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 It also gives information on projects, replaced and withdrawn publications.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

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

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.

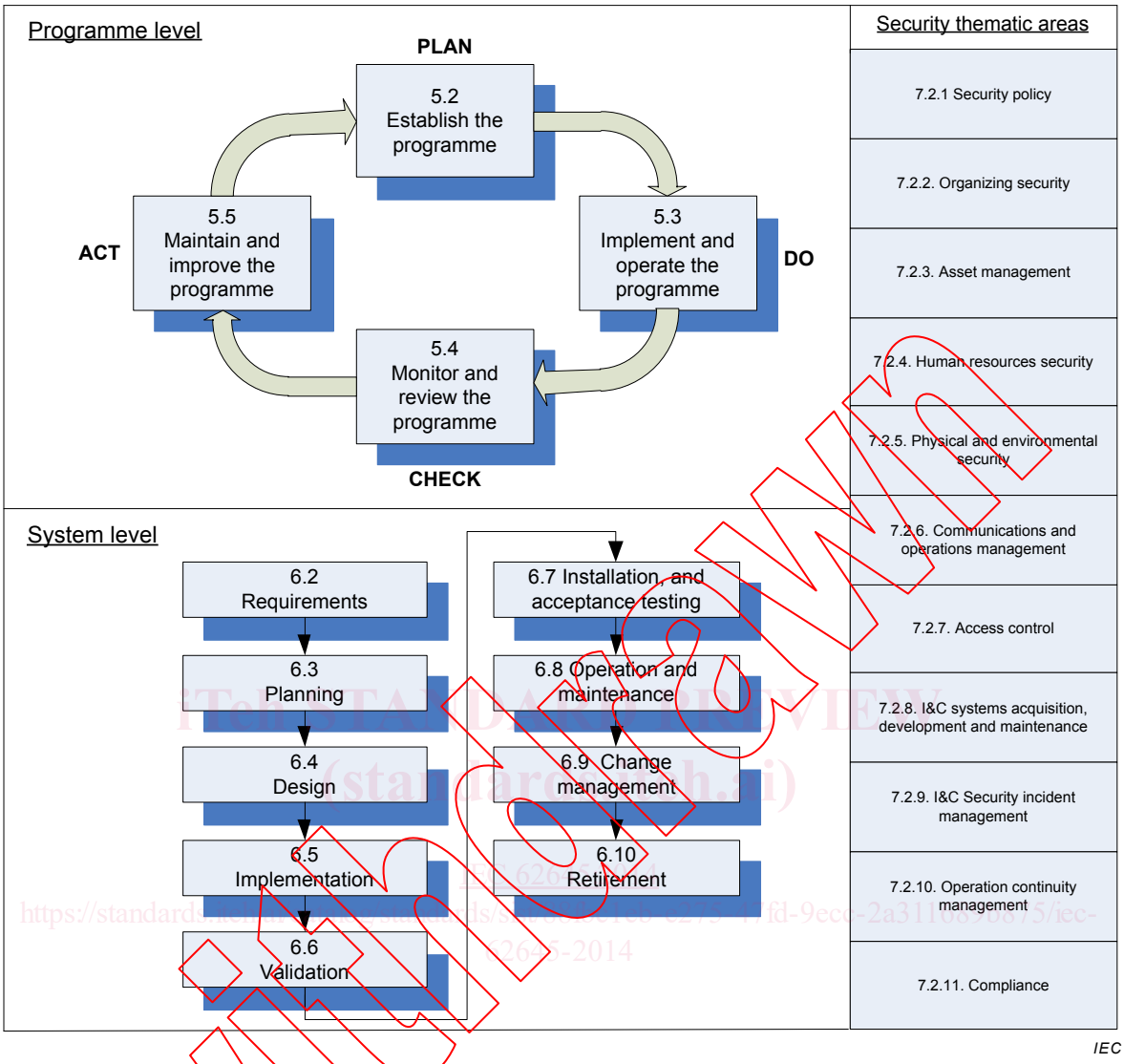

Figure 1 – Overall framework of IEC 62645

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]