



BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of IEC 63096:2020.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Instrumentation, Control & Electrical Systems of Nuclear Facilities.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020

Published by BSI Standards Limited 2020

ISBN 978 0 539 00167 9

ICS 27.120.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2020.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



IEC 63096

Edition 1.0 2020-10

INTERNATIONAL STANDARD



**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

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	11
1.1 General.....	11
1.2 Objectives.....	12
1.3 Application.....	12
1.4 Framework.....	13
2 Normative references	13
3 Terms, definitions and abbreviated terms	15
3.1 Terms and definitions.....	15
3.2 Abbreviated terms.....	22
4 Nuclear I&C programmable digital systems specific security controls.....	23
4.1 Target audience and related life-cycle activities	23
4.2 Source for definition of nuclear I&C programmable digital systems specific security controls.....	24
4.2.1 General	24
4.2.2 Security degrees and baseline requirements.....	25
4.2.3 Computer-based tools for I&C system– engineering, –maintenance and –diagnostic	26
4.2.4 Safety and security	26
4.3 Security controls catalogue	26
4.3.1 General	26
4.3.2 ISO/IEC 27002 is the basis for IEC 63096 security controls	26
4.3.3 Modification/ extension of the ISO/IEC 27002:2013 security control description.....	27
4.3.4 Structure of each security control description	27
4.4 Process of selecting security controls	30
4.4.1 General	30
4.4.2 Process of selecting and implementing security controls for the actual I&C platform and I&C system.....	32
4.4.3 Process of selecting and implementing security controls for D- activity → I&C Platform Development	36
4.4.4 Process of selecting and implementing security controls for E- activity → I&C system engineering	36
4.4.5 Process of selecting and implementing security controls for O- activity → Operation and Maintenance of I&C system	38
4.4.6 Additional process requirements valid for controls for the “actual I&C platform and I&C system” and for the D-, E- and O- activity	39
4.5 Documentation and traceability of security controls.....	40
4.5.1 Documentation of security controls selection (statement of applicability)	40
4.5.2 Traceability.....	40
5 Cybersecurity policies.....	40
5.1 Management direction for <i>cybersecurity</i>	41
5.1.1 Policies for <i>cybersecurity</i>	41
5.1.2 Review of the policies for <i>cybersecurity</i>	43
6 Organization of <i>cybersecurity</i>	44
6.1 Internal organization	44
6.1.1 <i>Cybersecurity</i> roles and responsibilities.....	44

6.1.2	Segregation of duties.....	47
6.1.3	Contact with authorities	48
6.1.4	Contact with special interest groups	49
6.1.5	<i>Cybersecurity</i> to project management.....	49
6.2	Mobile devices and teleworking.....	50
6.2.1	Mobile device policy	50
6.2.2	Teleworking	53
7	Human resource security	56
7.1	Prior to employment.....	56
7.1.1	Screening	56
7.1.2	Terms and Conditions of Employment.....	58
7.2	During employment.....	58
7.2.1	Management responsibilities.....	58
7.2.2	<i>Cybersecurity</i> Awareness, Education and Training.....	59
7.2.3	Disciplinary process.....	59
7.3	Termination and change of employment.....	60
7.3.1	Termination or change of employment responsibilities	60
8	Asset management.....	60
8.1	Responsibility for assets	60
8.1.1	Inventory of assets	60
8.1.2	Ownership of assets	62
8.1.3	Acceptable use of assets	62
8.1.4	Return of assets	62
8.2	Information classification	63
8.2.1	Classification of information.....	63
8.2.2	Labelling of information	64
8.2.3	Handling of assets	65
8.3	Media handling	65
8.3.1	Management of removable media	65
8.3.2	Disposal of media	66
8.3.3	Physical media transfer	66
8.3.4	<i>NUC – Removable media management</i>	66
9	Access control.....	67
9.1	<i>Requirements</i> of access control	67
9.1.1	Access Control Policy	67
9.1.2	Access to network and network services.....	74
9.2	User access management.....	77
9.2.1	User registration and de-registration.....	77
9.2.2	User access provisioning	77
9.2.3	Management of privileged access rights	78
9.2.4	Management of secret authentication information of users.....	79
9.2.5	Review of user access rights	80
9.2.6	Removal or adjustment of access rights.....	80
9.3	User responsibilities.....	81
9.3.1	Use of secret authentication information	81
9.4	System and application access control.....	81
9.4.1	Information access restriction	82
9.4.2	Secure log-on procedures.....	82
9.4.3	Password management system.....	82

9.4.4	Use of privileged utility programs	83
9.4.5	Access control to program source code	84
10	Cryptography	84
10.1	Cryptographic controls	84
10.1.1	Policy on the use of cryptographic control.....	85
10.1.2	Key management.....	89
11	Physical and environmental security	91
11.1	Secure areas	91
11.1.1	Physical security perimeter	91
11.1.2	Physical entry controls.....	93
11.1.3	Securing offices, rooms and facilities	94
11.1.4	Protecting against external and environmental threats	94
11.1.5	Working in secure areas	95
11.1.6	Delivery and loading areas <i>and ware houses</i>	95
11.2	Equipment	96
11.2.1	Equipment siting and protection.....	96
11.2.2	Supporting utilities	98
11.2.3	Cabling security	99
11.2.4	Equipment maintenance	99
11.2.5	Removal of assets	100
11.2.6	Security of equipment and assets off-premises	101
11.2.7	Secure disposal or re-use of equipment.....	102
11.2.8	Unattended user equipment.....	103
11.2.9	Clear desk and clear screen policy	104
12	Operations security.....	104
12.1	Operational procedures and responsibilities	105
12.1.1	Documented operating Procedures	105
12.1.2	Change management.....	106
12.1.3	Capacity management	107
12.1.4	Separation of development, testing and operational environments	107
12.2	Protection from malware	108
12.2.1	Controls against malware	108
12.3	Backup	110
12.3.1	Information backup	110
12.4	Logging and monitoring.....	111
12.4.1	Event logging.....	111
12.4.2	Protection of log information	113
12.4.3	Administrator and operator logs	113
12.4.4	Clock synchronisation	114
12.4.5	<i>NUC – Centralization of collected cybersecurity events</i>	115
12.4.6	<i>NUC – Logs correlation and cyberattack scenarios identification</i>	115
12.5	Control of operational software	116
12.5.1	Installation of software on operational systems	116
12.5.2	<i>NUC – Only needed software packages</i>	118
12.6	Technical vulnerability management	119
12.6.1	Management of technical vulnerabilities.....	119
12.6.2	Restrictions on software installation.....	121
12.6.3	<i>NUC – Technical vulnerabilities information sources and channels</i>	121
12.6.4	<i>NUC – Restrictions on software execution</i>	122

12.7	Systems audit considerations	122
12.7.1	Systems audit controls	123
13	Communications security	123
13.1	Network security management	123
13.1.1	Network controls	123
13.1.2	Security of network services	130
13.1.3	Segregation in networks	132
13.2	Information transfer	136
13.2.1	Information transfer policies and procedures	136
13.2.2	Agreements on information transfer	138
13.2.3	Electronic messaging	138
13.2.4	Confidentiality or non-disclosure agreements	140
14	System acquisition, development and maintenance	141
14.1	Security requirements of information systems	141
14.1.1	<i>Cybersecurity</i> Requirements Analysis and Specification	141
14.2	Security in development and support processes	142
14.2.1	Secure development policy	142
14.2.2	System change control procedures	143
14.2.3	Technical review of applications after operating platform changes	144
14.2.4	Restrictions on changes to software packages	145
14.2.5	Secure system engineering principles	145
14.2.6	Secure development environment	146
14.2.7	Outsourced development	147
14.2.8	System security testing	148
14.2.9	System acceptance testing	148
14.3	Test data	149
14.3.1	Protection of test data	149
15	Supplier relationships	150
15.1	<i>Cybersecurity</i> in supplier relationships	150
15.1.1	<i>Cybersecurity</i> policy for supplier relationships	150
15.1.2	Addressing security within supplier agreements	151
15.1.3	Information and communication technology supply chain	153
15.2	Supplier service delivery management	154
15.2.1	<i>Cybersecurity</i> policy for supplier relationships	154
15.2.2	Managing changes to supplier services	155
16	<i>Cybersecurity</i> incident management	156
16.1	Management of <i>I&C cybersecurity</i> incidents and improvements	156
16.1.1	Responsibilities and procedures	156
16.1.2	Reporting <i>I&C cybersecurity</i> events	162
16.1.3	Reporting <i>I&C cybersecurity</i> weaknesses	162
16.1.4	Assessment of and decision on <i>I&C cybersecurity</i> events	163
16.1.5	Response to <i>I&C cybersecurity</i> incidents	164
16.1.6	Learning from <i>I&C cybersecurity</i> incidents	165
16.1.7	Collection of evidence <i>from I&C</i>	165
17	<i>Cybersecurity</i> aspects of business continuity management	167
17.1	<i>Cybersecurity</i> continuity	167
17.1.1	Planning <i>cybersecurity</i> continuity	167
17.1.2	Implementing <i>cybersecurity</i> continuity	168

