

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2019 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 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.

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.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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 une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-7548-1

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

CONTENTS

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

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

F.1.2	Categorization of RRs in accordance with potential hazards	47
F.1.3	Safety categories as input to security degree assignment	48
F.1.4	Impact on operational capacity as input to security degree	49
F.1.5	Considerations on requirements associated to security degrees	49
F.2	Applicability of IEC 62645 security graded approach to fuel cycle facilities	49
F.3	Applicability of IEC 62645 security graded approach to SMR	49
F.4	Reference documents	50
Annex G (informative) High-level correspondence table between IEC 62443 series and IEC 62645.....		51
Bibliography.....		53
Figure 1 – Overall framework of IEC 62645.....		11
Figure 2 – E/E/PE items.....		14
Figure D.1 – Overview of IEC SC 45A standards with cybersecurity relation		44
Figure E.1 – Selection of security controls		46
Table C.1 – Correspondence between ISO/IEC 27001:2013 and IEC 62645		41
Table F.1 – Correspondence between safety categories and classes as per IEC 61513.....		48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

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

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

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

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

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

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

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

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

c) Recommendations and limitations regarding the application of this standard

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Scope

1.1 General

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2 Application

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

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

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

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

1.3 Framework

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

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

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

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

- the term "information security" used in the referenced ISO/IEC 27001:2013 content correspond to "cybersecurity" in this document (as defined in Clause 3);
- the terms "information security policy" used in the referenced ISO/IEC 27001:2013 content correspond to "I&C digital programmable system policy" in this document.

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

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

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

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

Figure 1 presents the overall framework of this document.

