control during operations and maintenance

During the operational and maintenance phase, the periodic security audits of security features shall be performed. 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. 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 5.2.3.2.7.

6.8.2 Periodic reassessment of risks and security controls

The effectiveness of the security controls implemented into the system shall be reassessed on a periodic basis. Testing of security controls shall also be conducted if necessary to verify the effectiveness of controls following specific events.

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

6.9 Change management

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

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.

Unauthorized or undocumented changes to network configuration or characteristics by the plant personal or a third-party can void the integrity of the I&C security defensive model. Therefore, careful control of design and maintenance practices shall be provided to prevent violations of this type.

6.10 Retirement activities

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

An effective continuing programme shall address the retirement lifecycle phase. Procedure(s) shall be in place to address proper retirement of I&C CB&HPD devices and disposal of media and resident software in a controlled manner, to avoid disclosure of sensitive information. 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 specific considerations to take into account in nuclear I&C environments when selecting and enforcing security controls in the framework of a programme elaborated according to Clause 5 and Clause 6 requirements. It is organized along the eleven security thematic areas covered in ISO/IEC 27002 and the Annex A of ISO/IEC 27001:2005.

NOTE ISO/IEC 27002 uses the term “security categories”. In the frame of this IEC standard, the term “security thematic area” has been preferred in order to avoid confusion with “safety categories.”

Some statements, recommendations and requirements of this clause may be redundant with the ones made in former clauses: this is because some controls are programmatic in essence and already dealt with for this reason in these former clauses. However, the interest and objective of the present clause are to put them in perspective (and in some cases complete them) through the eleven security thematic areas of the ISO/IEC 27000 series framework.

This clause does not provide a detailed or exhaustive list of security controls. The specific implementation should be designed taking into account the specific technical, operational and managerial issues involved in context with the considered nuclear power facility.

7.2 Security thematic areas

7.2.1 Security policy

The objective of this subclause is to provide plant management direction and support for I&C CB&HPD system security in accordance with business requirements, safety considerations, and plant performance while being compliant with all applicable national laws and regulations.

Plant management shall set a clear policy direction in line with regulation and overall security requirements (including corporate security policy, physical security, and cyber security) through the issue, implementation and management of an organizational wide security policy.

7.2.2 Organizing security

The objective of this subclause is to manage security of I&C CB&HPD systems within the facility.

A management framework shall be established to initiate and control the implementation of a I&C CB&HPD system security programme in all I&C CB&HPD system life cycle phases. The framework shall take into account the different knowledge base, threat issues and operational considerations that differentiate I&C systems and their associated experts. Support for onsite security specialists should be provided if supportable by the organization.

Identification and establishment of links and technical exchanges with external security specialists and groups, including national and international authorities should be

accomplished. Ongoing and interactive cooperation with these resources should be an integral part of the security management process.

7.2.3 Asset management

The objective of this subclause is to achieve and maintain the appropriate protection of assets to ensure safe operation and performance, compliant with appropriate national laws and regulations.

All assets shall be accounted for and have a responsible owner.

The responsibility for maintenance and operational compliance of appropriate controls should be assigned. While the implementation of appropriate controls may be delegated by the owner as appropriate, the owner should be responsible for the proper protection and functionality of the asset. The owner should be responsible for maintaining compliance of asset with the national regulations and ensuring that asset and respective controls are properly identified, evaluated and maintained as per system security plan. Owner should be responsible for proper evaluation of asset's risk component and overall level of vulnerability as discussed in Clause 5 and ensuring that appropriate and effective measures are utilized for asset protection. Owner should also be responsible for ensuring that new and emergent threats do not impact the required operation of asset – to the extent required by the system risk assessment.

7.2.4 Human resources security

The objective of this subclause is to ensure that employees, contractors and authorized third parties understand their responsibilities, are suitable and qualified for the roles they are considered for and/or assigned, and to minimize the risk of theft, fraud, misuse or intentional sabotage of the facility.

Security responsibilities should be addressed prior to employment in job descriptions and terms and conditions of employment. Ongoing training, awareness and education programs should be utilized to minimize potential security risks. Formal processes for handling of security infractions should be established.

All candidates for employment, contractors and authorized third parties should be adequately screened, especially – but not limited to – sensitive positions. Appropriate national regulation and law shall be followed for hiring procedures and coordination/utilization of national authorities should be utilized for background screening to the extent possible.

Employees, contractors and authorized third parties should sign agreements acknowledging their agreement on security roles and responsibilities, prior to employment.

Ongoing personnel reliability programs should be utilized to identify potential issues.

Upon reassignment or termination of employment, employees, contractors and authorized third parties should be briefed on any continuing security requirements imposed and agree in writing. Access to equipment, facilities and resources shall be terminated once the employee or third party contractor is terminated or reassigned and all equipment should be returned expeditiously and access to the equipment terminated.

Reassignment should be treated in the same way as termination with subsequent hiring into the new position. An exception may be made with regard to background checks if the new assignment is of the same or a lower required access level.

7.2.5 Physical and environmental security

Physical protection is outside the scope of this standard. Nevertheless, it is recognized that fundamental aspect and basis for I&C system security protection depends on physical security and physical protection as implemented by national laws and regulations.

7.2.6 Communications and operations management

The objective of this subclause is to ensure the correct and secure operation of the facility.

Responsibilities and procedures for management and operation of the facility in case of attacks on I&C CB&HPD systems shall be established. This includes the development of appropriate operating procedures. The safe and reliable operation of a nuclear power facility requires detailed and accurate operational procedures for the facility which should be tied into the computer security requirements.

7.2.7 Access control

The objective of this subclause is to control logical access to facilities I&C systems' information and operation.

Security degree, as defined in 5.2.3.1.3, should be the basis for required levels of access control. Access control shall take into account established policies for information dissemination and authorization and as well operational access constraints.

Access controls should not prevent or degrade any safety or control action that may be required by an operator or other legitimate user.

7.2.8 I&C systems acquisition, development and maintenance

The objective of this subclause is to ensure systems are developed and maintained in an appropriate and secure manner commensurate to their security degree.

Systems should have cyber security elements considered and designed in from the requirements stage.

Designers and developers shall have established and verified secure development methodologies in place throughout the development lifecycle of a system.

All subcontractors and other support companies and staff that have involvement with systems development should be required to adhere to the same requirements as the primary developer. In particular, the I&C CB&HPD designer/provider shall show that it has a security policy in place, applying to each of its development sites in accordance with local security policy and procedures.

Contractual requirements for secure systems development should be written into all acquisition efforts.

Hardware acquisition efforts should have procedures in place to ensure equipment used in system development and operation is cyber secure and not provided in an already compromised state.

Maintenance procedures should be developed and in place to ensure all required and appropriate recommended security upgrades are applied as soon as reasonable to maintain system security. Published vulnerabilities (e.g. those published by control system vendors and CERTs) should be continuously monitored and appropriate measures should be taken if I&C CB&HPD systems in use are affected by a known vulnerability.

Prior to any patches and/or upgrades, system functionality shall be verified to ensure that such patch or upgrade will not impact the safety function of the system.

Any graded approach to recommendations and requirements during development, operation and maintenance shall be based upon assigned security degree (as per 5.2.3).

System designers shall ensure that all security controls necessary to be supplied by vendor products and services are adequately documented in procurement documentation. Vendors shall supply evidence of compliance to such security controls, including functionality, testability, necessary upgrade procedures, configuration management policies/procedures, change control policies/procedures, etc. Any exceptions made to security controls shall be assessed by the system designers and either accepted as is with appropriate justification or with compensating measures in system design documentation.

7.2.9 I&C security incident management

The objective of this subclause is to ensure I&C security events associated with I&C systems are identified and mitigated in a timely manner.

Formal event reporting and response procedures shall be in place. All system users should be formally trained and made aware of policies, procedures and practices for response to suspected and confirmed cyber attacks and other security events. Any potential security event identified should be reported to a designated point of contact (organization not individual to provide for continuity). External information resources should be actively monitored for potential security threats and appropriate action taken as needed.

A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of I&C CB&HPD cyber security incidents.

Training aspects and procedures enabling the identification of potential cyber security incident should be in place.

7.2.10 Operation continuity management

The objective of this subclause is to counteract interruptions to activities from the effects of major failures of I&C systems due to malicious actions and to ensure their timely resumption.

Processes to support operation continuity management with regards to cyber security and the impact of malicious events should be integrated into the facilities existing operation continuity programmes.

This programme should identify the processes and procedures required to resume full operation at the facility after a cyber event. Reduced levels of I&C operational capability should be planned for and evaluated in the overall continuity plan. Differentiations should be made between functioning safety functions as a minimal level and full plant availability as the highest level. Variations to this scale should be made depending upon nation specific regulations and guidance.

Procedures which are rarely executed (e.g. emergency procedures) should be routinely practiced to ensure they can be appropriately executed when necessary and under stress.

7.2.11 Compliance

The objective of this subclause is to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The design, operation, use and management of nuclear power plant I&C systems will be subject to statutory, regulatory or contractual obligations. In many cases these requirements

will differ between nations. Advice on legal and regulatory compliance should be sought from the facility or organization's legal and regulatory experts or other qualified personnel. This guidance should present information in a manner that guarantees compliance with regulation and law in all nations. Requirements vary from country to country.

