IEC TR 63415

Edition 1.0 2023-08

TECHNICAL REPORT

colour inside

Nuclear Power plants – Instrumentation and control systems – Use of formal security models for I&C security architecture design and assessment

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-7340-1

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

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 9
2 Normative references 10
3 Terms and definitions 10
4 Abbreviated terms 12
5 I&C system security life cycle and security modelling activities 13
6 Description of a typical NPP I&C system 15
7 Security requirements and security architecture 16
7.1 General framework 16
7.2 Integrated security model 18
7.3 Basics of the information exchange model (DM) 18
7.4 Basics of the security model (SLM) 18
7.5 Basic principles of the secure design 19
7.6 Asset ranking and ordering 19
7.7 Information property of the asset 19
7.8 Security degrees concept and security architecture 20
7.9 Establishing a relation between the data model and the security model 21
8 Procedure of I&C security modelling 21
8.1 General 21
8.2 General approach to asset classification 24
8.3 Security degree assignment and the analysis of model conformance 24
8.4 Classification in hierarchical systems 24
9 Case study of I&C security architecture synthesis 26
9.1 General 26
9.2 Definition of the security model 26
9.3 Selecting the detail level in system analysis 27
9.4 Asset classification 27
9.5 Identification and initial classification of assets 28
9.6 Data model 28
9.7 Analysis of the model and synthesis of architecture 29
9.8 Assessment of the modified security architecture 33
10 NPP cybersecurity simulation for security assessment of I&C systems 34
11 Conclusion 35
Annex A (informative) Data model 37
Annex B (informative) Security model definition (SLM) 40
Annex C (informative) Justification of the secure by design principle 41
Annex D (informative) Mapping of security and data model 43
Annex E (informative) Formal approach to asset clustering and classification 46
E.1 Input data types and the choice of data representation for the analysis 46
E.2 Order relation on a security graph 46
E.3 Data renormalization 47
E.4 Criteria and clustering method 47
Annex F (informative) Some algorithmic aspects for security architecture synthesis 49
Annex G (informative) Asset classification using clustering method: an example 50

Annex H (informative) Mathematical notations in the integrated security mode 53
H.1 Integrated cybersecurity model, ICM 53
H.2 Model of information exchange, DM 53
H.3 Allowed transformation of a security graph 53
H.4 Relationship of secure information transfer between two assets 53
H.5 Relationship of simple information transfer between two assets 53
H.6 Asymmetric operations between two assets 53
H.7 Access rules model 53
H.8 Relationship of simple information transfer between security degrees 54
H.9 Relationship of secure information transfer between security degrees 54
H.10 Operator R of mapping between two models 54
Bibliography 55

Figure 1 – Structure of a typical I&C system 16
Figure 2 – Procedure of security architecture synthesis 23
Figure 3 – I&C information model with subsystem hierarchy (left) and without it (right) 25
Figure 4 – Simplified information model of security. (secure relation between degrees are shown by dashed lines) 27
Figure 5 – General security graph for I&C subsystem without taking into account security controls. The borders show boundaries for workstation server and gate subsystem. 29
Figure 6 – Changes in the security graph for I&C subsystem when OS_WS asset is targeting allocation to a separate zone. The edges belonging to the minimal cut are shown with bold lines. 30
Figure 7 – General view of the security graph for I&C subsystem, taking into account security controls for OS assets. The security degree structure is shown in a) and the zone structure is shown in b). Degrees and zones are shown in a solid rectangle. The degree is numbered. 31
Figure 8 – Changes in the security graph for I&C subsystem when server assets are targeting allocation to a separate zone from the workstation. The edges belonging to minimal cut are highlighted with bold line. 32
Figure 9 – General representation of the security graph for practical I&C subsystem, taking into account all assigned security controls for the assets. The security degree structure is shown in a) and zone structure is shown in b). The degrees and zones are shown in solid rectangle. The degrees are numbered 33
Figure 10 – General scenario of use of the digital twin for stress tests 35
Red and orange arrows mean secure information transfer, black arrows mean “common” information transfer. 43
Figure D.1 – Sketch of link transformation 43
Figure D.2 – Example of domains of connectivity in a graph – Here the graph splits into three domains 44
Figure G.1 – Security graph of the system in the information exchange model 50
Figure G.2 – Transitive closure of the security graph by the relation w 51
Figure G.3 – Asset partitioning by security degrees 51

Table 1 – I&C life cycle stages and corresponding scenarios for the use of security modelling 13
Table 2 – List of assets of a typical control system channel and IS target characteristics 28

Table 3 – Information security characteristics for assets in the architecture of a I&C subsystem 34
Table A.1 – Correspondence of the physical properties of I&C systems with the properties of the security graph 37
Table E.1 – NPP I&C asset properties 46
Table F.1 – Computational methods for analyzing the security graph 49
Table G.1 – Table of attributes 50
Table G.2 – Partition of the assets into security degrees 52

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – USE OF FORMAL SECURITY MODELS FOR I&C SECURITY ARCHITECTURE DESIGN AND ASSESSMENT

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.