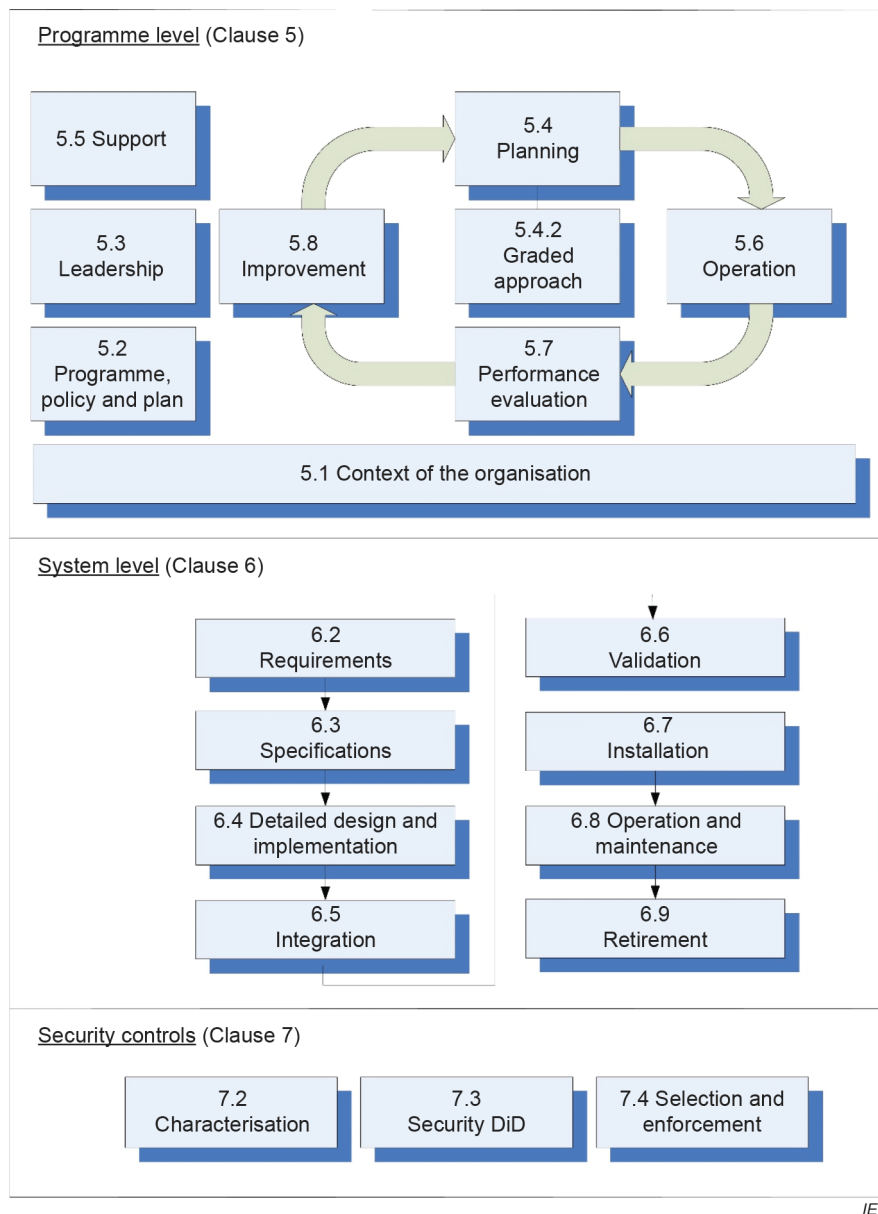


Figure 1 – Overall framework of IEC 62645

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

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

3.1

attack vector

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

3.2

authorization

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

3.3

availability

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

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

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

3.4

computer-based item

item that relies on software instructions running on microprocessors or microcontrollers

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

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

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

[SOURCE: IEC 62138: 2018, 3.8]

3.5

confidentiality

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

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

3.6

cyberattack

malicious acts by digital means

3.7

cybersecurity

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

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

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

Note 1 to entry: This definition is tailored with respect to the IEC 62645 standard scope and overall SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the SC 45A standard series. See Annex A for more detail about such exclusions.

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

3.8 design

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

[SOURCE: IAEA Safety glossary, 2007 edition]

3.9 Design Basis Threat DBT

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

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

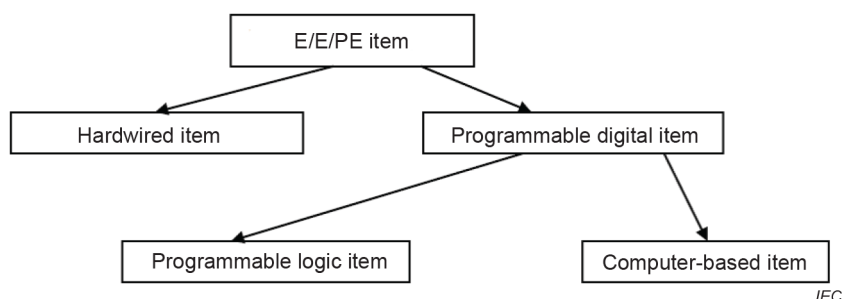
[SOURCE: IAEA INFCIRC/225/Rev.4:1999, modified: note 1 added]

3.10 Electrical/Electronic/Programmable Electronic item E/E/PE item

item based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

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

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



IEC

Figure 2 – E/E/PE items

[SOURCE: IEC 62138: 2018, 3.15]

3.11**HDL-Programmed Device****HPD**

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

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

Note 2 to entry: The development of HPDs can use Pre-Developed Blocks.

Note 3 to entry: HPDs are typically based on blank FPGAs (Field Programmable gate Arrays) or similar micro-electronic technologies.