17.1.3	Verify, review and evaluate <i>cybersecurity</i> continuity	169
17.2	Redundancies	170
17.2.1	Availability of <i>I&C systems</i>	170
18	Compliance	170
18.1	Compliance with legal and contractual requirements	171
18.1.1	Identification of applicable legislation and contractual requirements	171
18.1.2	Intellectual property rights	172
18.1.3	Protection of records	172
18.1.4	Privacy and protection of personally identifiable information	173
18.1.5	Regulation of cryptographic controls	174
18.2	Information security reviews, <i>audits</i> , and <i>inspections</i>	175
18.2.1	Independent review of cybersecurity	176
18.2.2	Compliance with security policies and standards	177
18.2.3	Technical compliance reviewing.....	177
19	<i>NUC – Cybersecurity and architecture</i>	179
19.1	<i>NUC – Cybersecurity and architecture controls</i>	179
19.1.1	<i>NUC – Security levels</i>	179
19.1.2	<i>NUC – Security zones</i>	180
19.1.3	<i>NUC – Administration security zones</i>	181
19.1.4	<i>NUC – Data extraction and collection</i>	182
19.1.5	<i>NUC – Temporary elements introduction within a security zone</i>	182
20	<i>NUC – Virtualization environment and infrastructure</i>	183
20.1	<i>NUC – Virtualization environment and infrastructure controls</i>	183
20.1.1	<i>NUC virtualized I&C environments</i>	183
Annex A (informative)	Security Controls by Security Degrees, activities, I&C platform or I&C system, preservation focus, control focus and ISO/IEC 27002 modification	185
Annex B (informative)	Correspondence with IEC 62645:2019.....	235
Annex C (informative)	Sample list for documentation of project specific security controls selections	240
Annex D (informative)	Semi-formal representation and exchange of security controls	243
Annex E (informative)	Cryptography	244
E.1	Risk categorization	244
E.2	Information to be provided for transporting data	244
E.3	Cybersecurity roles	244
E.4	Two-factor authentication process for key management system access	245
Bibliography		246
Figure 1 – E/E/PE items		17
Figure 2 – Overview		31
Figure 3 – Process of selecting and implementing security controls for the actual I&C platform and I&C system		33
Table A.1 – Security controls overview		186
Table B.1 – Correspondence between IEC 62645:2019 and IEC 63096		235
Table C.1 – Sample list for documentation of project specific security controls selections		241

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 environment.

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 systems – 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*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 27000, IAEA NSS17, IEC 61513, IEC 62645 and IEC 62859, and the following 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>

3.1.1

3rd party software

software that is not developed by the I&C platform developer but purchased from another vendor and integrated into the I&C platform

3.1.2

business continuity

ability of a company to continue working after a computer failure due to a cybersecurity event that might interrupt business

Note 1 to entry: Typically, the term refers to all kinds of events that might interrupt business. In the context of this document the term has been adapted and focused on cybersecurity events.

3.1.3

administrative controls

policies, procedures and practices designed to protect computer systems by controlling personnel actions and behaviours

Note 1 to entry: The administrative controls are directive in nature, specifying what employees and third-party personnel should and should not do. In the nuclear environment, administrative controls are understood to include operational and management controls.

3.1.4

application software

software that defines the project specific behaviour of an I&C system that is based on an I&C platform. The application software is typically developed by utilizing the engineering tool(s) that are provided by the I&C platform (e. g. functional plan editor, plant display editor).

3.1.5

compensatory control

alternative security control that is selected and that meets the security requirements in case a highly recommend security control cannot be implemented due to technical, or other reasons or if it contradicts safety requirements

Note 1 to entry: Contradictions between security requirements and safety requirements shall be resolved.

3.1.6

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]

3.1.7

cyberattack

attempt by digital means to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

Note 1 to entry: Cyberattacks include targeted and non-targeted (e.g. malwares) attacks by digital means. Cyberattack is synonymous with digital attack.

[SOURCE: IEC 62859:2016, 3.2]

3.1.8

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 (including 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 (including 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: Computer security, security and cybersecurity are considered synonymous in this document.

[SOURCE: IEC 62645:2019, 3.7]

3.1.9

cybersecurity event

identified occurrence of a system, service or network state indicating a possible breach of cybersecurity policy or failure of controls, or a previously unknown situation that *might* be security relevant

[SOURCE: ISO/IEC 27000:2018, modified: Term “information security event” changed to “cybersecurity event”.]

3.1.10

cybersecurity incident

single or a series of unwanted or unexpected cybersecurity events (3.1.9) that have a significant probability of compromising *nuclear safety*, plant operations and threatening cybersecurity

[SOURCE: ISO/IEC 27000:2018, modified: Term “information security incident” changed to “cybersecurity incident”.]

3.1.11

development environment

environment needed for the I&C platform development (D-activity). It also includes but is not limited to topics regarding organisation, personnel, physical space, processes, assets, IT infrastructure, development tools.

3.1.12

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 1.

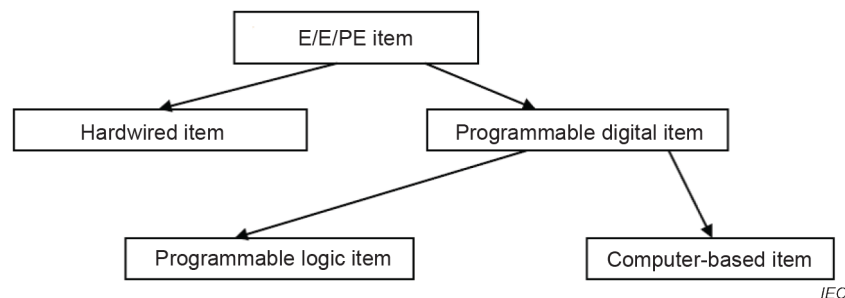


Figure 1 – E/E/PE items

[SOURCE: IEC 62138: 2018, 3.15]

3.1.13

electronic messaging

exchange of electronic data from one person to another person using electronic information transmission technology such as email, fileserver, instant messaging or other electronic data interchange means

3.1.14 engineering environment

environment needed for the project specific I&C engineering (E_b - activity). It also includes but is not limited to topics regarding organisation, personnel, physical space, processes, assets, IT infrastructure, I&C engineering tools

Note 1 to entry: This also includes the tools for the development of the I&C application software.

3.1.15 hardened I&C

I&C programmable digital system, whose surface of cybersecurity vulnerability is reduced by applying appropriate security controls

Note 1 to entry: The term hardened I&C is also used in the context of safety for I&C and electrical systems.

3.1.16 highly recommended security control

security control that shall be implemented unless there is an approved justification, why it cannot be implemented (e.g. security control does have negative impact on safety function)

3.1.17 I&C platform

set of hardware and software components that finally work co-operatively in one or more defined architectures (configurations). The development of plant specific I&C configurations and of the related application software may be supported by I&C engineering tools. An I&C platform usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate project specific application software

Note 1 to entry: An I&C platform represents an I&C programmable digital system and can therefore be a programmable logic item or a computer-based item or a combination of both.

Note 2 to entry: An I&C platform may be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier.

Note 3 to entry: The term I&C platform, as used in this document, also includes I&C products and Electrical Power Systems (EPS) platforms and products.

[SOURCE: IEC 61513:2011, modified: Term “equipment family” changed to “I&C platform”.]

3.1.18 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]

3.1.19**legacy I&C**

I&C system based on outdated technology, hardware or software components

3.1.20**nuclear I&C programmable digital system**

programmable logic items and computer-based items

3.1.21**mobile devices**

intelligent processor-based non-stationary devices that are not permanently installed (e.g. not permanently installed in a cabinet) such as notebooks, laptops, programming or diagnostic devices for the I&C platform or cell phones

3.1.22**optional security control**

security control that could be implemented but does not have to be implemented

3.1.23**penetration test**

authorized simulated cyberattack on a computer system, performed to evaluate the security of the system

Note 1 to entry: Fuzzing is typically in the scope of penetration testing. Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.

3.1.24**physical controls**

physical barriers for the protection of computer and supporting assets from physical damage and unauthorized physical access

Note 1 to entry: The physical controls include barriers such as locks, physical encasements, tamper seals, isolation rooms, gates and guards.

3.1.25**product**

system made available for consumer or business use. It is anything that can be offered to a market to satisfy the desire or need of a customer

3.1.26**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]

3.1.27**programmable logic item**

item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable

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: A programmable logic item is a kind of programmable digital item.

Note 3 to entry: See also the definition of E/E/PE item and the associated notes.

3.1.28

RACI model

tool that can be used for identifying roles and responsibilities. Processes do not process themselves, people have to "do" something to make the processes happen

3.1.29

security controls

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

Note 1 to entry: For better understanding, synonyms for the term "security control" are "security measure", "security countermeasure" or "security provision".

Note 2 to entry: Physical security/protection is considered within this document a subset of security controls. Security controls dealing with physical security are addressed in Clause 11. For details on the cybersecurity scope in the context of physical protection for nuclear I&C programmable digital systems, see IEC 62645.

Note 3 to entry: Although physical security is a subset of the security controls, the requirements on the systems applied for physical security (e. g. physical access control systems) are not in the scope of this document. For details on the cybersecurity scope in the context of physical protection for nuclear I&C programmable digital systems, see IEC 62645.

Note 4 to entry: A security control is a measure to control security and is not actual "controls" in the sense of I&C systems.

