IEC 63096

Edition 1.0 2020-10

INTERNATIONAL STANDARD

colour inside

Nuclear power plants – Instrumentation, control and electrical power systems – Security controls

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-8837-5

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – SECURITY CONTROLS

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 63096 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/1346/FDIS	45A/1353/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.

This document is based on ISO/IEC 27002:2013.

Clause 5 through Clause 18 of this document follow ISO/IEC 27002:2013, Clause 5 through Clause 18.

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

For I&C systems in nuclear power plants this IEC standard specifically focuses on the selection and application of security controls from the included security controls catalogue, in order to prevent, detect and react to cyberattacks against computer based I&C systems.

This standard applies to all Nuclear I&C programmable digital systems throughout the life cycle of the system. It may also be applicable to other types of nuclear facilities. It applies to the I&C programmable digital systems of new nuclear power plants and to the modernization or modification of I&C Programmable Digital Systems in existing plants. It was prepared and based on IEC 62645 and ISO/IEC 27002, IAEA and country specific guidance in this expanding technical and security focus area.

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

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

This standard (IEC 63096) is a third level IEC SC 45A document tackling the generic issue of cybersecurity controls and supplements IEC 62645 with more details on security controls.

IEC 62645 is considered formally as a second level document with respect to IEC 61513. IEC 62645 is the top-level document with respect to cybersecurity in the SC 45A standard series.

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

It is important to note that this standard establishes additional cybersecurity related requirements for I&C systems with regard to the I&C platform and I&C system functionality and the environments for the development of I&C platforms and the engineering, installation, commissioning, operation and maintenance of I&C systems in nuclear power plants.

Aspects for which special requirements and recommendations have been produced are:

– IAEA guidance on computer security at nuclear facilities

– ISO/IEC series on Information Security Management Systems (ISMS)

– Regulatory interpretations for country specific requirements for countries participating in this project.

It is recognized that this is an evolving area of regulatory requirements, due to the changing and evolving nature of computer security threats.

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 power 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 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.

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.

The IEC SC 45A standards series consistently implements and details 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.

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, that are based on the requirements of a standard such as IEC 61508.

NOTE 2 IEC/SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in 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 – SECURITY CONTROLS

1 Scope

1.1 General

Since strict requirements on safety and availability of nuclear I&C apply, due consideration of cybersecurity threats is needed.

Since nowadays nuclear I&C programmable digital systems are largely based on digital systems including networks, individual I&C systems are more and more interconnected, and the I&C equipment is widely spread within the NPP area, security controls for prevention, detection and correction are needed to protect nuclear I&C programmable digital systems from external and internal cybersecurity threats.

The objective of this document is to extend the SC 45A series of documents addressing cybersecurity with IEC 62645 as its top-level document, by defining nuclear I&C programmable digital system specific security controls for I&C systems of the Safety Classes 1, 2, 3 and for non-classified (NC) I&C systems. The safety classification of I&C systems, and associated safety requirements, are among the biggest differences compared to typical IT systems and standard industrial automation systems. Annex B contains a correspondence between IEC 62645 and IEC 63096.

This document, based on the security controls defined in ISO/IEC 27002, reflects the special security control requirements for nuclear I&C programmable digital systems. The original ISO/IEC 27002 requirements are either modified, detailed or completed, wherever deemed necessary from a nuclear I&C programmable digital system perspective. Additional nuclear I&C programmable digital system specific security controls that are not identified in ISO/IEC 27002, but deemed necessary are also added.

This document refers in detail to ISO/IEC 27002:2013. A later modification of ISO/IEC 27002:2013 will not automatically influence the modifications, detailing and completions given by IEC 63096 without analysing the consequences from the nuclear I&C perspective.

By applying and extending the ISO/IEC 27002:2013 security controls, this document implicitly reflects all lifecycle phases of nuclear I&C programmable digital system platforms and systems.

By selecting the highly recommended security controls based on the processes as defined in IEC 62645 and the additional process details described within this document the risk level will be reduced to an acceptable level.

The selection of security controls ensures that both safety and security requirements are met according to IEC 62859. If a specific security control negatively influences safety, safety prevails (see IEC 62859) and a compensatory security control should be implemented.

For the development of this document ISO/IEC 27009 has been followed as far as applicable, also considering that ISO/IEC 27009 is not binding for the SC 45A IEC standard series.

ISO/IEC 27019 explicitly excludes the “process control domain of nuclear facilities”.

NOTE The term “process control domain of nuclear facilities” is a quote from ISO/IEC 27019.

1.2 Objectives

This document provides a catalogue of highly recommended and optional security controls graded (see Clause 5 to Clause 20) in line with the security degrees defined by IEC 62645. These are intended for nuclear I&C programmable digital systems and architecture including related activities (I&C platform development, project engineering, operation and maintenance).