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

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

[SOURCE: IEC 62566: 2012, 3.7]

3.12**I&C function**

function to control, operate and/or monitor a defined part of the process

[SOURCE: IEC 61513:2011, 3.28]

3.13**I&C system**

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

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

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

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

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

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

[SOURCE: IEC 62138: 2018, 3.26]

3.14**integrity**

the property of protecting the accuracy and completeness of assets

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

3.15**programmable digital item**

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

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

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

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

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

[SOURCE: IEC 62138:2018, 3.35]

3.16

risk

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

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

3.17

risk assessment

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

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

3.18

security controls

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

3.19

security degree

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

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

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

3.20

security programme

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

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

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

3.21

security zone

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

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

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

**3.22
threat**

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

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

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

**3.23
vulnerability**

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

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

4 Abbreviated terms

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

5 Establishing and managing a nuclear I&C programmable digital system security programme**5.1 Context of the organization****5.1.1 Understanding the organization and its context**

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

5.1.2 Understanding the needs and expectations of interested parties

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

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

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

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

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

5.2 Programme, policy and plan

5.2.1 I&C digital programmable system security program

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

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

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

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

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

- a) definition of the computer security organization and responsibilities and the process of periodic reviews;
- b) development of the process of designating assets subject to computer security protective measures including computer systems, computer system applications and network connections;
- c) implementation of methods of personnel management in computer security and I&C programmable digital system security including training, qualification and termination/transfer;
- d) development and performance of the process for risk assessment, taking into account the country specific design basis threat (DBT) as applicable, for the complete I&C architecture as well as for every I&C system;
- e) performance of an assessment of the residual risk that is transferred/accepted from design to operation;
- f) definition of the fundamental architecture and design principles and requirements for system security design and configuration management for plant systems and vendor support required to maintain the cybersecurity features incorporated in the design;
- g) identification of operational security procedures for access control, data security, communication security, platform and application security, system monitoring, computer system security maintenance and modification and security incident handling;
- h) in particular, definition of a process for assessment of off-the-shelf components, both hardware and software to ensure as far as reasonably possible that they are free from malicious software or functionality;
- i) establishment of security requirements for the preparation and formalization of deliveries of hardware, data, software, code or information between different sites of the designers, or between a designer and a third party, or between the designer and the utility.

5.2.2 Policy

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

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

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

5.2.2.4 These requirements shall be:

- a) measurable,
- b) enforceable,
- c) and achievable.

5.2.3 Plan

The I&C programmable digital system security plan shall:

- a) be the implementation of that policy in the form of organizational roles, responsibilities and procedures,
- b) specify and detail the means for achieving the security goals,
- c) contain the primary actions to be taken and the associated response in terms of intrusion detection and prevention, assessment of consequences, and the countermeasures necessary to mitigate consequences.

5.3 Leadership

5.3.1 Leadership and commitment

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

5.3.2 Roles, responsibilities and authorities

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

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

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

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

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

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

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

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

- a) utility corporate security requirements;

- b) internal corporate security policy;
- c) national legislative material;
- d) national regulatory material;
- e) computer and I&C programmable digital system security industry best practices;
- f) current and projected threat status in the nuclear industry and in other industries using I&C equipment used in nuclear plants;
- g) to establish information channels concerning continuous update on current and projected threat status in the nuclear industry and in other industries using I&C equipment used in nuclear plants.

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

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

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

5.4 Planning of the programme

5.4.1 Cybersecurity objectives and planning to achieve them

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

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

5.4.2 Addressing risks and opportunities of the programme

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

5.4.3 Graded approach to I&C security and risk assessment

5.4.3.1 Classification scheme

5.4.3.1.1 General

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

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

5.4.3.1.1.2 The classification scheme is based on the following principles:

- a) consequences of cyberattack regarding safety shall be assumed as more serious than those regarding plant performance;
- b) systems shall be considered from a functional point of view and assigned to a given security degree according to their possible direct or indirect impact on plant safety and performance. The security degree of a system is assigned based on the most sensitive function (i.e. the one which leads to the most severe impacts when maliciously manipulated or disrupted) it implements;
- c) such a consequence-based assignment approach shall be rigorous and repeatable, ensuring reproducibility and consistency of the security posture. This analysis shall include the possibility that other I&C systems are subject to the same attack (e.g. similar systems in separate redundancies).