[SOURCE: IEC 62645:2019, 3.18]

3.1.30

security controls for the actual I&C platform and I&C system

technical security controls that come either with the I&C platform or are project specifically engineered and physical security controls that are recommended for the I&C system in the plant environment

3.1.31

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: 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.

[SOURCE: IEC 62645:2019, 3.19]

3.1.32

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 similar concept as "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.

[SOURCE: IEC 62645:2019, 3.20]

3.1.33**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: IEC 62645:2019, 3.21]

3.1.34**severe security incident**

security incident that results in a breach of confidentiality, integrity or availability

3.1.35**source code**

I&C platform system software is typically developed based on programming language (e. g. C, C++). The code written based on the syntax of a specific programming language is the so-called source code

3.1.36**statement of applicability**

selection and implementation of security controls should be documented within a statement of applicability to assist with compliance requirements

[SOURCE: ISO/IEC 27000:2018, 3.5.5 e), modified: “controls” extended to “security controls”.]

3.1.37**technical controls**

hardware and/or software solutions for the protection, detection and mitigation of and recovery from intrusion or other malicious acts

3.1.38**teleworking**

use of information technology and telecommunications technology to access the I&C platform development environment or the I&C system engineering environment from a remote location

3.1.39**tools**

engineering or diagnostic tools that come with the I&C platform or tools that can be used for implementing a security control as indicated in the tools line for each security control

3.1.40**virtualization**

simulation of the software and/or hardware upon which other software runs

[SOURCE: NIST Special Publication 800-125:2011, Guide to Security for Full Virtualization Technologies]

3.1.41**web**

refers to the world wide web, an internet-based hypertext system

3.2 Abbreviated terms

A	Availability
BIOS	Basic Input Output System
BR	Baseline Requirement
BT	Building Technologies
c	Correction
C	Confidentiality
CA	Certificate Authority
CB&HPD	Computer Based & HDL- Programmed Device
CIA	Confidentiality, Integrity, Availability
CERT	Computer Emergency Response Team
COTS	Commercial Off-The-Shelf
CSA	Cryptography Security Administrators
CSM	Cryptography Security Manager
CSO	Computer Security Officer
CSSO	Computer System Security Officer(s)
CSV	Comma- Separated Values
CSW	Cryptography Security Witnesses
d	Detection
D	I&C Platform Development
DBT	Design Basis Threat
DEO	Development Engineering Operation
E	Project engineering for plant specific I&C system
ES	Electrical Systems
FAT	Factory Acceptance Test
GPS	Global Positioning System
GUID	Globally Unique Identifier
HDL	Hardware Description Language
HMI	Human-Machine Interface
I	Integrity
IACS	Industrial Automation and Control System
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
ICS	Industrial Control System
ICS-CERT	Industrial Control System – Computer Emergency Response Team
ICT	Information and Communication Technology
ID	Identifier
IMS	Integrated Management System
IT-	Information Technology -
LAN	Local Area Network
NC	Non-Classified
NCS	Nuclear Control Systems
NDA	Non-Disclosure Agreement

NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NUC	Nuclear
O	Operation and Maintenance of I&C system
OEM	Original Equipment Manufacturer
OS	Operating System
p	Prevention
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PoC	Point of Contact
PrKI	Private Key Infrastructure
QA	Quality Assurance
RACI	Responsible, Accountable, Consulted, Informed
RefList	Reference List
S1	Security Degree 1
S2	Security Degree 2
S3	Security Degree 3
SD	Security Degree
SIEM	Security Incident Event Monitoring
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SW	Software
SWID	Software Identification
TID	Tamper-Indicating Device
UK	United Kingdom
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTF-8	8-Bit UCS Transformation Format
V&V	Verification and Validation
VLANS	Virtual LANs
VPN	Virtual Private Network
XML	Extensible Mark-up Language

4 Nuclear I&C programmable digital systems specific security controls

4.1 Target audience and related life-cycle activities

This document is intended for the parties responsible for the following I&C related activities:

- a) I&C Platform Development (project independent I&C platform development)
 - Requirements (Requirements specification phase)
 - Specifications (Functional specification phase)
 - Detailed design and Implementation (HW selection and development, System Software development/ coding)

- Integration (I&C platform component integration test phase)
- Validation (I&C platform system integration test phase and I&C platform release)
- Maintenance
- Retirement (Discontinuation of I&C platform development and maintenance)
- b) Project Engineering for plant specific I&C system (System level development based on I&C platform)
 - Project Engineering activities before Installation and Commissioning
 - Requirements (project specifically)
 - Specifications (project specifically)
 - Detailed design and implementation (project specifically)
 - Integration (offsite integration)
 - Validation (factory acceptance testing)
 - Shipping to site
 - Project Engineering activities for Installation and Commissioning
 - Installation (Onsite Integration and Acceptance Testing)
 - Commissioning (Commissioning and Acceptance Testing)
- c) Operation and Maintenance of I&C system (System level)
 - Operation and Maintenance
 - Retirement

The responsibility for the above-mentioned activities varies from project to project and does not explicitly show all related V&V in order to keep the activity list simple.

If additional activities, not reflected in this document, appear, the respective party decides to what main activity the missing activity belongs and then follows the resulting security controls.

NOTE Modifications are not explicitly mentioned in the above activities and life cycle phases. However, also I&C platform or I&C system modifications are to be done according to the above-mentioned life cycle phases. The life cycle phases are taken from IEC 62645.

4.2 Source for definition of nuclear I&C programmable digital systems specific security controls

4.2.1 General

The security controls described in this document are based on the following sources:

- IEC 62645: IEC 63096 provides more detailed content on the three types of cybersecurity controls than given by IEC 62645 (technical, physical and administrative controls) and is in line with the security degrees as defined in IEC 62645;
- ISO/IEC 27002:2013 providing a catalogue of security controls, grouped under 14 clauses and 35 categories. Where it is deemed necessary, IEC 63096 details or complements these to match these to the nuclear specific requirements and cybersecurity protections needs of a typical I&C architecture and its individual I&C systems for NPPs.

ISO/IEC 27002:2013 is information security-oriented and does not consider nuclear I&C programmable digital system specific aspects and is not directly applicable in this context;

NOTE 1 In the frame of IEC 63096 edition 2, other codes and standards might be analysed for additional useful controls for the nuclear I&C domain (e. g. IEC 62443).

NOTE 2 Edition 1 already includes some selected references to IEC 62443.

The security controls described in this document fully take into account:

- IEC 62645: The security grading in IEC 63096 is in line with the security degrees as defined in IEC 62645;
- IEC 62859: Considerations on coordinating the requirements between safety and cybersecurity (IEC 62859);
- Safety classification of individual I&C systems and their role for plant safety and availability (IEC 61513, IEC 61226);
- Typical Overall I&C architectures consisting of Safety Class 1, Class 2, Class 3 and NC-I&C systems including the interfaces between these I&C systems and their interfaces to computer systems outside of the I&C perimeter (IAEA SSG-39, NSS17, NSS33-T, IEC SC 45A standard series).

NOTE 3 The overall I&C architectures consists of multiple individual I&C systems. An individual I&C system typically has an interface to other individual I&C systems. An individual I&C system could also have interfaces to other computer system beyond the I&C perimeter (e. g. to the office environment or technical support centre). The security controls for the resulting interface are covered by this document.

Finally, this document relies on:

- State of the art requirements from the nuclear industry and nuclear authority landscape at the point of time of developing this document (e.g.: ISO/IEC 27000 series, NIST SP 800-53);
- Experience from cybersecurity threat and risk analyses that have already been performed for recent nuclear I&C programmable digital system projects at the point of time of developing this document;
- Considerations for legacy I&C platform.

4.2.2 Security degrees and baseline requirements

One of the major differences between IEC 63096 and other industrial cybersecurity standards (e.g. IEC 61508, 62443) is the objective for protection. Nuclear I&C programmable digital systems perform functions that are required to ensure the safe operation of a nuclear power plant, thereby preventing unacceptable radiological consequences (IAEA Safety Fundamentals). In nuclear all individual I&C systems are assigned to a specific safety class according to the category (category defined in IEC 61226) of the safety function (i.e. consequence-based evaluation) they are performing. The industrial standards IEC 61508 and IEC 62443 are based on safety integrity levels.

Therefore, the security grade approach introduced by IEC 62645 takes great care to ensure protection of these safety functions. IEC 62645 defines three security degrees (S1, S2 and S3).

For this document, a security baseline called “Baseline Requirement” has been introduced for all I&C systems independent from their security degree.

That means that all I&C systems independent from their security degree shall follow those security controls that are highly recommended for the security baseline “Baseline Requirement”. That means that I&C systems not assigned to a Security Degree shall meet the “Baseline Requirement”.

NOTE In given contexts, the “Baseline Requirement” can be considered as a security degree.

In addition to the security baseline “Baseline Requirement” this document defines for each individual security control additional highly recommended security controls depending on the security degree of the individual I&C system.

Also depending on the security degree including the security baseline “Baseline Requirement” some security controls are indicated as optional. That means that the user of this document can decide on whether to apply this security control or not. If an optional security control is not selected no compensatory security control is necessary. A justification is not required.

