

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

(standards.iteh.ai)

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

IEC 62645:2019
<https://standards.iteh.ai/catalog/standards/sist/4c5919a-17d0-410c-851f-0afe7c1fe4e/iec-62645-2019>



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 It also gives information on projects, replaced and withdrawn publications.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

iTeh STANDARD PREVIEW (standards.iteh.ai)

[IEC 62645:2019](https://standards.iteh.ai/catalog/standards/sist/41e5919a-17d0-410e-85f1-0afef7c1fe4e/iec-62645-2019)
<https://standards.iteh.ai/catalog/standards/sist/41e5919a-17d0-410e-85f1-0afef7c1fe4e/iec-62645-2019>

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.

[IEC 62645:2019](#)

<https://standards.iteh.ai/catalog/standards/sist/41e5919a-17d0-410e-85f1-0afef7c1fe4e/iec-62645-2019>

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.

<https://standards.iteh.ai/catalog/standards/sist/41e5919a-17d0-410e-85f1-6a1e1e1e1e1e/iec-62645-2019>

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.

<https://standards.iteh.ai/catalog/standards/sist/41e5919a-17d0-410e-85f1-0afef7c1fe4e/iec-62645-2019>

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.

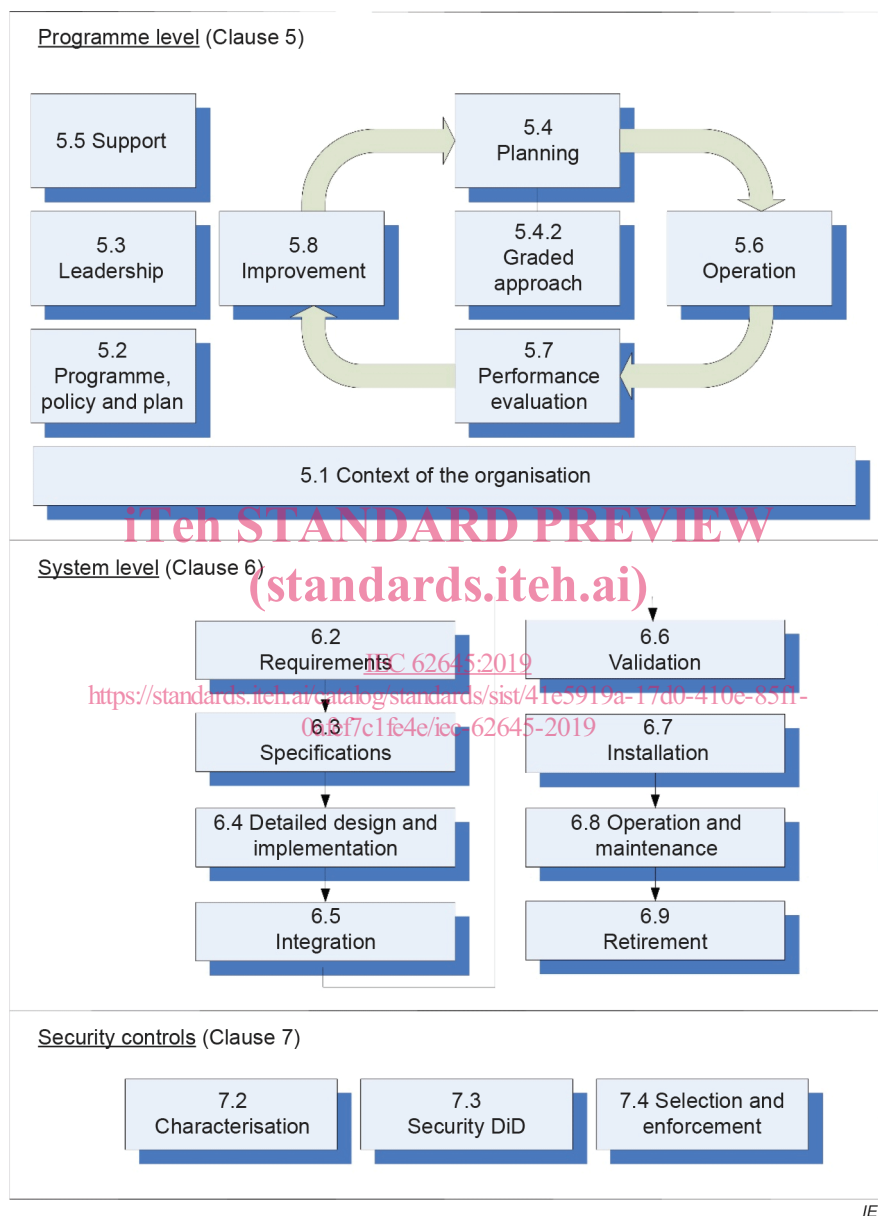


Figure 1 – Overall framework of IEC 62645

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;