Privacy and intellectual property rights shall be protected to the degree required by appropriate law at a minimum.

Annex A
(informative)

Generic considerations about the security degrees

A.1 Rationale for three security degrees

A.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 CB&HPD systems. However, if this eases linkage between the two scales, there is not a one-to-one mapping between safety categories and security degrees.

NOTE This standard only deals with I&C CB&HPD 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.

Indeed, in the context of this standard, 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.

A.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 a I&C CB&HPD system is, the more stringent its security degree has to be, the following has been proposed:

- I&C CB&HPD systems processing safety category A functions involve the most stringent security degree (S1),
- I&C CB&HPD systems processing safety category B functions involve at least an intermediate security degree (S2),
- I&C CB&HPD 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 CB&HPD 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.

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

The security classification of I&C CB&HPD systems necessary to plant availability and performance is then to be considered.

Consequences of a cyber-attack on I&C CB&HPD 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 cyber-attack on a S2 security classified CB system.

A.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 CB&HPD systems, integrating plant safety and availability dimensions:

- S1 for I&C CB&HPD 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 CB&HPD systems processing safety categories B functions or functions which could have the same impact on safety when manipulated maliciously (including potentially specific C or non-classified functions) and systems processing functions necessary to operate the plant,
- S3 for I&C CB&HPD systems which cannot impact in real time either plant safety or plant availability.

Regarding plant safety or availability, the security degree of a I&C CB&HPD system may be upgraded to the degree corresponding to consequences of a successful cyber-attack on the most sensitive function it processes.

A.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.

A.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 shall be analyzed in order to assign them an adequate security degree.

The second step consists of a vulnerability analyses for each system.

The third step aims at designing proper cyber-protection for each I&C system taking account of the generic requirements associated to its degree and the results of its vulnerability analyses.

Annex B
(informative)

Correspondence with ISO/IEC 27001:2005

Table B.1 – Correspondence between IEC 62645 and ISO/IEC 27001:2005 on a structural level

ISO/IEC 27001 structure	Correspondence with IEC62645	Remarks
Foreword	**Foreword**	
0 Introduction	**Introduction**	
0.1 General		
0.2 Process approach		
0.3 Compatibility with other management systems		
1 Scope	**1 Scope**	Scope breakout in IEC 62645 is aligned with IEC 61513.
1.1 General		The correspondence is on the formal presence of the subclause, not on the content
1.2 Application		
2 Normative references	**2 Normative references**	
3 Terms and definitions	**3 Terms and definitions**	There is no such subclause in ISO/IEC 27001 (Clause 4 in 62645:2014)
4 Information security management system	**5 Establishing and managing a nuclear I&C CB&HPD system security programme**	
4.1 General requirements	5.1 General	
4.2 Establishing and managing the ISMS	5.2 to 5.5, see infra.	
4.2.1 Establish the ISMS	5.2 Establish the programme	IEC 61226 structure has been used. ISO/IEC 27001:2005, 4.2.1 a) → IEC 62645:2014,5.2.1 b) → 5.2.2 c) – g) → 5.2.3 h), i) → 5.1.2 j) → no equivalence
4.2.2 Implement and operate the ISMS	5.3 Implement and operate the programme	ISO/IEC 27001:2005, 4.2.2 a) – c) → IEC 62645:2014, 5.3.1

ISO/IEC 27001 structure	Correspondence with IEC62645	Remarks
		d) → 5.3.2 e) → 5.3.3 f) – h) → 5.1.2
4.2.3 Monitor and review the ISMS	5.4 Monitor and review the programme	
4.2.4 Maintain and improve the ISMS	5.5 Maintain and improve the programme	
4.3 Documentation requirement	5.1.3 Documentation requirements	
4.3.1 General		
4.3.2 Control of documents		
4.3.3 Control of records		
5 Management responsibility	5.1.2 Roles and responsibilities	
5.1 Management commitment		
5.2 Resource management		
5.2.1 Provision of resources		
5.2.2 Training, awareness and competence		
6 Internal ISMS audits	**Maybe integrated in 5.3 and 5.4**	
7 Management review of the ISMS	**Maybe integrated in 5.3 and 5.4**	
7.1 General		
7.2 Review input		
7.3 Review output		
8 ISMS improvement	**Maybe integrated in 5.4**	
8.1 Continual improvement		
8.2 Corrective action		
8.3 Preventive action		
Annex A (normative) Control objectives and controls	**7 Security controls**	

Annex C
(informative)

Correspondence with NIST security framework

C.1 Scope

The scope of this annex is to provide a qualitative comparison between the overall security framework described in this standard to that of the framework developed by the National Institute of Standards and Technology (NIST). This is accomplished by comparing the document structure of this standard to the structure of NIST SP 800-82 dated September 2008 (final public draft) and other supporting NIST documentations.

This comparison is not to be considered as an equivalency between the two documents; however it can be used as a guide to develop such an equivalency. Keep in mind that the NIST publication is not a standard in the strictest sense, but rather a guideline document providing best practices to develop a cybersecurity framework for industrial control systems. Also, the NIST publication is not focused on one particular industry and is intended for US Federal agencies, however it can be applied to other organizations and industries.

NOTE Information in the NIST standard described herein was used extensively in the requirements for nuclear power plant cyber security controls in the U.S. in Reg Guide 5.71 and NEI 08-09.

It is recommended that this annex be updated whenever this standard, or the NIST publication, are revised. A future version of this annex may provide a more detailed subclause-by-subclause analysis between the two standards to provide a better correlation between them.

C.2 Correspondence between IEC 62645 and NIST SP 800-82

Table B.1 provides a general correspondence between the cybersecurity framework developed in this standard to that developed by NIST for Industrial Control Systems. The majority of the NIST cybersecurity framework is described in NIST SP 800-82, however other NIST publications provide guidelines on specific aspects of a cybersecurity framework. These other publications will be highlighted in the table. The correspondence in Table B.1 is based on the current structure of this IEC standard and a comparison of appropriate subclauses in the NIST publication(s). Any deviations, special cases, or notes are provided in the third column of the table.

NOTE The correspondence between this standard and the NIST publication(s) does not mean that the requirements in this standard are adequately addressed by similar requirements in the NIST publication(s) (or vice versa). It is intended to provide a general structural comparison so that further detailed requirements-based comparisons can be completed in the future.

Table C.1 – Correspondence between IEC 62645 and NIST SP 800-82 on a structural level

IEC 62645 structure	Correspondence with NIST SP 800-82	Remarks
5 Establishing and managing a nuclear I&C CB&HPD system security programme		
5.1 General		
5.1.1 Overall concepts: programme, policies and procedures		
5.1.2 Roles and responsibilities	4.2.3 Define Charter and Scope	This subclause qualitatively describes that roles and responsibilities shall be agreed upon and documented.
	4.2.3 Define Charter and Scope 4.2.4 Define ICS Specific Security Policies and Procedures	
5.1.3 Documentation requirements	4.2.3 Define Charter and Scope 4.2.4 Define ICS Specific Security Policies and Procedures 4.2.5 Define and Inventory ICS Systems and Networks Assets NIST SP 800-53A	The NIST cybersecurity framework does not provide a specific subclause outlining documentation requirements/guidelines, however various lifecycle stages of a security programme describe aspects of the the programme that should be documented.
5.2 Establish the programme	4.2 Developing a Comprehensive Security Program	
5.2.2 Defining the programme scope and boundaries	4.2.3 Define Charter and Scope	
5.2.1 Defining security policy	4.2.4 Define ICS Specific Security Policies and Procedures	NIST SP 800-82 covers discussions on both policy and approach, including risk-based assessments and graded security measures.
5.2.3 Graded approach to I&C security and risk assessment	4.2.5 Define and Inventory ICS Systems and Networks Assets 4.2.6 Perform Risk and Vulnerability Assessment	
5.2.4 Management approval	4.2.1 Senior Management Buy-in	NIST SP 800-82 4.2.1 is very brief with no details, however, 4.1 develops the business case for cybersecurity to obtain management approval.
5.3 Implement and operate the programme		