4.2.3 Computer-based tools for I&C system– engineering, –maintenance and – diagnostic

4.2.3.1 Security controls

Computer-based tools for I&C- engineering, -maintenance and -diagnostic purposes shall be considered a component of the I&C platform. These tools will typically be delivered as part of the I&C system to the NPP site. As a result, security controls shall also be selected for these types of computer based I&C platform tools.

4.2.3.2 Threat and risk assessment

Computer-based tools for I&C- engineering, -maintenance and -diagnostic shall also be considered an asset in terms of the threat and risk analysis. As a result, computer-based tools for the I&C system are also subject to the threat and risk assessment.

4.2.4 Safety and security

Since nuclear I&C programmable digital systems perform safety functions, it can be the case that a specific highly recommended security control negatively impacts the respective safety function. In this case, according to IEC 62859, safety prevails. As a result, the highly recommended control cannot be implemented and a compensatory security control, that does not negatively influence the safety function, shall be implemented (see also 4.4.6.1).

IEC 62859 defines the details on handling the safety and security topic.

4.3 Security controls catalogue

4.3.1 General

The security controls catalogue is represented by Clause 5 through Clause 20.

For each security degree the security controls catalogue constitutes the generic Statement of Applicability for the nuclear I&C programmable digital system domain.

NOTE A Statement of Applicability is requested by ISO/IEC 27001:2013, 6.1.3d).

Annex A contains an overview list of all security controls. For each security control all important properties as described in 4.3.4 are included. Annex A also provides information on whether the original ISO/IEC 27002:2013 security control has been taken over with no modification, modified or extended or whether a new security control that is not included in ISO/IEC 27002:2013 has been added.

The Annex A overview table is also available in the CSV (comma-separated values) format (.csv) and the XLSX format (.xlsx). Both files are embedded as attachments to the IEC 63096 PDF- document.

For easy filtering and project specific additions the CSV file can be easily imported into spread sheet or data base tools. The XLSX file has the filtering option already included.

4.3.2 ISO/IEC 27002 is the basis for IEC 63096 security controls

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

One of the objectives for developing the IEC 63096 was to make it a self-standing standard that can be used without having to look in parallel into IEC/ISO 27002:2013.

Description of modifications and extensions of ISO/IEC 27002:2013 controls is given in 4.3.3.

Every ISO/IEC 27002:2013 modification or extension is marked by *italics*. 4.3.3 describes how an ISO/IEC 27002:2013 security control applies to IEC 63096.

The ISO/IEC 27002:2013 'should' statements remain unchanged. Whether a security control is highly recommended or optional is defined in each implementation guidance table (see 4.3.4) and supersedes the ISO/IEC 27002:2013 "should" statements.

All ISO/IEC 27002:2013 instances of the term "information security" have been substituted by the term "cybersecurity".

4.3.3 Modification/ extension of the ISO/IEC 27002:2013 security control description

For each security control four cases with respect to ISO/IEC 27002:2013 are possible:

- Security control from ISO/IEC 27002:2013 applies to IEC 63096 without modification;
- ISO/IEC 27002:2013 security control is modified or extended to better meet the specific requirements from the nuclear I&C programmable digital system domain. Modifications are in *italics*;
- A new security control is added. This is the case where ISO/IEC 27002:2013 does not describe needed nuclear I&C programmable digital system specific security controls. New security controls are marked by the abbreviation "NUC" (Nuclear), in the respective heading. The abbreviation is inserted between the heading number and the heading text. The new control clause including its heading is in *italics*.
- ISO/IEC 27002:2013 clauses that do not apply can be recognized in Annex A by the status "u" (unconsidered).

If the ISO/IEC 27002:2013 implementation guidance is extended by additional nuclear I&C programmable digital system specific line items these are marked by capital letters starting from A in parenthesis (e.g. (A)).

If an ISO/ IEC 27002:2013 implementation guidance line item was not marked by a lower letter, capital letters starting from A in parenthesis (e.g. (A)) , all in *italics*, are added, in order to create a reference for this line item.

Clause 19 and Clause 20 have been added.

To find out what ISO/ IEC 27002:2013 clauses have been modified or extended or what additional security controls have been added, see the column "ISO/IEC 27002:2013" of Table A.1 in Annex A.

4.3.4 Structure of each security control description

Each security control description is structured as follows:

a) Control

This item contains a short description of the specific security control.

b) Preservation of:

Description of the objective of the security control in terms of Confidentiality, Integrity and Availability (CIA):

- C → Confidentiality
- I → Integrity
- A → Availability

c) Control focus:

This item describes the security control in terms of prevention, detection and correction. To avoid confusion with the letters C, I and A from the item “Preservation of:” lower case letters have been selected for the security control focus:

- p → Prevention
- d → Detection
- c → Correction

NOTE Regarding the term “correction”, this document follows the ISO/IEC 27000 series terminology. In this context IAEA uses the term “response”, which is considered synonym.

Examples for the three control focuses are:

- Prevention
 - Security awareness training
 - Data diode
- Detection
 - Security Incident Event Monitoring (SIEM) system
 - Intrusion Detection System
- Correction
 - Operating system security updates
 - Restoration of backup data

d) Implementation guidance

The implementation guidance depends on the security degree (as defined in IEC 62645) that is assigned to the individual I&C system.

If no security degree is assigned to an individual I&C system, the implementation guidance of the security baseline “Baseline Requirement” applies.

For the security baseline and the security degrees following column headings are defined:

- BR → Baseline requirement
- S3 → Security degree 3
- S2 → Security degree 2
- S1 → Security degree 1

The applicability of the implementation guidance is defined in the respective columns BR, S3, S2 or S1.

The applicability of the implementation guidance depends on one or several of the following activities, shown by the following letters (D, E, O) in columns BR, S3, S2, S1. For a better granularity of the applicability of a security control additional specific subscripts for selected sub-activities are added:

- D → I&C Platform Development
- E → Project Engineering for plant specific I&C system
 - E_b → Project Engineering before “Installation” and “Commissioning”
 - E_d → Sub- activities “Requirements”, “Specifications” and “Detailed design and implementation”
 - E_g → Sub- activity “Integratgation (offsite integration)”
 - E_v → Sub- activity “Validation (factory acceptance testing)”
 - E_s → Sub- activity “Shipping to site”
 - E_{ic} Project Engineering activities “Installation” and “Commissioning”
 - E_i → Sub- activity “Installation (onsite Integration and Acceptance testing)”

- $E_c \rightarrow$ Sub- activity “Commissioning (Commissioning and Acceptance Testing)”
- $O \rightarrow$ Operation and Maintenance of I&C system
 - $O_o \rightarrow$ Sub- activity “Operation”
 - $O_m \rightarrow$ Sub- activity “Maintenance”
 - $O_r \rightarrow$ Sub- activity “Retirement”

The above-mentioned sub-activities are consistent with IEC 62645.

The project specifically chosen life cycle model may vary from the standard model in IEC 62645 (e.g. to combine more than one life-cycle activity in a mutual step) but generally will enclose all the sub-activities mentioned above. Therefore, the introduced set of subscripts will match also in such specific cases.

Examples:

- E_{ic} : Comprises Engineering sub- activities “Installation” and “Commissioning”
- E_{gy} : Comprises Engineering sub- activities “Integration (offsite integration)” and “Validation (factory acceptance testing)”
- E_s : Comprises Engineering sub- activity “Shipping to site” only
- E_b : Comprises all Engineering sub- activities except “Installation” and “Commissioning”

If no subscript is added, the security control is applicable to all sub-activities of the respective activity (D, E, O).

In this context, see 4.1.

Depending on the security control it is possible that the implementation guidance table is specifically available for each or a combination of activities (D, E or O).

For each security degree it is identified, whether the specific security control is highly recommended, optional, not permitted or not applicable. This is depicted by the following nomenclature:

- Activity letter (D, E, O) without parenthesis, e. g. “D”:
The specific security control is highly recommended and shall be implemented.
- Activity letter (D, E, O) in parenthesis, e. g. “(D)”:
The specific security control is optional.
- “Not permitted”:
The specific security control is not permitted.
- “N./A.”:
The specific security control does not necessarily increase cybersecurity in the frame of nuclear I&C programmable digital system considering the effort and is therefore not applicable.

Examples:

- (DE)O: The respective security control is optional for activities D and E, but is highly recommended for activity O.
- (EO): The respective security control is optional for activities E and O, and not applicable to activity D.
- EO: The respective security control is highly recommended for activities E and O, and not applicable to activity D.
- $E_{ic}O$: The respective security control is highly recommended for activities E_i , E_c and O, and not applicable to activity D.

Security controls for the actual I&C platform and I&C system:

These are security controls that are required to be part of the applied I&C platform or the designed I&C system (i.e. integrated) and therefore demand additional attention. Such controls can be specific technical controls that are either a property of the I&C platform (e.g.

whitelisting) or can be project specifically engineered for the I&C system (e.g. integration of a data diode). This type of controls also includes physical security controls (e.g. locks for I&C cabinets and locating I&C cabinets in dedicated locked rooms) that are necessary due to physical protection requirements or regulations (i.e. protection against sabotage, insider threat mitigation).

All controls meeting these criteria are marked by a gray shading in the security control description columns BR, S3, S2 and S1. Additionally, the activity letters (D, E, O) are underlined (dual way of coding for better recognition by the reader).