This document establishes requirements and guidance to:

– select and apply security controls for nuclear I&C programmable digital systems;

– propose and apply compensatory security controls in case a highly recommended security control cannot be implemented (e. g. due to technical reasons);

– credit/inherit existing security controls and safety provisions implemented for I&C systems important to safety as compensatory security controls;

– handle the security of legacy I&C.

Application of cybersecurity controls on the overall I&C architecture level is not considered in this document.

Safety remains the top priority from a nuclear I&C programmable digital system perspective. IEC 62859 provides requirements and guidance to coordinate cybersecurity measures with safety.

1.3 Application

This document is intended to be used for designing I&C systems for new NPPs, and modernizing and modifying I&C systems for existing NPPs throughout the I&C programmable digital systems lifecycle. It may also be applicable to other types of nuclear facilities.

This document addresses the whole scope of nuclear I&C programmable digital systems, both safety and non-safety classified.

The scope of this document also includes sensors, actuators and electrical systems that belong to the I&C control loop.

It is also applicable to those parts of electrical systems covered by IEC 63046, which rely on digital programmable technology. For better readability the terms “nuclear I&C programmable digital systems”, “I&C system” or “I&C platform” used in this document implicitly include electrical systems if the electrical system includes a programmable digital systems.

NOTE It is recognized that electrical systems are not necessarily classified according to IEC 61226. Therefore, the security degree classification used in this document might not be usable for electrical systems.

This document also defines security controls on access control and physical protection as needed for protecting nuclear I&C programmable digital systems and electrical systems against cyberattacks. The NPP wide cybersecurity for Facility Management (Building Technology) is beyond the scope of IEC SC 45A. For details on the cybersecurity scope in the context of physical protection for nuclear I&C programmable digital systems, see IEC 62645.

This document is applicable to nuclear I&C programmable digital systems of NPPs, including their maintenance and configuration tools (e.g. engineering or diagnostic tools). This also includes the interfaces to 3rd party I&C programmable digital systems, 3rd party computer systems or other IT- networks.

The scope of this document includes:

– Security controls for the I&C platform and the I&C system itself.
– Security controls for the I&C platform development environment.
– Security controls for the I&C system engineering environment including installation and commissioning phases.
– Security controls for the I&C system operation and maintenance environmen.t

This document is intended to be used by the audience, as defined in 4.1, for the following activities:

– I&C Platform Development.
– Project Engineering for plant specific I&C system.
– Operation and Maintenance of I&C system.

1.4 Framework

This document comprises the following normative clauses:

– Clause 4 deals with the selection of security controls and its interconnection to IEC 62645 and IEC 62859.
– Clause 5 through Clause 18 comprise the security control clauses and for each control clause the control categories as defined in ISO/IEC 27002:2013.

  ISO/IEC 27002:2013 security control clauses are either taken over without modification or modified or completed for the nuclear I&C programmable digital systems domain. Necessary nuclear specific modifications are indicated clearly within each clause.

  For each security control clause, additional nuclear I&C programmable digital system specific information is given: Applicability for security degrees, applicability for activities (life cycle), the preservation objective (confidentiality, integrity and availability) and the security control focus (prevention, detection and correction).
– Clause 19 and Clause 20 comprise nuclear security specific control clauses that are additional to the ISO/IEC 27002:2013 clauses.

NOTE Annex A summarizes all security controls including their applicability for security degrees, their applicability for activities, the preservation objective and the control focus.

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, control and electrical power systems important to safety – Categorization of functions and classification of systems*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61513, *Nuclear power plants – Instrumentation and control for systems 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 62443-2-1:2010, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62443-2-4, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

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

IEC 62645:2019, *Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements*

IEC 62671, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

IEC 62859:2016, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

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

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

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

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

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

ISO/IEC 27007*, Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing*

ISO/IEC TS 27008, *Information technology – Security techniques – Guidelines for the assessment of information security controls*

ISO/IEC 27033 (all parts), *Information technology – Security techniques – Network security*

ISO/IEC 27035-1*, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management*

ISO/IEC 27035-2*, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*

ISO/IEC 27036-1*, Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*

ISO/IEC 27036-2*, Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements*

ISO/IEC 27036-3, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*

ISO/IEC 27037, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*

ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

ISO/IEC 29101: *Information technology – Security techniques – Privacy architecture framework*

ISO 15489-1, *Information and documentation – Records management – Part 1: Concepts and principles*

ISO 31000, *Risk management – Guidelines*

IAEA Nuclear Security Series No. 10, *Development, Use and Maintenance of the Design Basis Threat (NSS10)*

IAEA Nuclear Security Series No. 17, *Technical Guidance – Computer Security at Nuclear Facilities (NSS17)*

IAEA Nuclear Security Series No. 33-T, *Technical Guidance – Computer Security of Instrumentation and Control Systems at Nuclear Facilities (NSS33-T)*

IAEA Specific Safety Guide No. SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants (SSG-39)*

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST SP 800-57 Part 1 Revision 4, *Recommendation for Key Management – Part 1: General*