IEC TR 63415 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
45A/1465/DTR	45A/1476/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under 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 document 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

Over the last twenty years, Instrumentation and Control (I&C) systems for nuclear facilities and Nuclear Power Plants (NPP) have progressed from using hard-wired, mostly analogue components to the versatile mostly digital systems. This progression to digital systems have enhanced design flexibility, and provides for increased acquisition of system performance data but also introduces susceptibility to cyber-attacks for the system itself and nuclear facility as a whole. The generally recognized solution of the I&C NPP security provision problem is to define security requirements as early as possible during the life cycle of the I&C system. These requirements are mapped into the appropriate system's architecture and security measures (controls) during the design stage. However, in practice, security controls are often introduced only at the final stages of system development. It may lead to a "disagreement" between system architecture and security controls that presumably make the application of implemented measures ineffective.

On a technical view, the problem may be represented as a set of particular issues, such as asset classification, selection, and assignment of security controls providing protective barrier measures against cyber-attacks, arrangement of information links between assets, etc. Current I&C NPPs security development practice addresses these issues. The work [1][1] deals with assets classification issue. The technical level IEC 63096 standard [6] deals with selection of the security controls. However, in general, the cybersecurity provision of the I&C system is still an unresolved issue, especially at the stage of system design and approval of functional requirements and cybersecurity measures. It is intended that this Technical Report is used by operators of NPPs (utilities), systems evaluators and by licensors.

b) Situation of the current Standard in the structure of the IEC SC45A standard series

IEC 63415 is a 4th level IEC/SC45A document covering the use.

For more details on the structure of the IEC SC45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the Standard

To ensure that the document will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

d) Description of the structure of the IEC SC45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The IEC SC 45A standard series comprises a hierarchy of four levels. The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046.

IEC 61513 provides general requirements for instrumentation and control (I&C) systems and equipment that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems.

IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical power systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general requirements for specific topics, such as categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, human factors engineering, 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.

[1] Numbers in square brackets refer to the Bibliography.

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

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

The IEC SC 45A standards series consistently 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, the IAEA safety guide SSG-51 dealing with human factors engineering in the design of NPPs and the implementing guide NSS42-G for computer security at nuclear facilities. The safety and security terminology and definitions used by the SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework, IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 and IEC 63046 refer to ISO 9001 as well as to IAEA GSR 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, IEC 63351 is the entry document for the human factors engineering standards and IEC 62342 is the entry document for the ageing management standards.

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

NOTE 2 IEC TR 64000 provides a more comprehensive description of the overall structure of the IEC SC 45A standards series and of its relationship with other standards bodies and standards.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS – USE OF FORMAL SECURITY MODELS FOR I&C SECURITY ARCHITECTURE DESIGN AND ASSESSMENT

1 Scope

The TR provides an overview over the formalized modelling and designing of cybersecure architectures to apply for I&C system cybersecurity enforcement at NPPs. The plant-specific risk assessment can use the techniques covered by this TR.

The formal security models are often used in the analysis and design of I&C security architectures. A formal security model is a mathematical notation such as algebra and set theory or logical expression that defines the security properties of a system and the relationships between different components. It provides a rigorous way to reason about the security of a system and to identify potential vulnerabilities and threats.

This document considers the complex problem of NPP I&C architecture synthesis to address particular issues:

- asset classification,
- barrier measures assignment,
- the information transfer and links conformity with security requirements.

This document provides guidance on creating a comprehensive security model applicable to NPP I&C systems that describes NPP I&C cybersecurity architecture and aids in accomplishing the main tasks of I&C system secure design, which are:

- specification of system designs with increased determinism that enhance security,
- mapping of the security requirements into the security architecture of the I&C system,
- definition of the security requirements for information exchange between components within the I&C system, operators and other systems,
- assistance in the determination of the security degree assignment with a model-based technique considering asset properties and formal grouping of the assets,
- design and establishment of security zones boundaries.

These tasks are closely related with the I&C NPP security framework established by IEC 62645 [2] and implement the Secure by Design principle (SeBD) [3].

This document presents the following limitations. The presented methods of the security modelling rely on the following properties of the I&C system:

a) The system is built upon the hierarchical principle, the hierarchy exists both at the level of functional system architecture (subsystems, software and hardware components etc.) and at the security architecture level (degrees and zones);

b) The focus is on preserving integrity, which prevails over the principle of maintaining confidentiality.

c) The availability property and any time related behaviour are out of the scope of this document;

d) The notion of a “secure” communication or a “secure” barrier in the document generally does not define the exact mechanism (controls) of how the secure property is achieved. It just assumes that an appropriate set of the security controls is implemented in situ;

e) The approach takes into account the existing nuclear safety classification scheme [7].

In addition to a general consideration of the I&C system security, several assumptions about properties of the I&C system have been made to facilitate the analysis, namely:

- the set of the assets is fixed and stable over a long period of time;
- peer-to-peer relations between assets are fixed and known;
- technological/functional requirements are determined.

The users of the presented methods are supposed to be familiar with basics of graph theory, discretionary access models, and documents listed in Clause 2.

Specific software tools implementing the presented methods eases the requirements to the users' mathematical background.

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

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

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

IEC 63096, *Nuclear power plants – Instrumentation, control and electrical power systems – Security controls*

NTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021)