Information on tools for implementing the specific security control is included in the line item “Tools:” immediately following the standard implementation guidance.

NOTE Tools for configuration or maintaining the associated I&C are considered an asset.

In some cases, a compensatory security control for legacy I&C systems is included in the line item “Legacy:” immediately following the tool specific implementation guidance. This compensatory control can be applied if the actual security control cannot be implemented due to technical limitations of the legacy system.

e) References

If the implementation guidance takes guidance from or provides related guidance to other standards than ISO/IEC 27002:2013, the respective standards are referenced there. If no guidance is taken from another standard or no related guidance to other standards is given, the References heading is not included.

4.4 Process of selecting security controls

4.4.1 General

The process of selecting security controls distinguishes between two main areas:

- Security controls for the actual I&C platform and I&C system
- Security controls for the environments for the DEO- activities

The “security controls for the environments for the DEO- activities” are sub divided into:

- D → I&C Platform Development (project independent I&C platform development)
- E → Project Engineering for plant specific I&C system (System level development)
- O → Operation and Maintenance of I&C system (System level)

The split into “security controls for the actual I&C platform and I&C system” and the “security controls for the environments for the DEO- activities” within IEC 63096 and how IEC 63096 connects with the other SC 45A cybersecurity standards, IEC 62645 and 62859, is illustrated in Figure 2:

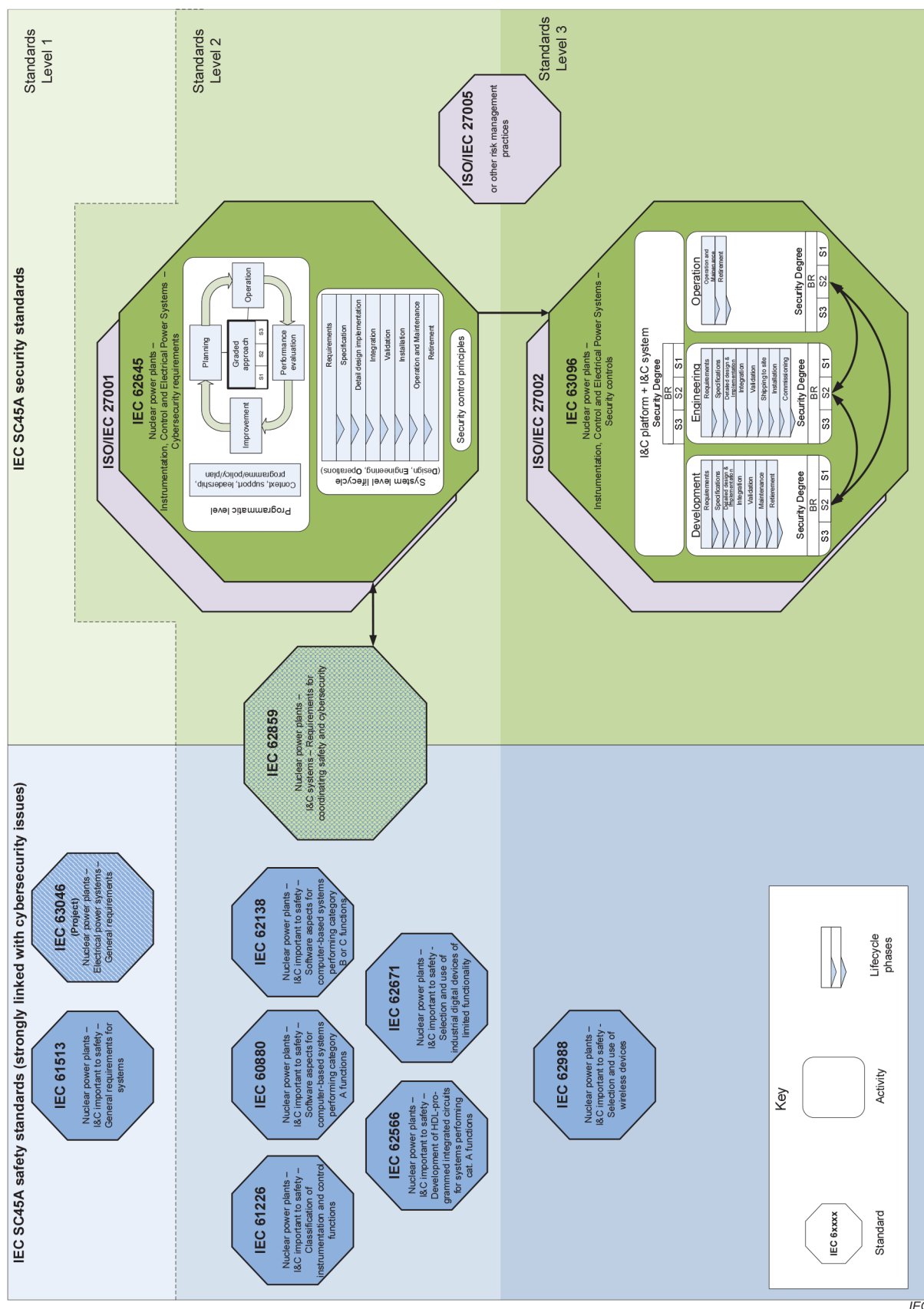


Figure 2 – Overview

The following subclauses provide details on the process of selecting and implementing “security controls for the I&C platform and I&C system” and for the “environments for the DEO activities”

4.4.2 Process of selecting and implementing security controls for the actual I&C platform and I&C system

4.4.2.1 General

Figure 3 gives a high-level overview on the process of selecting and implementing security controls for the actual I&C platform and I&C system for nuclear power plants. It also shows where the IEC 63096 connects with the other SC 45A cybersecurity standards, IEC 62645 and 62859.

Before starting with the main process steps as described below, according to IEC 62645 an initial Threat and Risk Assessment for the I&C system for intended environment in the plant shall be done before selecting security controls.

The main process steps are (see yellow numbered circles in Figure 3):

- 1) I&C system security degree assignment according to IEC 62645.
- 2) Selection of the “security controls for the actual I&C platform and I&C system” from the IEC 63096 security controls catalogue.
- 3) Definition of the final “Security defence-in-depth I&C architecture” and security controls implementation that results in the “Hardened I&C Systems”.
- 4) Update of the Threat and Risk Assessment for each individual I&C system for detection and mitigation of potential remaining security risks. This includes the definition and implementation of additionally needed suitable security controls for mitigating newly surfaced unacceptable cybersecurity risks.

Due to potential additional or modified I&C system assets and the continuously changing threat landscape:

- 5) Periodical reassessment and additionally event driven reassessment of the Threat and Risk Assessment, in case new threats, new vulnerabilities are identified, or new assets are added.

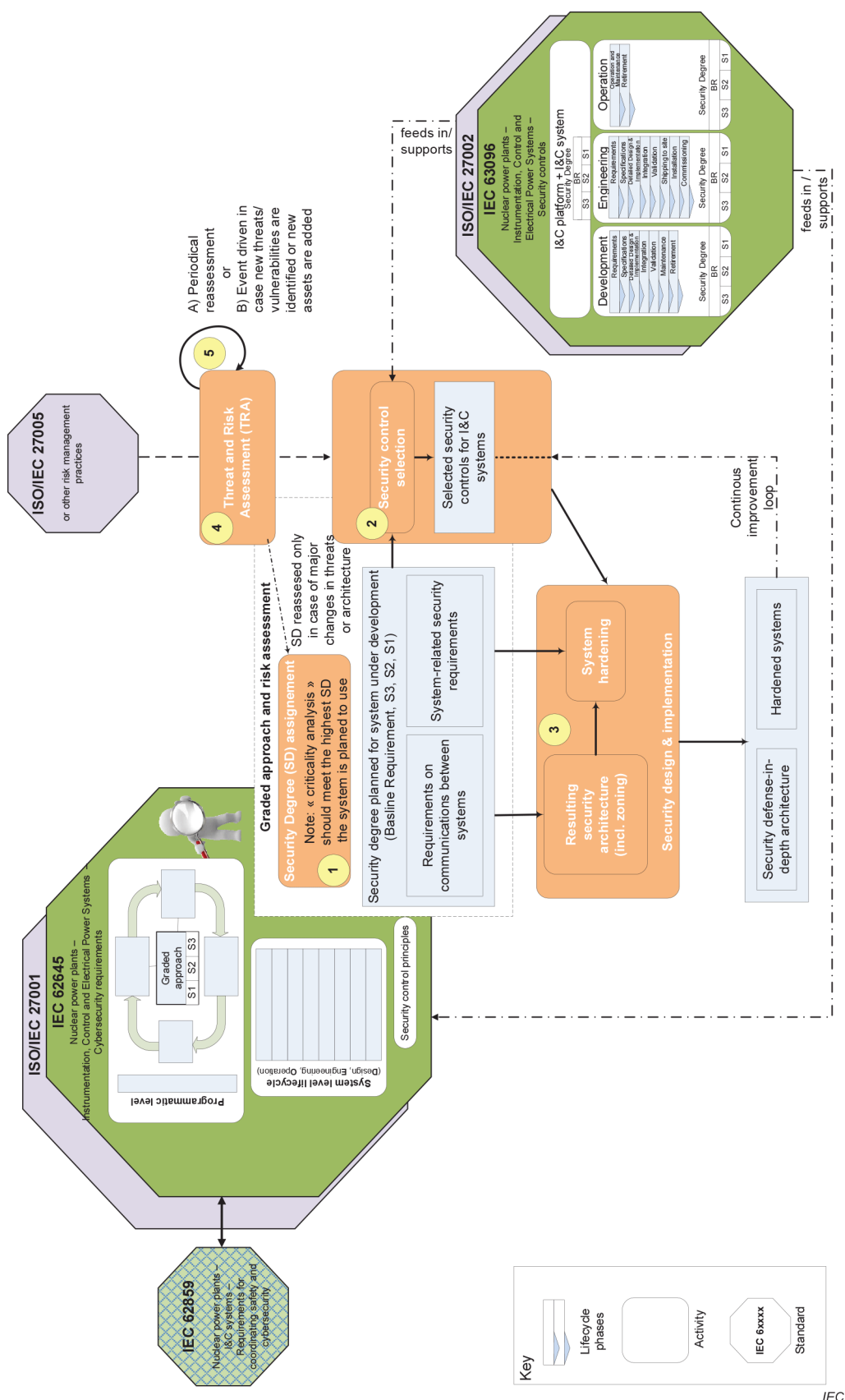


Figure 3 – Process of selecting and implementing security controls for the actual I&C platform and I&C system