IEC 62645 structure	Correspondence with NIST SP 800-82	Remarks
5.3.1 Implementation of general requirements	4.1 Business Case for Security 4.2.6 Perform Risk and Vulnerability Assessment 4.2.7 Define the Mitigation Controls	Although NIST SP 800-82 does not have clear or specific guidelines on the implementation of the cybersecurity plan, implementation guidelines are presented in the various subclauses of the document. For example 4.1 discusses that costs and resources should be considered for implementation, 4.2.6 discusses a risk-based approach should be implemented, and 4.2.7 discusses the implementation of sufficient mitigation controls to limited risks due to cybersecurity threats.
5.3.2 Effectiveness measurement definition	NIST SP 800-53A, chapter 2	
5.3.3 Training and awareness	4.2.8 Provide Training and Raise Security Awareness 6.2.9 Awareness and Training	NIST SP 800-82 6.2.9 provides additional guidance located in NIST SP 800-12, 16, 50, and 53.
5.4 Monitor and review the programme	NIST SP 800-53A, chapter 3	
5.5 Maintain and improve the programme	NIST SP 800-53A, chapter 3	3.4 provides a general qualitative discussion about the assessment of security reports, actions resulting from them, and the update and maintenance of the programme.
6 Life-cycle implementation for I&C CB&HPD system security		
6.1 General		
6.2 Requirements activities	NIST SP 800-53, 3.1 Managing Risk, and 3.2 Categorizing the Information System	The requirements phase is described as assessing the I&C systems for security risks and selecting suitable mitigating controls based on several factors to minimize those risks.
6.3 Planning activites		
6.3.1 Identification of I&C CB&HPD devices	4.2.5 Define and Inventory ICS Systems and Networks Assets 4.2.6 Perform Risk and Vulnerability Assessment	
6.3.2 Security degree assignment		
6.4 Design activities	NIST SP 800-53, 3.3 Selecting Security Controls	
6.5 Implementation activities	NIST SP 800-53, 3.4 Monitoring Security Controls	The implementation, testing, and installation phase guidelines are provided throughout chapter 3 of the NIST publication. Detailed lifecycle stages are not described in the NIST publication however these aspects of the lifecycle stages are likely covered in chapter 3.
6.6 Validation activities		
6.7 Installation and acceptance testing activities		

IEC 62645 structure	Correspondence with NIST SP 800-82	Remarks
6.8 Operations and maintenance activities	6.2.5 Maintenance 6.2.6 System and Information Integrity NIST SP 800-53	
6.9 Change management	6.2.4 Configuration Management NIST SP 800-53	
6.10 Retirement activities		NOTE No particular guidance is provided in the NIST framework covering the retirement aspects of I&C system in relation to cybersecurity issues. Guidance/requirements from this standard should be considered.
7 Security controls	**6 ICS Security Controls**	
7.1 General		
7.2 Security thematic areas	6 ICS Security Controls	
7.2.1 Security policy	4.2.3 Define Charter and Scope 4.2.4 Define ICS Specific Security Policies and Procedures	
7.2.2 Organizing security	6.1.2 Planning NIST SP 800-53	
7.2.3 Asset management	6.3.1 Identification and Authentication 6.3.2 Access Control NIST SP 800-53	
7.2.4 Human resources security	6.2.1 Personnel Security 6.2.9 Awareness and Training NIST SP 800-53	
7.2.5 Physical and environmental security	6.2.2 Physical and Environmental Protection NIST SP 800-53	
7.2.6 Communications and operations management	6.3.4 System and Communications Protection NIST SP 800-53	

IEC 62645 structure			Correspondence with NIST SP 800-82	Remarks
		7.2.7 Access control	6.2.7 Media Protection 6.3.1 Identification and Authentication 6.3.2 Access Control NIST SP 800-53	
		7.2.8 I&C systems acquisition, development and maintenance	6.1.3 System and Services Acquisition 6.2.5 Maintenance 6.2.6 System and Information Integrity NIST SP 800-53	
		7.2.9 I&C security incident management	6.2.6 System and Information Integrity 6.2.8 Incident Response NIST SP 800-53	
		7.2.10 Operation continuity management	6.2.3 Contingency Planning NIST SP 800-53	
		7.2.11 Compliance	6.3.3 Audit and Accountability NIST SP 800-53	

Annex D
(informative)

Attackers profiles and attack scenarios

A possible set of attacker profiles is established concerning both internal/insider threats and potential external threats for the particular facility. Some country-specific design basis threat (DBT) include cybersecurity aspect and are inputs in this process. Types of attackers are described considering their resources, the time span of the attack, the tools that are likely to be used and the attacker's motivations. An adequate process of intelligence gathering is established to ensure the completeness and relevance of each facility's attacker matrix.

Security organization of the facility builds up data on feasible attack scenarios. The I&C system of nuclear facility can be attacked with the purpose of:

- building up a later coordinated attack intended to sabotage the plant and/or to remove nuclear material;
- endangering human or environmental safety;
- launching an attack towards another site;
- creating confusion and fear;
- gaining monetary profit for a criminal group of people;
- creating major market instabilities and gains for selected market players.

Depending on the objectives or aims of the attack, the attacker is likely to exploit different system vulnerabilities. Such attacks can lead to:

- unauthorized access to information (loss of confidentiality);
- interception and change of information, software, hardware, etc. (loss of integrity);
- blockage of data transmission lines and/or shutdown of systems (loss of availability);
- unauthorized intrusion into data communication systems or computers (loss of reliability).

All these aspects can have major consequences and impacts on the functionality of the I&C systems, which may, directly or indirectly, compromise the safety and security of the facility. When building up attack scenarios, the technological trends and ease of access to attack technologies are to be considered. See reference [IAEA Nuclear Security Series No. 17] for some scenarios illustrating fictional, but realistic, attacks on the I&C systems. Typically access to I&C systems is granted based upon rights granted to roles associated with real staff members of a nuclear power plant. Such model is to be defined within the security policy of the power plant and all I&C systems installed need to provide the capabilities required to enforce such access control on the level of both, physical and logical access. Since modern I&C systems may be accessed through communication channels without any kind of physical access to the system, all communication channels taken together are called logical access. The access control further considers direct and indirect communication channels. The direct ones are obviously identifiable by showing an initiator and a target[1], the indirect ones are more difficult to identify since they could hide themselves in direct communication channels or be intentionally transferred objects of code or data. As a consequence of this, measures need to be designed into I&C safety system environments that allow effective countermeasures to block unauthorized direct and indirect access.

[1] Initiators may be humans or technical systems, the targets are considered to be the I&C system to be protected.

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*

IAEA Nuclear Security Series No. 17:2011, *Reference Manual, Computer Security at Nuclear Facilities*

NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, MD, August 2009

NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security – Computer security,* National Institute of Standards and Technology, Gaithersburg, MD, 2011

U.S. Nuclear Regulatory Commission Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities*, January, 2010.

ISA TR99.02.01-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*

U.S. Nuclear Regulatory Commission Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, Rev. 2

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*

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

PIETRE-CAMBACEDES, L., TRITSCHLER, M., and ERICSSON, G. N., "Cybersecurity myths on power control systems: 21 misconceptions and false beliefs", *Power Del., IEEE Transactions on*, 2011, vol. 26, no 1, p. 161-172

BRUNDLE, M. and NAEDELE, Martin, "Security for process control systems: An overview", *Security & Privacy, IEEE*, 2008, vol. 6, no 6, p. 24-29

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

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

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

Le texte de cette norme est issu des documents suivants:

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

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

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

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

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Domaine d'application

1.1 Généralités

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2 Application

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

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

1.3 Cadre général

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

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

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

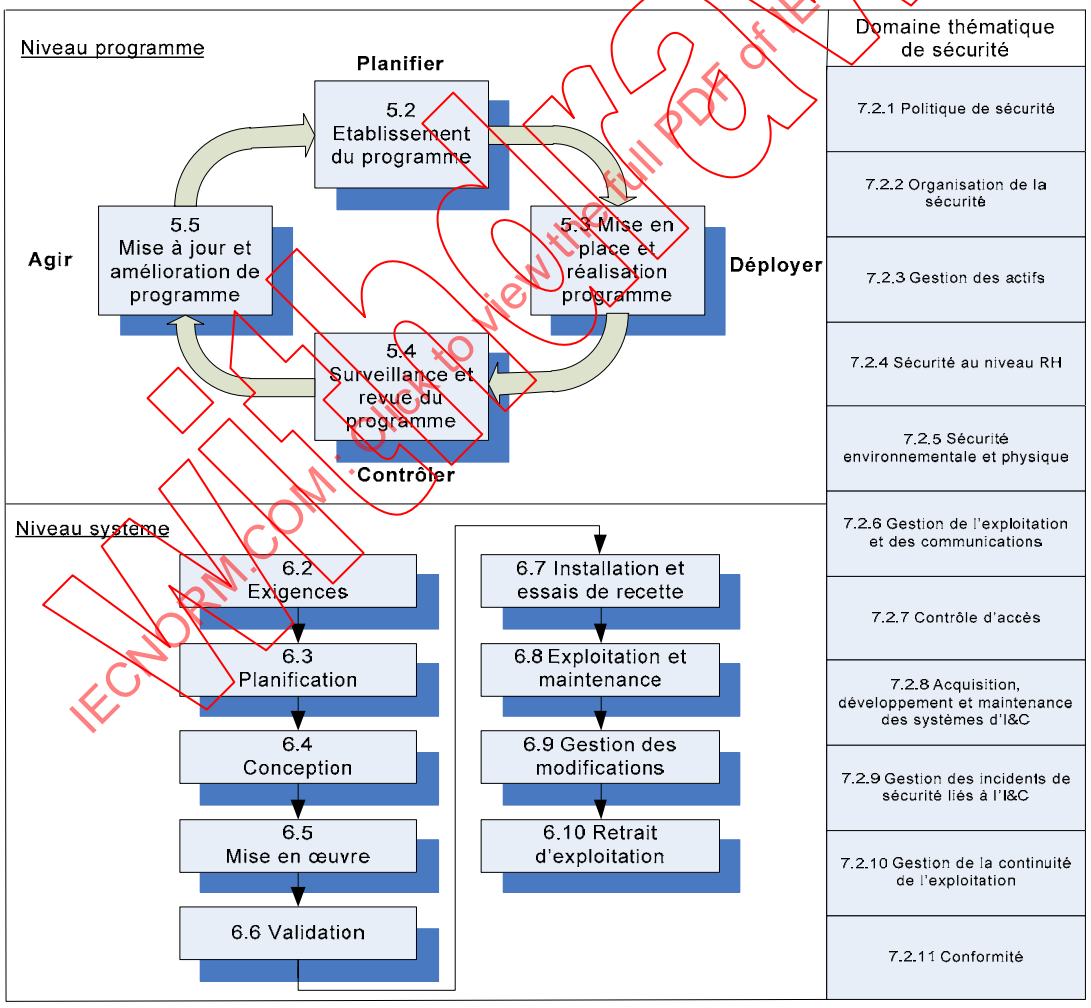

Figure 1 – Cadre général de l'IEC 62645

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

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

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

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

2 Références normatives

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

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

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

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

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

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

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

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

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

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

3 Termes et définitions

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

3.1
vecteur d'attaque
chemin ou moyen par lequel un programme malveillant ou attaquant peut avoir accès à un système programmé

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
système programmé
système d'I&C dont les fonctions dépendent en grande partie, ou sont totalement effectuées à l'aide de microprocesseurs, d'un matériel électronique programmé ou d'ordinateurs

Note 1 à l'article: Dans le contexte de la présente norme, ordinateur, système programmé, système numérique, appareil numérique, système informatique sont tous synonymes.

Note 2 à l'article: Dans le contexte de la présente norme les systèmes programmés-HPD d'I&C comprennent des sous systèmes programmés mais aussi potentiellement des sous systèmes réalisés à base de HPD et tous les composants susceptibles de contenir de l'électronique. Voir aussi la définition de HPD.

[SOURCE: IEC 60880:2006, 3.11]

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

- la divulgation d'informations qui pourraient être utilisées pour réaliser des actes malveillants qui pourraient amener à un accident, une situation non sûre ou dégrader les performances de fonctionnement de la centrale (confidentialité),
- les modifications malveillantes de fonctions qui pourraient porter atteinte à la fourniture ou à l'intégrité d'un service demandé par des systèmes programmés-HPD 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 l'installation (intégrité),
- la rétention, la prévention pour l'accès à ou la communication d'informations, de données ou de ressources (y compris la perte de vue) malveillantes qui pourraient compromettre la

fourniture par un système d'I&C d'un service demandé qui pourrait avoir pour conséquence un accident, l'apparition d'une situation non sûre ou une dégradation des performances de l'installation (disponibilité).

Note 1 à l'article: Cette définition est taillée sur mesure par rapport au domaine de la présente norme, se concentrant sur la prévention, la détection et la réaction aux actes malveillants portant atteinte aux systèmes programmés-HPD d'I&C en utilisant des moyens numériques. Il est reconnu que terme «cybersécurité» à un sens plus large au niveau des autres normes et documents guide et souvent qu'il couvre les menaces non malveillantes, les erreurs humaines et la protection contre les risques naturels, qui sont en dehors du domaine de la présente norme (voir 1.1).

Note 2 à l'article: Dans le cadre de la présente norme, sécurité informatique et cybersécurité sont considérées comme synonymes et «accès non autorisé» est synonyme de «accès logique non autorisé».

3.7
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]

3.8
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.

[SOURCE: AIEA INFCIRC/225/Rev.4:1999, modifié]

3.9
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 micro-électroniques prédéveloppées.

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

Note 3 à l'article: Les HPD sont typiquement basés sur des FPGA ou des technologies micro-électroniques similaires.

[SOURCE: IEC 62566:2012, 3.7]

3.10
fonction d'I&C
fonction permettant de commander, exploiter et/ou surveiller une partie définie du procédé.

[SOURCE: IEC 61513:2011, 3.28]

3.11
système d'I&C
système exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même. Sa technologie est électrique et/ou électronique et/ou électronique programmable

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 actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées

Note 1 à l'article: Voir également «système», « fonction d'I&C».

Note 2 à l'article: Tout réseau fait ou partie d'un système d'I&C ou est un système d'I&C lui même.

[SOURCE: IEC 61513:2011, 3.29]

3.12
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 27000:2009]

3.13
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. Elle se mesure par une combinaison de la probabilité d'un événement et de la gravité de ses conséquences

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

3.14
évaluation du risque
processus général de détermination, d'estimation, d'analyse et d'évaluation systématiques du risque

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

3.15
mesure de sécurité
moyen de gestion de sécurité qui peut être administratif, technique ou managérial

3.16
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 couronnée de succès, 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 ils correspondent à S1, S2 et S3. Les raisons sous-jacentes à l'utilisation de trois degrés de sécurité pour les systèmes programmés-HPD d'I&C sont fournies par l'annexe A. La présente norme traite seulement des systèmes programmés-HPD 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 lorsqu'on aborde de façon globale l'installation.

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 que l'on trouve communément utilisé dans d'autres normes et dans les pratiques industrielles.

3.17
zone de sécurité
concept permettant de regrouper des systèmes informatiques 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]

3.18
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 de la présente norme (voir 1.1), les évènements ou la survenance d'évènement sont limités à ceux qui sont malveillants – ce qui ne couvre pas les aspects accidentels (par exemple les risques naturels, les erreurs humaines), couverts par d'autres normes 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]

3.19
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 Abréviations

Programmé-HPD	Programmé et intégrant potentiellement des HPD (Circuits intégrés programmés en HDL)
EIUI	Equipe d'Intervention en cas d'Urgence Informatique
RSSP	Responsable Sécurité des Systèmes Programmés
DBT	Menace de référence (Design Basis Threat)
HDL	Langage de description de matériel (Hardware Description Language)
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
PDCA	Planifier-Déployer-Contrôler-Agir
PLC	Automate programmable (Programmable Logic Controller)
PSP	Plan de Sécurité du Projet
AQ	Assurance Qualité
V&V	Vérification et Validation

5 Etablissement et gestion d'un programme de sécurité des systèmes programmés-HPD d'I&C

5.1 Généralités

5.1.1 Concepts d'ensemble: programme, politiques et procédures

Un programme de sécurité pour les systèmes programmés-HPD d'I&C (souvent dénommé programme par la suite dans la présente norme) doit définir les étapes et les actions à entreprendre pour définir et appliquer les mesures techniques et organisationnelles de façon cohérente pour atteindre les objectifs sécurité qui sont définis dans la politique de sécurité, explicitement couverts par les plans de sécurité.

Ce programme 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 informatique.

Des programmes de sécurité informatique doivent être mis en œuvre par utilisation des politiques et procédures documentées approuvées par le personnel en charge du programme de sécurité.

Une politique doit décrire les attentes et les exigences relatives à la gestion de la sécurité informatique et doit permettre d'avoir un environnement cohérent et gérable. Cette politique doit être élaborée et prise en compte avec les autres politiques et les procédures développées durant la vie du programme de sécurité des systèmes programmés-HPD d'I&C.

Un programme de sécurité des systèmes programmés-HPD d'I&C d'une centrale nucléaire doit comprendre les activités suivantes:

- définition des responsabilités et de l'organisation liées à la sécurité informatique et du processus de réexamens périodiques;
- développement du processus de désignation des actifs sujets aux mesures de protection de sécurité informatique comprenant les systèmes informatiques, les applications des systèmes informatiques et les connexions réseaux;
- mise en œuvre des méthodes de gestion du personnel pour les aspects liés à la sécurité informatique et à la sécurité des systèmes programmés-HPD d'I&C, ceci comprenant la formation, la qualification des personnes et leur départ ou leur transfert;
- développement et conduite du processus d'évaluation du risque, 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;
- conduite de l'évaluation du risque résiduel qui est transféré/accepté de la conception à l'exploitation;
- 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 nécessaires pour maintenir les fonctionnalités liées de sécurité informatique prévues à la conception;
- 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 de la sécurité informatique et de ses modifications, l'incidence des traitements et des systèmes de secours;
- 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;
- 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 la société productrice d'électricité.

Une politique de sécurité informatique doit définir les objectifs de sécurité informatique de haut niveau applicables pour l'installation nucléaire. Les exigences de la politique de sécurité pour les systèmes programmés-HPD d'I&C doivent être déclinées dans des documents de niveau inférieur, qui sont utilisés pour mettre en œuvre la politique et réaliser les contrôles associés à celle-ci et elle doit pouvoir faire l'objet de mesures, être exécutoire et ses objectifs doivent pouvoir être atteints.

Le plan de sécurité des systèmes programmés-HPD d'I&C doit être la mise en œuvre de cette politique sous la forme de procédures, de responsabilités et de rôles organisationnels. Le plan doit définir et détailler les moyens permettant d'atteindre les objectifs de sécurité. Le plan doit contenir les actions principales à entreprendre et les réponses associées en termes

de détection et de prévention d'intrusion, d'évaluation des conséquences et de contre-mesures nécessaires pour atténuer les conséquences.