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

5.4.3.1.1.4 Security degree assignment shall be documented.

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

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

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

5.4.3.1.2 Link between safety categories, safety classes and security degrees

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

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

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

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

5.4.3.1.3 Description of the security degrees and associated assignment criteria

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

- a) The functions and systems shall be analysed to determine the maximum consequences on the plant safety and performance (as defined in 5.4.3.1.1) of malicious actions or events involving them.
- b) This analysis shall be documented.
- c) The systems shall be assigned to degrees S1 (the most stringent) to S3 according to these maximum consequences,
- d) Security degrees should be assigned to I&C programmable digital systems as follows:
 - I&C programmable digital systems processing safety category A functions to security degree S1,
 - I&C programmable digital systems processing safety category B functions, and I&C programmable digital systems with direct and immediate impact on plant safety or on the main nuclear process operation, to no lower than security degree S2,
 - I&C programmable digital systems supporting Category C functions to S1, S2 or S3 according to the maximum consequences,
 - and I&C programmable digital systems assisting plant operation and maintenance to security degree S3.

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

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

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

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

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

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

5.4.3.2 Assignment of technical requirements

5.4.3.2.1 General

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

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

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

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

5.4.3.2.2 Link with security risk assessment activity and Design Basis Threats

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

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

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

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

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

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

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

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

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

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

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

5.4.3.2.3 Confidentiality

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

- confidentiality of data exchanged, treated and/or stored by I&C digital programmable systems (measures, commands, set points, etc.), and
- confidentiality of information about I&C digital programmable systems (e.g., detailed design and specifications, status, versions, network maps, etc.).

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

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

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

5.4.3.2.4 Baseline requirements

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

- a) Design measures shall be defined to provide adequate confidence that the treatments of a system assigned to a given security degree are not degraded by systems assigned to a less stringent security degree.
- b) Any I&C system should be configured and parameterized so as to minimize the vulnerability of the system.
- c) Any pre-developed component should be selected, configured and parameterized so as to minimize the vulnerability of the system.
- d) The system security analysis, including risk assessment, shall be taken into account in the system security plan. If the analysis shows that the planned measures are not sufficient then the security analysis shall identify the need for additional countermeasures.

- e) The security policy shall be adapted to each I&C system or group of systems. A correspondence should be established between the overall security policy and its adaptation to the I&C systems or groups of systems. This can be done more or less formally.
- f) Effective protection measures should be included in the design, configuration and/or parameter assignment of programmable equipment concerning:
 - user selective access control to the software functions and memory spaces,
 - data connections to systems with less stringent security degree,
 - traceability of software or parameter modifications.
- g) During verification and validation of the system, the effectiveness of the security functions shall be demonstrated through suitable tests with the system in its final configuration.
- h) I&C systems should support technical measures to provide an effective authentication procedure before access is permitted.
- i) Human-machine-interfaces either to operate the plant or off-line dedicated functions, or used for I&C system maintenance, should restrict access to the minimally necessary extent, both in terms of authorized staff and authorized operations. When the minimally necessary extent cannot be reached, compensating security controls should be implemented.
- j) A security assessment of the on-site configuration and parameter assignment should take place to verify that suitable countermeasures have been implemented against potential security threats.
- k) Software modification activities shall be systematically planned for and performed and consider potential security threats.
- l) Logs should be checked periodically from a security perspective for safety-classified I&C programmable digital systems and systems monitoring safety-classified I&C programmable digital systems.
- m) Logs should be checked periodically for systems ensuring cybersecurity functions (e.g., filtering and/or segmentation equipment). These logs should be centrally managed and correlated where possible as long as it does not compromise security (e.g., network segmentation) or safety separations (e.g., for independence purposes).
- n) The number of access points to networks shall be minimalized to the extent possible to minimize vulnerability.
- o) Provisions for anomaly detection should be implemented and alarms should be analyzed with appropriate response measures taken. Implementation shall be compatible with safety requirements.
- p) Physical access to I&C systems shall be strictly controlled to prevent access from unauthorized persons. This shall be enforced by physical security measures (e.g., locked cabinet, physical access control to the room or area) and covered by appropriate organizational and administrative measures. These measures shall be commensurate with the security degree of the systems considered.
- q) Physical and logical access of contractors to I&C systems shall be restricted according to their mission, both in terms of duration and systems involved.
- r) All temporary provisions, for example root access and supplementary connections for test devices, shall be identified and registered.
- s) Software configuration and hardware implementation changes shall be forbidden when not planned, approved by the owner, and documented.
- t) Arrangements shall be in place to enable a timely restoration of an acceptable level of service in the event of a successful cyberattack. Measures shall be put in place to minimize the possibility that these arrangements are themselves vulnerable to the same cyber threats.