The following clauses provide more details on the process of selecting and implementing security controls for the actual I&C platform and I&C system. This guidance is consistent with IEC 62645.

NOTE IEC 63096 already considers the structuring of ISO/IEC 27002 and the recommendations of ISO/IEC 27005. Additionally, the guidance on the validation of security controls according to ISO/IEC 27034-4 could be considered.

4.4.2.2 Security degree assignment (Step 1)

As described in IEC 62645 a specific security degree shall be assigned to each individual I&C system.

In case of major changes in threats, vulnerabilities or architecture, the security degree assignment should be reassessed, which contributes to the continuous improvement process.

The process of assigning security degrees is defined in IEC 62645.

4.4.2.3 Selection of the “security controls for the actual I&C platform and I&C system” from the IEC 63096 security controls catalogue (Step 2)

According to the required security degree of the “actual I&C platform and the I&C system”, all applicable “security controls for the actual I&C platform and I&C system” from the security controls catalogue (see Clause 5 to Clause 20), which are labelled highly recommended, shall be implemented for the “actual I&C platform and I&C system”.

The applicable security controls for the respective security degree are marked in the security controls catalogue by a gray shading in the security control description, columns BR, S3, S2 and S1, and by underlined activity letters (DEO) in the respective security degree column.

Whether the “security controls for the actual I&C platform and I&C system” are implemented in the I&C platform by the I&C platform development or during engineering is not substantial. Substantial is that the respective security controls get implemented in the final I&C system (technical controls) and will be provided for the final I&C system in the plant (physical controls).

A variety of technical security controls provided by the I&C platform require configuration during the engineering activity. Depending on the character of the technical security control, some technical security controls can be completely implemented during the I&C system engineering without an I&C platform development activity.

It is implicitly assumed that the “security controls for the actual I&C platform and I&C system” will be properly taken care of during the D and or E- activity. As a result, technical controls for the I&C platform and I&C system typically show the E_{gvsic} and the O- activity in order to express that the technical security control needs to be activated/ configured/ engineered during the I&C system “offsite integration” and to be in place before the beginning of and during the I&C system “factory acceptance testing” and also needs to stay in place for “Installation”, “Commissioning” and “Operation and Maintenance”.

Remarks on the I&C platform:

- If due to technical reasons security controls cannot be delivered as intrinsic part of the I&C platform (e. g. disabling of hardware interfaces of a computer) and can only be activated/ configured by the I&C system administrator during the E- activity, these security controls shall be described in the I&C platform security hand book and shall also be subject to I&C platform testing and release.
- Security controls that are needed for the I&C system border protection in the frame of the security zoning (see IEC 62645) should be part of the I&C platform. If this is not the case the I&C platform shall allow the integration of the border protections during the E- activity.

Remark regarding safety and security:

- The security controls including border protections selected above, shall not negatively impact the safety properties of the I&C platform or the I&C system (see IEC 62859). If a security control cannot be implemented, since it negatively impacts I&C platform and I&C system safety properties, a justification shall be provided, and a compensatory security control shall be implemented (see 4.4.6.1).

4.4.2.4 Security design & implementation (Step 3)

For requirements on performing the process steps (summarized in Figure 2 by the activity “Security design & Implementation”) consisting of the phases:

- Requirements,
- Specifications,
- Detailed design and implementation,
- Integration (offsite integration),
- Validation (factory acceptance testing),
- Shipping to site,

that result in the “Security defence-in-depth I&C Architecture” and the “Hardened I&C systems”, refer to IEC 62645.

Part of the “Security design & implementation” is also the implementation of security controls (hardening).

4.4.2.5 Threat and Risk assessment for the I&C system for intended environment in the plant (Step 4)

Based on the secured I&C system architecture the threat and risk assessment shall be performed for the intended environment in the plant for each hardened individual I&C System and its sub-systems or components (assets) and shall be based on the assumption that the security controls selected for the respective individual I&C system and its sub-systems or components are already in place for the intended environment in the plant.

It is important to point out that the implementation of security controls that are credited during the threat and risk assessment shall be ensured by taking appropriate quality assurance measures.

If the threat and risk assessment surfaces unacceptable risks, additional security controls shall be defined in order to reduce the risk to an acceptable level. The source for additional security controls can be, among others, not yet selected controls out of the controls catalogue or controls that can be inherited (see 4.4.6.3).

The criteria for deciding whether a cybersecurity risk is acceptable is to be defined specifically based on requirements from the respective authority.

One possible practice for threat and risk management is standardised in ISO/IEC 27005.

4.4.2.6 Periodical or event driven threat and risk assessment for the I&C system for intended environment in the plant (Step 5)

As per IEC 62645 it is recommended to regularly update the threat and risk assessment for the I&C system for the intended environment in the plant, especially in case new/modified assets or new regulations are to be met and also to reflect the fact that the cybersecurity threat landscape continuously changes and new vulnerabilities will occur.

An event driven reassessment of the Threat and Risk Assessment is necessary, in case new threats, new vulnerabilities are identified or new assets are added.

As a consequence, for newly surfaced unacceptable cybersecurity risks, new risk mitigations and security controls respectively shall be defined and implemented into the “Security defence-in-depth I&C Architecture” and the “Hardened I&C systems”.

4.4.3 Process of selecting and implementing security controls for D- activity → I&C Platform Development

As described in 4.4.2.3 it is implicitly assumed that “security controls for the actual I&C platform” that are to be implemented for the I&C platform will be properly taken care off during the D activity.

Therefore, the D-applicability in the security controls catalogue (see Clause 5 to Clause 20) mainly focuses on the I&C platform development environment. This includes but is not limited to organisation, personnel, physical space, processes, assets, IT infrastructure or development tools.

According to the required security degree, the I&C platform shall be used for all security controls from the security controls catalogue (see Clause 5 to Clause 20), which are labelled highly recommended for the D- activity for the respective security degree, and shall be implemented for the I&C platform development environment.

The applicable security controls for the respective security degree are marked by the letter “D” in the columns BR, S3, S2 and S1 in the security controls catalogue.

4.4.4 Process of selecting and implementing security controls for E- activity → I&C system engineering

4.4.4.1 General

As described in 4.4.2.3 it is implicitly assumed that “security controls for the actual I&C system” that are to be implemented for the I&C system will be properly taken care off during the E activity.

Therefore, the E-applicability in the security controls catalogue (see Clause 5 to Clause 20) mainly focuses on the I&C system engineering environment. This includes but is not limited to organisation, personnel, physical space, processes, assets, IT infrastructure or engineering tools.

According to the required security degree, the I&C system shall be used for all security controls from the security controls catalogue (see Clause 5 to Clause 20), which are labelled highly recommended for the E- activity for the respective security degree, and shall be implemented for the I&C system development environment.

The applicable security controls for the respective security degree are marked by the letter “E” in the columns BR, S3, S2 and S1 in the security controls catalogue.

4.4.4.2 Technical, physical and administrative controls that are expected to be in place for the I&C system for the intended environment in the plant

Physical and administrative controls that are expected to be in place for the I&C system for the intended environment in the plant shall be defined and described during the I&C system engineering. The description of these controls shall be handed over to the parties responsible for “Installation”, “Commissioning and “Operation and Maintenance” (E_{IC} and O- activity). A written acknowledgement of receipt shall be ensured.

In addition to that the parties responsible for the E_{ic} and O- activity shall be informed in a documented way that the technical security controls that come with the delivered I&C system shall be maintained during the E_{ic} - and O- activity. A written acknowledgement of receipt shall be ensured.

4.4.4.3 Risk mitigation for the I&C system “Integration or Validation” phase (E_{gv} - activity) – test bed environment

For the phase I&C system “Integration or Validation” (E_{gv} - activity) it is recommended to perform a specific threat and risk assessment under the assumption that the respective security controls from the security controls catalogue are implemented, while additionally analyzing the specific risks because this activity is typically performed in a test bed environment.