5.1.2 Rôles et responsabilités

La gestion du programme de sécurité informatique doit garantir que toutes les questions de sécurité informatique sont prises en compte de façon programmée dans les procédures et les politiques propres au nucléaire pour satisfaire aux exigences réglementaires et à celles de la société industrielle. Elle doit être coordonnée avec les programmes de sécurité de la société et le cadre politique en vigueur pour le site, ses programmes, ses pratiques et ses procédures, lorsque applicables.

La mise en œuvre d'un programme de sécurité pour les systèmes programmés-HPD 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.

Durant les phases de conception et de développement, il est probable que différentes sociétés 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.

Toutes les organisations impliquées à quelque niveau du cycle de vie que ce soit du développement des systèmes programmés-HPD d'I&C doivent documenter les structures organisationnelles, les responsabilités associées à chaque emploi venant en support du 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 sociétés.

Pour développer, approuver et mettre en œuvre un programme pour les systèmes programmés-HPD d'I&C, le personnel de direction de la centrale doit en coopération avec le concepteur d'I&C prendre en compte:

- les exigences de sécurité de la société productrice d'électricité,
- la politique de sécurité interne de la société,
- le cadre juridique national,
- le cadre réglementaire national,
- les meilleures pratiques industrielles en matière de sécurité informatique et de sécurité pour les systèmes programmés-HPD d'I&C,
- l'état des menaces courantes et de celles prévues liées au secteur de l'industrie nucléaire et aux autres secteurs industriels utilisant les équipements d'I&C utilisés dans les centrales nucléaires,
- la mise en place de canaux d'information pour mettre à jour en permanence l'état des menaces courantes et de celles prévues liées au secteur de l'industrie nucléaire et aux autres secteurs industriels utilisant les équipements d'I&C utilisés dans les centrales nucléaires.

Au niveau particulier de la centrale, la société productrice d'électricité doit:

- assumer la responsabilité d'ensemble pour tous les aspects relatifs à la sécurité informatique afin de garantir que l'installation est sûre et sécurisée;
- prendre en compte les exigences réglementaires applicables pour définir les objectifs de sécurité informatique pour la centrale;
- garantir une coordination appropriée avec les programmes de sécurité informatique des systèmes qui ne font pas partie de l'I&C et les régimes de protection physique;
- garantir le respect des lois et règlements;

- mettre en place un processus continu d'évaluation des risques relatifs à la sécurité des systèmes programmés-HPD d'I&C de l'installation;
- définir le niveau d'acceptabilité des risques pour l'installation en conformité avec les exigences réglementaires;
- assigner les responsabilités organisationnelles relatives à la sécurité des systèmes programmés-HPD d'I&C;
- garantir qu'une politique de sécurité des systèmes programmés-HPD d'I&C exécutoire est en place;
- fournir les ressources nécessaires à la mise en place d'un programme de sécurité des systèmes programmés-HPD d'I&C robuste;
- assurer des audits et des mises à jour périodiques des procédures et de la politique de sécurité des systèmes programmés-HPD d'I&C.

La surveillance générale de la sécurité des systèmes programmés-HPD 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. La présente norme fait référence au rôle du Responsable Sécurité des Systèmes Programmés (RSSP), ou équivalent. La responsabilité du RSSP doit couvrir:

- le conseil à l'équipe de direction de la société et ou du projet;
- la coordination et le contrôle du développement des activités de sécurité informatique;
- la coordination de la sécurité informatique avec les autres aspects de la sécurité et de la sûreté;
- la garantie que le programme de sécurité informatique prend en compte l'exploitation et la maintenance de l'installation et ne porte pas atteinte par inadvertance aux systèmes importants pour la sûreté;
- l'identification et la documentation des systèmes qui sont critiques pour le maintien de la sécurité informatique de l'installation;
- la conduite de l'évaluation des risques liés à la sécurité informatique;
- la conduite d'inspections, d'audits et de revues périodiques de sécurité, et la fourniture de rapports d'état à l'équipe de direction;
- le développement et la mise en place d'un processus d'évaluation et de formation à la sécurité informatique;
- le développement d'une stratégie, couvrant les procédures et les aspects formation, pour identifier les incidents relevant potentiellement de la cybersécurité;
- l'élaboration, le pilotage et la contribution aux réponses aux évènements pertinents concernant la sécurité informatique, y compris la coordination avec les organisations internes et externes;
- les investigations à mener suite à la survenance d'incidents ou à l'identification de vulnérabilités et la définition de recommandations concernant les actions correctives.

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

5.1.3 Exigences relatives à la documentation

Le programme de sécurité relatif aux systèmes programmés-HPD d'I&C doit définir les mesures nécessaires pour garantir que les éléments et les activités qui peuvent avoir un impact au niveau sécurité informatique font l'objet d'enregistrements suffisants, développés, revus, approuvés, livrés, utilisés et mis à jour pour refléter le travail accompli, ceci comprenant:

- les enregistrements produits lors de la définition, de la mise en œuvre et de la maintenance du programme;
- les enregistrements des résultats de l'évaluation des menaces qui couvrent des vulnérabilités particulières par rapport à la technologie employée, la configuration des systèmes programmés-HPD d'I&C, et la nature de leur utilisation, les exigences portant sur la maintenance ou les essais;
- les enregistrements portant sur l'ajout, la modification et le retrait d'actifs relatifs à l'I&C programmé couverts par le programme;
- les enregistrements et la documentation technique support, y compris les données d'audits et les enregistrements relatifs à la formation nécessaires pour satisfaire aux exigences nationales réglementaires particulières.

La documentation permet la démonstration que la conception des systèmes programmés-HPD d'I&C et leur mise en œuvre réelle satisfont aux exigences relatives au niveau de sécurité approprié par rapport à la présente norme, et qu'il a été fait part aux utilisateurs des systèmes des instructions et qu'ils ont reçu la formation appropriée sur le fonctionnement et la maintenance des éléments du système relatifs à la sécurité.

5.2 Etablissement du programme

5.2.1 Définition de la politique de sécurité

Les responsables du programme de sécurité (tels que définis en 5.1.2) doivent rédiger un document de haut niveau de politique de sécurité. Cette politique doit:

- inclure un cadre de travail pour définir les objectifs et établir les orientations de haut niveau et les principes d'action par rapport à la sécurité des systèmes programmés-HPD d'I&C;
- prendre en compte les exigences légales et réglementaires, aussi bien que les obligations de sécurité contractuelles;
- garantir que les exigences de sécurité sont appliquées à tous les niveaux de la chaîne d'approvisionnement pour toutes les activités du cycle de vie;
- se mettre en cohérence par rapport au contexte de gestion stratégique des risques pour l'installation nucléaire dans lequel l'établissement et la maintenance du programme de sécurité des systèmes programmés-HPD d'I&C aura lieu;
- établir les critères par rapport auxquels les risques seront évalués (voir 5.2.2) y compris la prise en compte des retours issus de l'exploitation des systèmes programmés-HPD d'I&C; et
- être approuvée par l'équipe de direction.

5.2.2 Définition du domaine d'application et des limites du programme

Le domaine d'application et les limites du programme de sécurité des systèmes programmés-HPD d'I&C doivent être définis en termes de caractéristiques portant sur l'organisation en place pour la centrale nucléaire de puissance, sa situation, les exigences réglementaires nationales, les actifs des systèmes programmés-HPD d'I&C et la technologie employée, et les risques associés au système d'exploitation. Il doit comprendre les détails des justifications relatives aux exclusions/modifications du domaine d'application (voir 1.1).

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

5.2.3.1 Schéma de classement

5.2.3.1.1 Généralités

La sécurité des systèmes programmés-HPD d'I&C doit reposer sur une approche graduée. Tous les systèmes programmés-HPD d'I&C doivent être assignés à un degré de sécurité. Le degré de sécurité d'un système d'I&C doit être attribué sur la base de l'évaluation des

conséquences maximales d'une cyberattaque réussie sur ce système en termes de sûreté et de performances de l'installation (voir 5.2.3.1.3 pour les critères d'assignation détaillés). Des exigences de sécurité graduées sont définies pour chaque degré de sécurité (voir 5.2.3.2.3 à 5.2.3.2.7).

NOTE Dans le contexte de la présente norme, les performances de l'installation sont considérées dans la perspective de la production d'électricité.

Le schéma de classement repose sur les principes suivants:

- les conséquences d'une cyberattaque concernant la sûreté doivent être considérées comme plus importantes que celles portant sur les performances de la centrale;
- 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'assignation d'un degré de sûreté 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 contrôlée ou perturbée de façon malveillante);
- une telle approche d'assignation reposant sur les conséquences doit être rigoureuse et pouvoir être répétée en garantissant la reproductibilité et la consistance de la position de 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).

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

Une approche graduée de la sécurité telle que décrite par la présente norme garantit que:

- le nombre d'interfaces entre systèmes assignés à différents degrés de sécurité doit être justifié;
- des limitations adaptées doivent être mises en œuvre aux interfaces entre systèmes appartenant à des degrés de sécurité différents.