5.4.3.2.5 Degree S1 additional requirements

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

- a) For S1 systems, I&C programmable digital communications shall be restricted to other S1-graded I&C programmable digital systems and to S2-graded I&C programmable digital systems, and to their associated computer-based tools.
- b) Communications should be oriented from S1-graded I&C programmable digital systems towards S2-graded I&C programmable digital systems.
- c) Data network transmission from a S2-graded system to a S1-graded system shall be limited to unavoidable transmissions (e.g. for priority actuators control systems, permissives, resets), and shall be supported by a complete justification and security risk-analysis. Any data transmitted from a S2-graded system to a S1-graded system shall be secured by adapted static provisions (e.g., format and time-window controls).
- d) Software upgrade and configuration change of S1-graded systems shall be possible only by local hardware interlock means (e.g. keys) and only for one channel at time. Bidirectional data transfer between I&C equipment of highest security degree and a dedicated service station shall be performed using a dedicated and separated data connection which is decoupled from other networks. This dedicated data connection shall be secured by technical, operational and administrative means. Access with permission for software or configuration changes shall be monitored by alarms in the control room or other appropriate place.
- e) There shall be provisions against hidden functions in the system software (e.g., software code verification).
- f) Compliance with 5.7 (Software security) and 12.2 (On-site software security) of IEC 60880:2006 and IEC 62566 shall be required for S1-graded systems.
- g) Physical access to S1-graded I&C systems shall be monitored by alarms in the control room or other appropriate place.

5.4.3.2.6 Degree S2 additional requirements

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

- a) Communications should be oriented from S2-graded systems towards S3-graded systems. S2-graded systems should act as initiators of the communication. These requirements (orientation and initiation) should be enforced by appropriate security provisions (e.g. dedicated filtering equipment).
- b) Data transmission from a S3-graded system to a S2-graded system shall be strongly restricted and justified on a case-by-case basis.
- c) Software upgrade and configuration change of a S2-graded system shall not be possible from a S3-graded system.
- d) Software upgrade and configuration change of S2-graded systems shall be done only one channel at a time, only during predefined time windows, and should be protected by appropriate interlocks. Bidirectional data transfer between S2-graded I&C equipment and a dedicated service station should be performed using a dedicated and separated data connection which is decoupled from other networks. This data connection shall be secured by technical, organizational and administrative means.
- e) Entering communication into S2-graded I&C systems, either from outside the plant or from non-I&C systems, shall be prevented.

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

5.4.3.2.7 Degree S3 additional requirements

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

- a) Access from non-I&C systems which could influence the I&C system functions shall be justified on a case-by-case basis and shall not compromise security and safety requirements associated to the system.
- b) Communications between S3-graded systems and non-I&C systems should be initiated from the S3 -graded systems. Exceptions shall be justified and the connection shall be monitored.