If the threat and risk assessment surfaces unacceptable risks, additional security controls shall be defined to reduce the risk to an acceptable level. The source for additional security controls can be, among others, not yet selected controls out of the controls catalogue or controls that can be inherited (see 4.4.6.3).

If the I&C system “Integration or Validation” (E_{gv} - activity) is performed by a different party, security controls that are expected to be in place during I&C system “Integration or Validation” shall be handed over to the party, responsible for I&C system “Integration or Validation”, for implementation in a documented way. A written acknowledgement of receipt shall be ensured.

4.4.4.4 Risk mitigation for the I&C system “Installation or Commissioning” phase (E_{ic} - activity)

For the phase I&C system “Installation or Commissioning” (E_{ic} - activity) it is recommended to perform a specific threat and risk assessment under the assumption that the respective security controls from the security controls catalogue are implemented, while additionally analyzing the specific risks of this activity.

If the threat and risk assessment surfaces unacceptable risks, additional security controls shall be defined to reduce the risk to an acceptable level. The source for additional security controls can be, among others, not yet selected controls out of the controls catalogue or controls that can be inherited (see 4.4.6.3).

It is recognized that during the phases “Installation or Commissioning” (E_{ic} - activity), it is challenging to have all I&C system related security controls already in place. If needed security controls are not yet in place during installation and commissioning, compensatory security controls shall be defined to reduce the risk to an acceptable level.

If the I&C system “Installation or Commissioning” (E_{ic} - activity) is performed by a different party, security controls that are expected to be in place during I&C system “Installation or Commissioning” shall be handed over to the party, responsible for I&C system “Installation or Commissioning”, for implementation in a documented way. A written acknowledgement of receipt shall be ensured.

4.4.4.5 Event driven threat and risk assessment for the I&C system for intended environment in the plant

If new cybersecurity threats are discovered during the I&C system engineering phase, the threat and risk analysis for the I&C system for the intended environment in the plant should be updated. If the threat and risk assessment for the I&C system surfaces new unacceptable risks, additional security controls shall be defined and implemented in order to reduce the risk to an acceptable level.

4.4.5 Process of selecting and implementing security controls for O- activity → Operation and Maintenance of I&C system

4.4.5.1 General

The O-applicability in the security controls catalogue (see Clause 5 to Clause 20) mainly focuses on the I&C system “operation and maintenance” environment. This includes but is not limited to organisation, personnel, physical space, processes, assets, IT infrastructure or engineering tools.

According to the required security degree, the I&C system shall be used for all security controls from the security controls catalogue (see Clause 5 to Clause 20), which are labelled highly recommended for the O- activity for the respective security degree, and shall be implemented for the I&C system operation and maintenance environment.

The applicable security controls for the respective security degree are marked by the letter “O” in the columns BR, S3, S2 and S1 in the security controls catalogue.

In addition to that, the topics described in the following clauses are also essential.

4.4.5.2 Technical, physical and administrative controls that are expected to be in place for the I&C system for the intended environment in the plant

Physical and administrative controls that are required and documented by the party responsible for the E_b- engineering sub-activity to be in place for the I&C system for the intended environment in the plant for the activities “installation and commissioning” and “operation and maintenance” shall be implemented and maintained in the plant.

In addition to that the technical security controls that come with the delivered I&C system for the intended environment in the plant and are described by the party for the E_b- activity shall also be maintained.

4.4.5.3 Regular validation that technical and physical security controls for the I&C system are still in place

For the “installation”, “commissioning” and “operation and maintenance” a process shall be put in place to ensure a regular validation that the technical and physical security controls for the I&C system for the intended environment in the plant are still in place.

4.4.5.4 Periodical or event driven threat and risk assessment for the I&C system for intended environment in the plant

As per IEC 62645 it is recommended to regularly update the I&C system threat and risk assessment for the I&C system for the intended environment in the plant, especially in case new/modified assets or new regulations are to be met and also to reflect the fact that the cybersecurity threat landscape continuously changes and new vulnerabilities will occur.

An event driven reassessment of the Threat and Risk Assessment is necessary, in case new threats or new vulnerabilities are identified or new assets are added.

Consequently, for newly surfaced unacceptable cybersecurity risks, new risk mitigations and security controls respectively shall be defined and implemented into the “Security defence-in-depth I&C Architecture” and the “Hardened I&C systems”.

4.4.6 Additional process requirements valid for controls for the “actual I&C platform and I&C system” and for the D-, E- and O- activity

4.4.6.1 Handling of highly recommended security controls that cannot be implemented or are not needed

Justification shall be provided if a specific highly recommended security control cannot be implemented due to technical or other reasons or if it contradicts safety requirements.

In this case a compensatory security control shall be defined as a substitute for the security control that cannot be implemented. Formal justification of the effectiveness of the compensatory security control shall be demonstrated by the threat and risk analysis.

If no compensatory control can be identified, the reason shall be documented and approved. For higher security degrees (S1 and S2) the approval shall be based on the related requirements of IEC 62645 and IEC 62859.

The objective of compensatory security controls is always to reduce the cybersecurity risk level to the level the original recommended security control would support.

In case the result of the project specific threat and risk analysis demonstrates that a highly recommended security control is not needed for achieving an acceptable risk level, the result of the threat and risk analysis also qualifies as justification.

NOTE See also 4.5.1 on the Statement of Applicability.

4.4.6.2 Handling of optional security controls

Optional security controls should be considered for implementation. If an optional security control is not implemented, no rationale or justification is needed.

Optional controls are also preferred candidates for compensatory controls.

4.4.6.3 Inheritance of already existing security controls

Already existing security controls can be inherited. That means that already existing measures can serve as compensatory security controls, in case a specific security control out of this document (IEC 63096) cannot be implemented.

For compensatory security controls credit can also be taken from safety provisions implemented for I&C systems important for safety (e. g. airlocks or physical segregation). Formal justification of the effectiveness of the inherited or credited security control shall be demonstrated by the threat and risk analysis.

4.4.6.4 Legacy

It is recognized that it might be difficult or even not feasible to implement a specific security control for legacy nuclear I&C programmable digital system components.

In this case compensatory security controls should be defined. For some security controls this document already suggests compensatory security controls from a legacy perspective.

Formal justification of the effectiveness of the compensatory security control shall be demonstrated by the threat and risk analysis.

4.5 Documentation and traceability of security controls

4.5.1 Documentation of security controls selection (statement of applicability)

Each security control selection (highly recommended and optional ones) shall be documented.

If a highly recommended security control is deselected for whatever reason, appropriate justification shall be given and documented.

If feasible, compensatory measures shall be defined and documented as well. Justification of the effectiveness of the compensatory security control shall be demonstrated by the threat and risk analysis.

NOTE If a contradiction between security requirements and safety requirements is the reason for deselection 4.4.5.1 applies.

Table A.1 can be used as a basis for developing the project specific “Statement of Applicability”, where all selected security controls as well as the justifications for non-selected highly recommended controls and the associated compensatory controls (if a compensatory control is feasible) are documented. Annex C provides an informative example.

4.5.2 Traceability

The traceability of the implementation of the selected security controls and the compensatory security controls shall be ensured (e.g. by a traceability matrix).

The traceability shall comprise the following activities.

- I&C Platform Development (D)
- Project Engineering for I&C system (E)
- Operation and Maintenance of I&C system (O)

In addition to that it needs to be checked whether the respective security controls are still in place

- after completion of the Integration (offsite integration),
- after completion of the Installation (Onsite Integration and Acceptance Testing),
- after completion of the Cold Commissioning,
- after completion of the Hot Commissioning and Acceptance Testing and
- during Operation and Maintenance of the I&C system (regular checking needed).

NOTE Since the time distance between Cold Commissioning and Hot Commissioning is very short for modernization projects, the check on whether the respective security controls are still in place after the Cold Commissioning can be skipped.

The traceability should be maintained whenever changes to the selection of security controls are made or I&C system assets have been added or removed.

5 Cybersecurity policies

Clause 5 of this document contains extracts and modifications from ISO/IEC 27002:2013, Clause 5, as described in 4.3.2.