L'évaluation du risque, 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 de mesures de sécurité complémentaires (voir 5.2.3.2.2).

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

L'approche de sécurité graduée décrite dans la présente norme a pour objectif de défendre la sûreté de la centrale et ses performances contre les cybermenaces, sur la base d'une analyse basée sur 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'affection des degrés de sécurité. La sécurité peut tirer profit des mesures de sûreté mises en œuvre conformément à l'IEC 61513 et aux 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 une correspondance stricte pour les systèmes d'I&C, une à un, entre les classes de sûreté et leurs degrés de sécurité.

5.2.3.1.3 Description des degrés de sécurité et des critères d'affectation associés

La présente norme définit trois degrés de sécurité, S1, S2 et S3, auxquels des exigences graduées de sécurité sont associés (tels que définis en 5.2.3.2). 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 5.2.3.1.1) que peuvent avoir des actions malveillantes 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 programmés-HPD d'I&C de la façon suivantes:

   – les systèmes programmés-HPD d'I&C réalisant des fonctions de catégorie A sont de degré de sécurité S1,

   – les systèmes programmés-HPD d'I&C nécessaires pour l'exploitation en temps-réel et les systèmes programmés-HPD d'I&C réalisant des fonctions de catégorie B sont d'un degré de sécurité qui n'est pas inférieur à S2,

   – les systèmes programmés-HPD d'I&C de catégorie C sont assignés suivant le principe des conséquences maximales, et les systèmes programmés-HPD d'I&C d'aide à l'exploitation de la centrale et à la maintenance sont de degré de sécurité S3.

   NOTE 1 Comme indiqué en 5.2.3.1.2, il n'y a pas de relation un pour un entre les catégories de sûreté et les degrés de sécurité. Par exemple, il est recommandé de classer les systèmes programmés-HPD d'I&C nécessaires pour l'exploitation en temps réel 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 l'installation est un critère à prendre en compte pour l'assignation des degrés de sécurité.

e) Un système peut être surclassé dans un degré de sécurité plus strict que celui auquel il a été assigné au titre du point d) si les conséquences d'un acte ou d'un évènement malveillant portant sur n'importe laquelle des fonctions qu'il réalise sont estimées équivalentes à celles correspondantes au degré de sécurité plus strict.

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

NOTE 2 La présente norme 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 lorsqu'on aborde de façon globale l'installation.

NOTE 3 Voir 5.2.3.2.7 pour les outils logiciel.

5.2.3.2 Affectation des exigences techniques

5.2.3.2.1 Généralités

Les exigences de sécurité pertinentes sont données pour tous les systèmes programmés-HPD d'I&C en 5.2.3.2.3. À ces exigences on doit ajouter les exigences de 5.2.3.2.4 pour les systèmes de degré S1, les exigences de 5.2.3.2.5 pour les systèmes de degré S2 et les exigences de 5.2.3.2.6 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.

Les exigences applicables aux outils logiciel, en particulier à ceux de maintenance et de diagnostic utilisés pour les systèmes programmés-HPD d'I&C sont fournies en 5.2.3.2.7.

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

Le programme de sécurité des systèmes programmés-HPD d'I&C d'une centrale nucléaire de puissance doit couvrir l'évaluation des menaces et des vulnérabilités: 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 les évaluations des vulnérabilités, de la mise en œuvre technique et les

analyses des menaces particulières et des scénarios d'attaque, (y compris les menaces de références (DBT) spécifiques au pays, quand ceci est pertinent).

Les activités d'évaluation des vulnérabilités et des menaces peuvent avoir pour conséquence l'identification et la mise en œuvre de contre-mesures complémentaires nécessaires pour empêcher ou limiter les conséquences d'attaques contre les systèmes d'I&C de la centrale. Les dispositions prises pour la sécurité doivent être compatibles avec les performances fonctionnelles prévues à la conception pour la solution.

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

- définition du contexte et des limites;
- identification et caractérisation des menaces;
- évaluation des vulnérabilités;
- élaboration de scénarios d'attaque;
- probabilité de poursuivre l'exploitation avec succès;
- 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.

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 pourraient porter atteinte aux systèmes programmés-HPD d'I&C installés. Le nombre de menaces potentielles et de vulnérabilités augmente habituellement lorsqu'on évolue de systèmes indépendants et isolés vers des systèmes interconnectés.

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 aux seuls risques identifiés. Il convient que la gestion des vulnérabilités associées aux systèmes programmés-HPD d'I&C se fasse au travers des études des publications faites par les EIUI (Equipe d'Intervention en cas d'Urgence Informatique), des contacts avec la communauté de la sécurité informatique, avec une attention particulières portée aux faiblesses des produits et des solutions d'I&C.

NOTE Les degrés de sécurité sont affectés aux systèmes ou aux sous-systèmes programmés-HPD d'I&C dès le départ du projet. Ils reposent sur les conséquences potentielles, telles que définies en 5.2.3.1.1, d'une attaque des systèmes d'I&C liée à la sécurité ou d'une des fonctions qu'ils réalisent. Les degrés de sécurité, au travers des exigences associées, aident à spécifier les systèmes.

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

5.2.3.2.3 Exigences génériques

Les exigences suivantes sont applicables à tous les systèmes programmés-HPD d'I&C, indépendamment du degré de sécurité auquel ils sont affectés.

a) Les mesures de conception doivent être définies afin d'établir un niveau de confiance approprié dans le fait que les traitements d'un système affecté à un degré de sécurité donné ne sont pas dégradés par des systèmes affectés à des degrés moins stricts.

b) Il convient que tout système soit configuré et paramétré de façon à minimiser les vulnérabilités du système.

c) Il convient que tout composant prédéveloppé soit choisi, configuré et paramétré de façon à minimiser les vulnérabilités du système.

d) L'analyse de sécurité d'un système doit être prise en compte dans le plan de sécurité du système. Si l'analyse montre que les mesures prévues ne sont pas suffisantes alors l'analyse de sécurité doit identifier les exigences 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 formelle ou informelle entre la politique de sécurité d'ensemble et son adaptation pour les systèmes ou les groupes de systèmes d'I&C;

f) Il convient d'intégrer dans la conception, la configuration et/ou l'affection 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 d'authentification efficaces avant qu'un accès soit autorisé.

i) 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, doivent limiter au minimum nécessaire les accès, aussi bien en termes de personnel autorisé que d'opérations autorisées.

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

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

l) Il convient que les journaux d'enregistrement soient vérifiés de façon périodique d'un point de vue de la sécurité pour les systèmes programmés-HPD d'I&C classés de sûreté et pour les systèmes de surveillance des systèmes programmés-HPD 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 corrélée 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 minimiser les vulnérabilités.

o) Il convient que les mesures relatives à la détection des anomalies soient mises en œuvre, que les alarmes soient analysées avec des mesures en réponse appropriées prises. 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 mesures 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 considérés.

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

r) Toutes les dispositions temporaires, par exemple les «accès root», les branchements supplémentaires d'appareil pour les essais 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, approuvée par le propriétaire et documentée.

t) Des dispositions doivent être en place pour permettre une restauration rapide d'un niveau de service acceptable dans le cas d'une cyberattaque couronnée de succès. Des mesures doivent être mises en place pour limiter la possibilité que ces dispositions soient elles même vulnérables aux mêmes cybermenaces.

5.2.3.2.4 Exigences supplémentaires pour le degré S1

La liste de l'ensemble minimal des exigences de sécurité pour les systèmes programmés-HPD d'I&C classés de degré S1 (en plus des exigences génériques) est fournie ci-dessous. Les mesures nécessaires 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 du système.

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

b) Il convient que les communications soient orientées des systèmes programmés-HPD d'I&C de degré S1 vers les systèmes programmés-HPD 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 seules les transmissions inévitables (par exemple les ordres prioritaires des systèmes de commande actionneurs, les permissifs, les réinitialisations) et doivent 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 d'inter-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 mesures 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 avec les paragraphes 5.7 (Sécurité du logiciel) et 12.2 (Sécurité informatique sur site) de l'IEC 60880:2006 et l'IEC 62566 doit être exigée pour les systèmes de degré S1.

g) L'accès physique aux systèmes de degré S1 doit être surveillé par alarme en salle de commande ou dans un autre endroit approprié.

5.2.3.2.5 Exigences supplémentaires pour le degré S2

La liste de l'ensemble minimal des exigences de sécurité pour les systèmes programmés-HPS classés de degré S2 (en plus des exigences génériques) est fournie ci-dessous. Les mesures nécessaires 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 soient orientées 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 mesures de sécurité appropriées (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 logiciel et de configuration de systèmes de degré S2 ne doivent pas être possibles à partir de système de degré S3.

d) Les modifications logiciel 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 inter-verrouillages appropriés. Il convient de réaliser le transfert bidirectionnel de données entre des équipements 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 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) et empêcher toute création non autorisée d'un nouvel accès à ces zones.