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

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

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

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

- 5.4.3.2.4 (baseline requirements) holds for all computer-based tools.
- For S1 degree, 5.4.3.2.5 holds except for its item g) (dealing with alarms) which is not relevant for computer-based tools, and except for its item e) (dealing with hidden functions) which is superseded by the following: there should be provisions against hidden functions in the tool system software.
- For S2 degree, 5.4.3.2.6 holds except for its items c), d) and f) which are not relevant for computer-based tools. Its item e) is superseded by the following: entering communication into S2-graded I&C systems, either from outside the plant or from non-I&C systems, should be prevented.
- For S3 degree, 5.4.3.2.7 holds (same requirements).

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

5.4.3.3 Security zones

5.4.3.3.1 A possible practical implementation of the graded approach is to group I&C programmable digital systems into logical zones, where graded protective principles are applied for each security zone (see definition in Clause 3). Zones allow I&C systems with similar importance concerning safety and plant performance (i.e. having the same security degree) to be grouped together for administration and application of protective measures. Criteria for a defining security zone may include organizational issues (such as ownership/responsibility), localization, architectural or technical aspects.

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

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

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

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

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

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

- c) Network equipment (switches, cables, etc.) shall be located in a security zone consistent with those of the interconnected I&C systems. In case of network equipment connected to multiple zones, if the zones have the same security degree, then, the potential security separations shall be defined by specific facility requirements (out of the scope of this document). If the zones have different security degrees, then the security requirements associated to security degrees apply (see 5.4.3.2.4 to 5.4.3.2.7). In particular those dealing with communications and interfaces between systems of different security degrees shall involve dedicated security provisions.
- d) Communication should only be initiated from a higher security zone (grouping systems assigned to a given security degree) to a lower security zone (i.e., grouping systems assigned to a lower security degree).
- e) Zone borders require decoupling mechanisms for data flow, consistent with the security degree of the associated I&C programmable digital systems.

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

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

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

5.5 Support

5.5.1 Resources

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

5.5.2 Training, competence and awareness

5.5.2.1 Training

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

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

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

5.5.2.2 Competence

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

5.5.2.3 Awareness

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

5.5.2.4 Expertise in training and awareness

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

5.5.3 Communications about cybersecurity

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

5.5.4 Documented information

5.5.4.1 General

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

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

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

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

5.5.4.2 Creating and updating

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

5.5.4.3 Control of documented information

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

5.6 Operation

5.6.1 Operation planning and control

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

5.6.2 Cybersecurity graded approach, risk assessment and risk treatment

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

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

5.7 Performance evaluation

5.7.1 Monitoring, measurement, analysis and evaluation

5.7.1.1 General

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

5.7.1.2 Security reviews and audits

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

5.7.1.2.2 As a consequence, the organization shall:

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

5.7.2 Internal audit

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

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

5.7.3 Management review

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

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

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

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

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

5.8 Improvement

5.8.1 General

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

- a) Implement programme improvements identified during internal and external programme reviews including corrective and preventive actions.
- b) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances, and as part of the ongoing training programme.
- c) Develop and implement a review programme to periodically evaluate and update the security threat assessment and information about identified vulnerabilities.
- d) Establish measures to evaluate whether the improvements achieved their intended objectives.

5.8.2 Nonconformity and corrective action

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

5.8.3 Continual improvement

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

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

6.1 General

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

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

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

6.2 System requirements specification

6.2.1 General

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

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

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

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

6.2.1.4 Product security specifications shall be provided by the suppliers.

6.2.2 Security degree assignment

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

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

6.3 System specification

6.3.1 Selection of pre-existing components

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

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

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

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

6.3.2 System architecture

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

6.4 System detailed design and implementation

6.4.1 General

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

- a) physical and logical access to the I&C system function,
- b) use of the I&C system, and
- c) data communication with other I&C systems.

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

6.4.1.3 The requirements shall be translated into specific design criteria.

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

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

6.4.2 Risk assessment at the design phase

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

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

6.4.3 Design project security plan

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

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

6.4.3.3 In particular, the designer shall show that:

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

6.4.4 Communication pathways

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

6.4.4.2 Cybersecurity controls shall be established to:

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

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

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

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

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