5.1 Management direction for *cybersecurity*

Objective:

To provide management direction and support for *cybersecurity* in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for *cybersecurity*

Control

A set of policies for *cybersecurity* should be defined, approved by management, published and communicated to employees and relevant external parties.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) At the highest level, organizations should define an “<i>cybersecurity</i> policy” which is approved by management and which sets out the organization’s approach to managing its <i>cybersecurity</i> objectives. <i>Cybersecurity</i> policies should address requirements created by: • business strategy; • regulations, legislation and contracts; • the current and projected <i>cybersecurity</i> threat environment. The <i>cybersecurity</i> policy should contain statements concerning: • definition of <i>cybersecurity</i>, objectives and principles to guide all activities relating to <i>cybersecurity</i>; • assignment of general and specific responsibilities for <i>cybersecurity</i> management to defined roles; • processes for handling deviations and exceptions. At a lower level, the <i>cybersecurity</i> policy should be supported by topic-specific policies, which further mandate the implementation of <i>cybersecurity</i> controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics. <i>Such policy should include different topics during different phases and are detailed in (B) through (D):</i>	DEO	DEO	DEO	DEO
<i>Tools: Not identified</i>				
<i>Legacy: Not identified</i>				

Implementation	BR	S3	S2	S1
(B) The set of policies for cybersecurity during development, should contain at least: • physical access control for the development area • access control for development systems • regulations on cybersecurity • guidelines for secure programming inclusive version control • regulations on cybersecurity for 3rd party components • requirements for tests specifically on security controls that are provided by the I&C platform • backup and restore • restrictions on software installations and use • protection from malware • management of technical vulnerabilities in the development area • management of technical vulnerabilities for the I&C platform • penetration testing on the I&C platform (to verify the effectiveness of technical controls and to uncover vulnerabilities that are not yet mitigated) • fuzz testing on the I&C platform (to analyse the robustness of the I&C platform against invalid input data) • Analysis of the I&C platform penetration testing results and definition of new security controls that are needed based on the cybersecurity risk present in the intended I&C platform environment All the policies should be put in force by the top-level management.	(D)	D	D	D
Tools: Not identified				
Legacy: Not identified				
(C) The set of policies for cybersecurity during engineering, should contain at least: • physical access control for all sites with equipment used by engineering • access control for all systems used by engineering • regulations for passwords and credentials • regulations on cybersecurity • regulations for documentation of the engineering process • requirements for tests • backup and restore • regulations on data transfer from and to 3rd parties • management of technical vulnerabilities • penetration testing on the I&C platform (in order to verify the effectiveness of technical controls and to uncover vulnerabilities that are not yet mitigated) All the policies should be put in force by the top-level management.	E	E	E	E
Tools: Not identified				
Legacy: Not identified				

Implementation	BR	S3	S2	S1
(D) The set of policies for cybersecurity during operation, should contain at least: • physical access control • access control for all systems • regulations for passwords and credentials • regulations on cybersecurity • regulations for documentation, backup and restore, periodic test on implemented security controls • requirements for remote access • requirements for retirements of persons and systems (remove access, data, etc.) • regulations on data transfer from and to 3rd parties • management of technical vulnerabilities on the engineering platform • management of technical vulnerabilities on the I&C platform if already being integrated for factory acceptance testing • penetration testing on the I&C platform during maintenance periods (in order to verify the effectiveness of technical controls and to uncover vulnerabilities' that are not yet mitigated) All the policies should be put in force by the top-level management.	$E_{ic}O$	$E_{ic}O$	$E_{ic}O$	$E_{ic}O$
Tools: Not identified				
Legacy: The policies should also include requirements for legacy system still in operation				

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of a “cybersecurity awareness, education and training programme” (see 7.2.2).

Other information

If any of the *cybersecurity* policies are distributed outside the organization, care should be taken not to disclose confidential information.

5.1.2 Review of the policies for cybersecurity

Control

The policies for *cybersecurity* should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	c
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) According to 5.1.1 each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. <i>Each owner of a policy should review and evaluate the policy on a regular basis or on specific changes or cybersecurity incidents.</i> The review should include assessing opportunities for improvement of the organization's policies and approach to managing <i>cybersecurity</i> in response to changes to the organizational environment, business circumstances, legal conditions or technical environment. The review of policies for <i>cybersecurity</i> should take the results of management reviews into account. Management approval for a revised policy should be obtained	DEO	DEO	DEO	DEO
<i>Tools: The review should be included in the IMS (integrated management system) or/and security programme tool of the company.</i>				
<i>Legacy: Policies for legacy systems still in use should also be reviewed and adapted to the specific topics regarding legacy.</i>				

6 Organization of cybersecurity

Clause 6 of this document contains extracts and modifications from ISO/IEC 27002:2013, Clause 6, as described in 4.3.2.

6.1 Internal organization

Objective:

To establish a management framework to initiate and control the implementation and operation of *cybersecurity* within the organization.

6.1.1 Cybersecurity roles and responsibilities

Control

All *cybersecurity* responsibilities should be defined and allocated.

6.1.1.1 a) The assets and *cybersecurity* processes should be identified and defined;

Control

Allocation of the *cybersecurity* responsibilities should be done in accordance with *cybersecurity* policies.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) Responsibilities for the protection of individual assets and for carrying out specific cybersecurity processes should be identified.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(B) Responsibilities for cybersecurity risk assessment management activities and, in particular, for acceptance of residual risks should be defined. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and I&C systems.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(C) An I&C system security programme (often referred to in this document as program) should define the steps and actions to be undertaken in order to define and apply consistent organizational and technical measures and procedures to enforce security objectives, defined in a security policy, explicitly addressed in security plans. This program should be developed based on risk assessment and include the policy and guidance established by the designer, country regulatory authority and existing plant specific policies and procedures to implement the computer security programme.	EO	EO	EO	EO
Tools: Not identified				
Legacy: Not identified				
(D) Computer security programmes should be implemented through the use of documented policies (see 5.1) and procedures approved by the personnel that are in charge of the security programme. A I&C systems security programme for the engineering and operation of an I&C system for a NPP should contain the following activities: • Definition of the computer security organization and responsibilities and the process of periodic reviews; • Development of the process of designating assets subject to computer security protective measures including computer systems, computer system applications and network connections; • Implementation of methods of personnel management in computer security and I&C system security including training, qualification and termination/transfer; • Development and performance of the process for risk assessment, taking into account the country specific design basis threat (DBT) as applicable, for the complete I&C system architecture as well as for every I&C system; • Performance of an assessment of the residual risk that is transferred/accepted from design to operation; • Definition of the fundamental architecture and design principles and requirements for system security design and configuration management for plant systems and vendor support required to maintain the cybersecurity features incorporated in the design; • Identification of operational security procedures for access control, data security, communication security, platform and application security, system monitoring, computer system security maintenance and modification and security incident handling; • In particular, definition of a process for assessment of off-the-shelf components, both hardware and software to ensure as far as reasonably possible that they are free from malicious software or functionality; • Establishment of security requirements for the preparation and formalization of deliveries of hardware, data, software, code or information between different sites of the designers, or between a designer and a third party, or between the designer and the utility.	EO	EO	EO	EO
Tools: Not identified				
Legacy: Not identified				

6.1.1.2 **NUC – Responsible entities and authorization levels for each asset or cybersecurity process should be defined and documented**

Control

Top management should ensure that entities relevant to cybersecurity should be assigned and communicated. Also, their authorization levels should be defined and documented.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) All organizations involved in any phase of the I&C system lifecycle should document the organizational structure and associated responsibilities for each position that support the computer security programme for those systems.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(B) I&C system security oversight should be assigned to a Computer System Security Officer(s) (CSSO), or equivalent.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(C) Security responsibilities should be addressed prior to employment in job descriptions and terms and conditions of employment. Top management should assign the responsibility and authority for: f) Ensuring that the cybersecurity management system conforms to the applicable cybersecurity requirements. g) Reporting on the performance of the cybersecurity management system to top management and within the organization.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(D) Employees, contractors and authorized third parties should sign agreements acknowledging their agreement on security roles and responsibilities, prior to employment.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				

6.1.1.3 **d) To be able to fulfil responsibilities in the cybersecurity area, the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments;**

Control

To be able to fulfil responsibilities in the cybersecurity area, the appointed individuals should be bestowed with the required competences and be able to keep up to date with developments related to their area.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) Ensuring that employees, contractors and authorized third parties understand their responsibilities, are suitable and qualified for the roles they are considered for and/or assigned, and to minimize the risk of theft, fraud, misuse or intentional sabotage of the facility.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(B) The necessary competences of persons doing work affecting cybersecurity performance should be determined.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(C) Actions should be taken to acquire the necessary competences. Checking of the persons doing work affecting cybersecurity performance should be realized on the basis of appropriate education, training or experience.	DEO	DEO	DEO	DEO
The effectiveness of these actions should be evaluated.				
Further details on this control can be provided in Clause 7.				
Tools: Not identified				
Legacy: Not identified				

6.1.1.4 e) Coordination and oversight of cybersecurity aspects of supplier relationships should be identified and documented;

Control

Cybersecurity requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) The organizations should identify and mandate cybersecurity controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement.	DEO	DEO	DEO	DEO
Tools: Not identified				
Legacy: Not identified				
(B) During the design and development phase, different companies are likely to be responsible for working on different I&C systems. The overall I&C system designer should clearly specify the I&C system supplier obligations with respect to computer security, and should verify that they are respected.	E	E	E	E
Further details on this control are provided in Clause 15.				
Tools: Not identified				
Legacy: Not identified				

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organizations assets.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance

Implementation	BR	S3	S2	S1
(A) Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered during the design of the controls. Some small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.	(DEO)	(DEO)	(D)EO	DEO
<i>Tools: Not identified</i>				
<i>Legacy: Not identified</i>				

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

<u>Preservation of:</u>	CIA	<u>Control focus:</u>	p
-------------------------	-----	-----------------------	---

Implementation guidance:

Implementation	BR	S3	S2	S1
(A) Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified cybersecurity incidents should be reported in a timely manner (e.g. if it is suspected that laws have been broken). Organizations <i>that are</i> under <i>cyberattack</i> from the Internet possibly need authorities to take action against the cyberattack source. Maintaining such contacts supports cybersecurity incident management (see Clause 16) or the business continuity and contingency planning process (see Clause 17). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).	(DEO)	DEO	DEO	DEO
<i>Tools: Not identified</i>				
<i>Legacy: Not identified</i>				