5.2.3.2.6 Exigences supplémentaires pour le degré S3

La liste de l'ensemble minimal des exigences de sécurité pour les systèmes programmés-HPD d'I&C classés de degré S3 (en plus des exigences génériques) 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 pourraient 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 programmés-HPD 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 dument justifiées et les branchements doivent être surveillés.

5.2.3.2.7 Exigences de sécurité pour les outils logiciel, y compris de maintenance et de diagnostic

Les outils logiciel, en particulier ceux utilisés à des fins de maintenance système et de diagnostic 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.

Un degré de sécurité inférieur peut être assigné dans le cas d'une connexion indirecte mettant en jeu des contrôles humains et/ou procéduraux. Dans le cas où les outils 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 place.

Il convient d'adapter comme suit les exigences de sécurité associées pour les outils logiciel:

- 5.2.3.2.3 (Exigences génériques) est applicable pour tous les outils logiciel.
- Pour le degré S1, 5.2.3.2.4 est applicable à l'exception du point g) (traitant des alarmes) qui n'est pas pertinent pour les outils, et à l'exception du point e) (traitant des fonctions

cachées) qui est remplacé par le suivant: il convient que des mesures soient mises en place contre les fonctions cachées dans le logiciel système de l'outil.

- Pour le degré S2, 5.2.3.2.5 est applicable à l'exception des point c), d et f) qui ne sont pas pertinents pour les outils. 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 l'installation ou à partir de système ne faisant pas partie de l'I&C.
- Pour le degré S3, 5.2.3.2.6 est applicable

NOTE Ces adaptations ont pour but de prendre en compte la différence technologique potentiellement importante entre les systèmes programmés-HPD d'I&C et les outils logiciel, en particulier pour les systèmes de sûreté.

5.2.3.3 Zones de sécurité

Une possible mise en œuvre pratique de l'approche graduée correspond à un regroupement des systèmes programmés-HPD d'I&C dans des zones logiques, pour lesquelles des principes de protection graduée sont appliqués pour chaque zone de sécurité (voir 3.17). Ces zones permettent de regrouper des systèmes d'I&C d'importance similaire pour la sûreté et les performances de l'installation (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 1 Dans le reste de la présente norme, le terme «zone» désignera une «zone de sécurité» telle que définie en 3.17 et dans ce paragraphe. Ce terme ne fait pas référence aux zones de sûreté et aux séparations géographiques associées (bien que certaines relations existent).

Il convient que l'application du modèle des zones soit conforme aux recommandations suivantes:

- 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 programmés-HPD d'I&C est assigné à un degré de sécurité moins strict (voir 5.2.3.1.3) que les autre 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 2 Les degrés de sécurité sont formellement associés aux systèmes programmés-HPD 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.
- 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.
- 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 de la présente norme. Si les zones ont des degrés de sécurité différents, alors les exigences de sécurité associées aux degrés de sécurité s'appliquent (voir 5.2.3.2.3 à 5.2.3.2.6). 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 de sécurité dédiées.
- L'initialisation des communications ne doit être faite que d'une zone de degré 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).
- Les frontières de zones nécessitent la mise en œuvre de mécanismes de découplage pour que le flux de données puisse être structuré en fonction de la politique de zonage.

Il n'existe par de relation une-pour-un entre les zones de sécurité et les degrés de sécurité; un degré de sécurité peut être assigné à plusieurs zones lorsque ces multiples zones ont besoin du même degré de sécurité. Les zones correspondent à des regroupements logiques et/ou physiques de systèmes informatiques, alors que les degrés de sécurité représentent les degrés de protection exigés.

5.2.4 Approbation hiérarchique

Une revue du programme de sécurité de l'ensemble des systèmes programmés-HPD d'I&C doit être régulièrement réalisée par la direction. Le résultat de la revue et de l'approbation hiérarchique doit comprendre toutes décisions et actions relatives aux points suivants:

- mise en œuvre et modifications des procédures et des mesures qui ont un effet sur le programme de sécurité des systèmes programmés-HPD d'I&C, telles que nécessaires, pour répondre aux évènements 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,
- critères originaux et amélioration des mesures mises en place concernant l'efficacité des contrôles,
- processus de décision et critères de déclanchement d'action ayant un impact sur l'exploitation de l'installation (par exemple poursuite de l'exploitation de la centrale, arrêt de la centrale, isolement des communications, maintenance des matériels).

Les décisions et les actions reposant sur cette revue hiérarchique doivent être prises à l'aide d'un processus décisionnel 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.

5.3 Mise en œuvre et fonctionnement du programme

5.3.1 Exigences génériques de mise en place

L'organisation doit:

- développer un programme de sécurité pour les systèmes programmés-HPD d'I&C qui satisfasse aux exigences génériques de sécurité de la présente norme;
- développer un plan de mise en place qui identifie les actions hiérarchiques, les ressources nécessaires et les priorités pour gérer les risques relatifs aux systèmes programmés-HPD d'I&C;
- mettre en place le programme de sécurité pour les systèmes programmés-HPD d'I&C en utilisant des mesures identifiées de nature technique, managériales et opérationnelles et/ou des actions de limitation des conséquences pour gérer les risques de façon appropriée;
- déployer de façon continue des efforts au niveau maintenance, mise à jour et réponse aux incidents liés à la sécurité pour garantir une protection continue des systèmes programmés-HPD d'I&C contre les cyberattaques;
- mettre en œuvre tous les plans en prenant en compte les questions de financement, d'allocation des rôles et des responsabilités et du soutien hiérarchique.

5.3.2 Définition d'un mesurage de l'efficacité

Le succès de la mise en place et de la réalisation d'un programme de sécurité pour l'I&C exige qu'un système de mesurage soit mis en place pour mesurer[1] l'efficacité des contrôles ou des groupes de mesures de sécurité utilisés. Ces métriques doivent permettre à l'organisation d'évaluer comment les contrôles atteignent les objectifs fixés.

Durant la phase de développement du programme de sécurité pour les systèmes programmés-HPD d'I&C il convient que l'organisation:

- définisse des métriques d'efficacité pour chaque mesure individuelle utilisée dans le programme;
- définisse des métriques d'efficacité pour les groupes de mesures qui sont considérés comme une entité distincte et prise comme telle dans le plan de sécurité;
- détermine les variantes particulières de mise en œuvre des mesures et des groupes de mesures qui nécessitent d'introduire des variantes au niveau des métriques de mesurage;
- définisse des métriques pour quantifier l'efficacité des actions de limitations des conséquences qui justifient une absence de mesures de sécurité;
- prépare un ensemble consolidé d'informations détaillées portant sur les métriques identifiées relatives au mesure particulière pour appuyer efficacement et de façon normalisée l'effort de surveillance de l'efficacité des mesures.

5.3.3 Formation et sensibilisation

La formation du personnel, y compris les sous contractants, dans l'organisation est nécessaire pour pouvoir garantir la sécurité d'un cyber environnement pour les systèmes programmés-HPD d'I&C. Celles-ci limitent la probabilité d'avoir des brèches au niveau sécurité et de l'apparition de problèmes internes liés à la sécurité. En conséquence:

- On doit développer et mettre en place un programme de formation formalisé pour le personnel concevant et exploitant les systèmes d'I&C.
- 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.
- Les organisations et les individus qui ont de l'expérience au niveau des systèmes programmés-HPD d'I&C doivent être dans l'absolu impliqués dans la sensibilisation et la formation, dans le contexte des centrales nucléaires de puissance.

5.4 Surveillance et réexamen du programme

Un des principaux facteurs contribuant au maintien de l'efficacité du programme de sécurité des systèmes programmés-HPD 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. En conséquence de quoi, l'organisation doit:

- établir un réexamen de programme 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 de l'I&C pour en garantir l'efficacité;

---

1 (Note de traduction) Le terme "mesure" (de sécurité), dans ce paragraphe comme dans tout le document, correspond au terme *(security) control* en anglais, au sens disposition de sécurité, et non au sens d'un suivi métrologique. Pour ce dernier sens, les termes « métriques » ou « mesurage » ont été ici préférés.

- établir 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.

5.5 Mise à jour et amélioration du programme

Le programme de sécurité des systèmes programmés-HPD d'I&C doit définir le processus pour:

- mettre en œuvre les améliorations concernant le programme identifiées durant les revues de programme internes ou externes y compris les actions prédictives ou correctives;
- 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;
- développer et mettre en œuvre un programme de réexamen pour évaluer périodiquement et mettre à jour l'évaluation des menaces pour la sécurité;
- définir les métriques pour évaluer si les améliorations ont atteint leurs objectifs.

6 Mise en œuvre du cycle de vie pour la sécurité des systèmes programmés-HPD 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 programmés-HPD d'I&C. Le cycle de vie pour la sécurité des systèmes programmés-HPD d'I&C est développé pour couvrir les systèmes programmés-HPD d'I&C et leurs composants de leur conception à leur retrait d'exploitation en passant par leur vie en service.

6.2 Activités relatives aux exigences

On doit adopter une approche descendante, en prenant en compte l'architecture d'ensemble de l'I&C et les équipements et composants individuels. Les spécifications doivent être écrites pour couvrir l'architecture d'ensemble de l'I&C d'un point de vue fonctionnel, avant de traiter des sous-structures fonctionnelles et de leurs interfaces.

NOTE Lorsqu'on écrit des spécifications, les systèmes nécessaires pour réaliser une fonctionnalité donnée ne sont pas connus, ainsi il n'est pas possible de réaliser les analyses d'évaluation des risques, en particulier l'évaluation des vulnérabilités n'est pas possible à ce stade.

Les composants et systèmes individuels peuvent être fournis et sécurisés par différents fournisseurs, pourvu que la sécurité au niveau de l'ensemble de la structure soit maintenue de façon consistante. Un degré de sécurité, tel que défini en 5.2.3.1, ainsi que les exigences de sécurité associées doivent être assignés à chaque système. Ces systèmes peuvent être assignés à des zones de sécurité satisfaisant à des exigences de sécurité supplémentaires.

6.3 Activités de planification

6.3.1 Identification des systèmes programmés-HPD d'I&C

Chaque système programmé-HPD d'I&C prévu à la conception de la centrale ou de l'installation doit être identifié. A ce niveau du processus, ceci ne correspond qu'à une liste de systèmes programmés-HPD d'I&C faisant partie de la conception de la centrale, sans faire apparaître de détails de conception, avec des choix de composants non confirmés.

6.3.2 Assignation des degrés de sécurité

Chaque système programmé-HPD 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 programmés-HPD d'I&C telle que décrite en 5.2.3.

6.4 Activités de conception

6.4.1 Généralités

Ce paragraphe 6.4 décrit les éléments de configuration de la conception particulière du système programmé-HPD d'I&C conçu conformément aux exigences définies ci-dessus en 6.2.

La phase de conception doit prendre en compte les objectifs de conception de la centrale ou de l'installation 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 de la présente norme) pour traiter des mesures de sécurité pour (a) les accès physiques et logiques aux fonctions 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. Il convient que le concepteur garantisse que la conception du code logiciel est conforme aux normes de conception pertinentes en la matière, pour traiter de la question des vulnérabilités potentielles qui pourraient avoir été introduites au niveau du processus de conception. Il convient de porter une attention particulière à la gestion de configuration. Les exigences doivent être traduites en critères de conception particuliers. L'accès à toute unité logiciel placée sous contrôle de configuration doit être sujet à des mesures 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.

Le concepteur doit faire l'inventaire complet de tous les systèmes d'I&C et de leurs interfaces en considérant tous les appareils utilisés dans la centrale, y compris les appareils d'essai, de maintenance et de diagnostic.

6.4.2 Evaluation des risques au niveau de la phase de conception

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 mise en œuvre technique et l'analyse des menaces et des scénarios d'attaques particuliers, (y compris les menaces de référence particulières au pays, le cas échéant). Les évaluations des risques peuvent conduire à améliorer les mesures de sécurité de façon à réduire les vulnérabilités.

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

6.4.3 Plan de sécurité de la conception du projet

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. Un plan de sécurité projet, couvrant l'exploitant mais aussi les tierces parties et les entités externes impliquées dans le projet doit être établi. En particulier le concepteur doit montrer que:

- il a en place une politique de sécurité;
- une telle politique s'applique pour chacun de ses sites de développement;
- elle est complétée au niveau des aspects locaux;
- elle garantit que ses propres tierces parties sont à un niveau de sécurité satisfaisant.

6.4.4 Chemins de communication

Les chemins de communications doivent faire l'objet d'évaluation au niveau de la conception planifiée du système et de ses composants. Faisant partie de ce processus, il convient de définir les limites du système et d'en établir une cartographie.

Les contrôles de cybersécurité doivent être établis pour:

- rendre exécutoire et documenter les autorisations données pour contrôler le flux d'informations dans et entre les systèmes interconnectés conformément aux degrés de sécurité assignés (voir 5.2.3.3);

  NOTE C'est le cas pours les systèmes assignés à différentes degrés de sécurité ou à différentes zones de sécurité.

- 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 programmés-HPD d'I&C, en cohérence avec l'évaluation des risques et l'approche graduée décrite en 5.2.2.

6.4.5 Définition des zones de sécurité

Il convient de définir les zones de sécurité durant la phase de conception (voir 3.17 et 5.2.3.3). Elles peuvent aussi être définies durant la phase de mise en œuvre (voir 6.5). L'assignation des systèmes programmés-HPD d'I&C aux zones de sécurité doit prendre en compte, comme indiqué en 5.2.3.1.2, le degré de sécurité précédemment assigné durant la phase de planification à chaque système programmé-HPD d'I&C.

6.4.6 Evaluation de la sécurité de la conception finale

Des évaluations de la sécurité doivent garantir une couverture complète de l'architecture d'I&C à l'étape finale de la conception.

6.5 Activités de mise en œuvre

Ce paragraphe s'intéresse à la mise en œuvre de la conception sécurisée pour la production de logiciel et de matériel sécurisés. Dans la phase de mise en œuvre, le logiciel et le matériel doivent être intégrés en fonction de la conception système en prenant en compte toutes les exigences de sécurité définies.

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.

6.6 Activités de validation

La Vérification et Validation (V&V) traditionnelle conforme aux normes doit être faite en fonction des exigences de sécurité spécifiées pour les systèmes programmés-HPD d'I&C. De plus, les essais doivent permettre de vérifier les aspects sécurité au niveau conception de l'I&C pour l'architecture matérielle, les dispositifs de communication externes et les configurations pour ce qui est des chemins de communication non autorisés et de l'intégrité système. 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. 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 faille de sécurité et ne réduit pas la fiabilité des fonctions de sûreté.

6.7 Phase d'installation et des essais de recette

L'installation et les essais de recette concernant les exigences de sécurité spécifiées doivent être conformes à la politique et aux procédures propres à la centrale, aussi bien qu'au programme de sécurité des systèmes programmés-HPD d'I&C, lorsque applicables. A la fin de l'installation le système doit être testé dans son environnement d'exploitation pour vérifier et valider que les caractéristiques de sécurité du système d'I&C sont correctes et qu'elles ont été incorporées dans le système conformément à ce qui était prévu à la conception.

6.8 Activités d'exploitation et de maintenance

6.8.1 Contrôle des modifications durant l'exploitation et la maintenance

Durant la phase d'exploitation et de maintenance, on doit réaliser des audits de sécurité périodiques des caractéristiques de sécurité. Avant chaque modification système ou maintenance, les composants qui sont affectés doivent être évalués pour confirmer que toutes les caractéristiques et les éléments de conception liés à la protection resteront fonctionnels. Après que de telles modifications ou que des activités de maintenance aient été réalisées, toute caractéristique ou toute mesure de protection sécuritaire doit être restaurée et les fonctionnalités de sécurité doivent être vérifiées. Les exigences de sécurité pour les outils logiciel sont traitées en 5.2.3.2.7.

6.8.2 Réévaluations périodiques des risques et des mesures de sécurité

L'efficacité des mesures de sécurité mis en œuvre dans les systèmes doit être réévaluée de façon périodique. Des tests des mesures de sécurité doivent être réalisés si nécessaire pour vérifier l'efficacité des contrôles suite à la survenance d'évènement particulier.

L'évaluation des risques doit être mise à jour périodiquement. Les risques qui surviennent ou qui deviennent apparents durant l'exploitation doivent être gérés avec diligence et en conformité avec les procédures définies et les exigences réglementaires.

6.9 Gestion des modifications

Les processus de gestion des modifications doivent suivre le plan procédural de la centrale, les engagements relatifs aux autorisations d'exploitation ou réglementaires, tels qu'applicables, pour maintenir en même temps la conformité aux référentiels et le contrôle de configuration. L'évaluation des risques doit être réalisée avant que toute modification soit faite qui pourrait affecter une caractéristique de sécurité. Il convient que le processus d'approbation soit adapté à la modification considérée.

Au minimum, l'impact sur la sécurité doit être considéré du point de vue de l'évaluation des risques et doit être documenté avant toute modification. Des justifications doivent être fournies pour démontrer que des mesures appropriées sont déjà en place ou seront mises en œuvre pour prendre en compte tous nouveaux risques identifiés de façon appropriée.

Les modifications non autorisées ou non documentées de la configuration ou des caractéristiques du réseau par le personnel de la centrale ou par une tierce partie peuvent mettre en péril l'intégrité du modèle de sécurité défensive de l'I&C. Aussi, on doit assurer un contrôle des pratiques de conception et de maintenance pour empêcher les violations de ce type.

6.10 Activités liées au retrait d'exploitation

La phase de retrait d'exploitation du système d'I&C doit être principalement de la responsabilité de l'équipe de direction de la centrale.

Un programme efficace continu doit couvrir la phase de retrait d'exploitation du cycle de vie. Une ou des procédures doivent être mises en place pour assurer un retrait correct des appareils programmés d'I&C et une mise au rebut sous contrôle des moyens support et du logiciel embarqué, pour éviter toute diffusion d'informations sensibles. De plus il convient de couvrir les aspects sécurité liés à la préparation du système pour son retrait, tels que le fonctionnement en parallèle du nouveau et l'ancien système, si nécessaire.