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

IEC TR 63415:2023-08(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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.

CONTENTS

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)

3 Terms and definitions

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

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

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

3.1
asset
physical or logical object owned by or under custodial duties organization, having either a perceived or actual value for organization

[SOURCE: IEC TS 62443-1-1 2009, 3.2.6]

3.2
I&C system
system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself.

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 1 to entry: See also “I&C function”.

Note 2 to entry: Any network is either a part of an I&C system or an I&C system by itself.

[SOURCE: IEC 61513:2011, 3.29]

3.3
I&C function
function to control, operate and/or monitor a defined part of the process

[SOURCE: IEC 61513:2011, 3.28]

3.4
data model
information exchange model

model that describes access relations between assets in I&C system during their functioning

3.5
digital twin
a digital twin is a formal digital representation of some asset, process or system that captures attributes and behaviours of that entity suitable for communication, storage, interpretation or processing within a certain context

3.6
integrity level
property of the asset which solely depends on the connectivity property

3.7
security architecture
plan and set of principals describing the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the service and the performance level required in the elements to deal with the threat environment

[SOURCE: IEC TS 62443-1-1:2009, 3.2.100]

Note 1 to entry: The security architecture defines the security structure of the I&C system as a system of systems, including the main functions, degrees, zones and boundaries of each system, the interconnection or independence of critical digital assets (CDAs), the priority of the goals of simultaneously operating in the system and the order of interaction between the personal and the machine in the I&C system.

Note 2 to entry: In narrower context the system architecture is a partitioning of the I&C system into a number of interconnected subsystems and components and the arrangement of system subsystems using zone approach to comply with security requirements related to the overall security degree of the system.

3.8
security controls
means of managing security which can be administrative, technical, or management

[SOURCE: IEC 62645:2019, 3.18, modified – “technical, physical, or administrative” replaced by “administrative, technical, or management]

3.9
security degrees
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: We assume that security degrees are ordered. The order from smaller to bigger number corresponds to the sequence from highest security to less strict security.

[SOURCE: IEC 62645:2019, 3.19]

3.10
security measure
abstract barrier that enables secure data transfer between assets

3.11
security policy
set of rules that specify or regulate how a system or an organization provides security services to protect its assets

Note 1 to entry: the term “security policy” used in the content of the document corresponds to “I&C digital programmable system policy” in IEC 62645 context.

Note 2 to entry: I&C programmable digital system security policy should be translated into requirements, which will be used to derive essential properties of the security models.

Note 3 to entry: Requirements may be expressed mathematically or in a natural non-formal language.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.112]

3.12
security model
security requirements model

model that defines collection of classes (degrees of cybersecurity) and relations between them, and rules governing asset attribution to a degree

3.13
security zone

A computer security zone is a logical and/or physical grouping of digital assets that are assigned to the same computer security level and that share common computer security requirements owing to inherent properties of the systems or their connections to other systems (and, if necessary, additional criteria).

[SOURCE: IAEA Nuclear Security Series No. 17-T: 2021, 2.9]

3.14
security architecture synthesis
process of bringing the information exchange model into accordance with the security requirements model

4 Abbreviated terms

CDA Critical Digital Asset
CPS Cyber Physical System
DAC Discretionary Access Control
MAC Mandatory Access Control

DM Data Model
ICM Integrated Cybersecurity Model
I&C Instrumentation and Control
LAN Local Area Network
NPP Nuclear Power Plant
OS Operation System
SeBD Secure by Design
SLM Security Level Model
TR Technical Report
WS Workstation

5 I&C system security life cycle and security modelling activities

The overall life cycle of the I&C programmable digital security system security forms the basis for the understanding how various components of a secure I&C system are related to each other. Development of the I&C system commonly includes the security related activities which are spread on life cycle stages defined by IEC 62645. The security policy ought to cover all life cycle stages. Omission of any stage in the security policy makes it very difficult to achieve cybersecurity in the next stages. Table 1 shows how security modelling is used on each security life cycle stages to strengthen the security of the I&C architecture.

Table 1 – I&C life cycle stages and corresponding scenarios for the use of security modelling

N	Life cycle stage (as per IEC 61513:2011)	Security tasks (as per IEC 62645:2019)	Application of security models
1.	System requirements specification		
2.	NA	Describe system using a top-down approach, considering the global I&C architecture	Top-down structural view of the system architecture. The mathematical models are used to model relations between I&C system components. See 9.6.
3.	NA	Security degree assignment	To facilitate the security degree assignment using mathematical methods. See Annex E.
4.	System specification	System architecture	The system architecture is partitioned into a number of interconnected subsystems and components which are combined to logical zones. That arrangement complies with security degree assigned to subsystems. The mathematical models are used to model relations between I&C subsystem and components. See 9.7.

N	Life cycle stage (as per IEC 61513:2011)	Security tasks (as per IEC 62645:2019)	Application of security models
5.	System detailed design and implementation	The design phase shall incorporate the objectives of the plant design as a whole and on the individual I&C subsystem security degree basis to address security controls over: physical and logical access to the I&C system function, use of the I&C system, and data communication with other I&C systems. The designer makes a complete inventory of all I&C systems and interfaces considering all devices used within the plant, including diagnostic, maintenance or test devices. Risk assessment at the design phase is used to identify and implement countermeasures required to prevent or mitigate the consequences of attacks against plant I&C system.	The security model: elaborates the possible data communication paths develops scenarios for physical and logical access to I&C assets identifies interfaces between I&C system and plant devices generates preliminary attack scenarios used for risk assessment. identifies logical boundaries makes formal assignment of the system and subsystem to physical security zones. See 9.7,9.8
6.	System integration	Integration testing confirms that the integrated security controls perform as required and do not adversely affect the system's ability to perform its required functions.	The effectiveness of the developed security models is verified in accordance with the implemented systems. The models are used to check that normal information paths do not conflict with security barriers. See 9.8
7.	System validation	Testing shall verify the I&C security design of the hardware architecture, external communication devices and configurations for unauthorized pathways and system integrity.	Possible attack scenarios to I&C system assets used for system validation are generated. All parts of Clause 9.
8.	System installation	At the end of the installation, the system shall be tested in the operational environment to verify and validate the correctness of the I&C system security features and the incorporation into the system in accordance with the design.	The effectiveness of the developed security models is verified against the installed systems. The check of installation correctness includes usually a reuse of attack scenarios identified and generated on previous stages. All parts of Clause 9.

N	Life cycle stage (as per IEC 61513:2011)	Security tasks (as per IEC 62645:2019)	Application of security models
9.	Operation and maintenance	During the operation and maintenance phase, the periodic security audits of security features shall be performed. Prior to any system modification or maintenance, the affected components shall be evaluated to confirm that all protective feature and design elements will remain functional.	Generation of new attack scenarios for ongoing risk assessments. The security models developed and verified on the previous life cycle stages is used: To assess the modification effect on security prior to applying them to the I&C system to investigate security incidents or identify vulnerabilities and weakness and recommend corrective actions; All parts of Clause 9.
10.	Retirement activities	NA	Developing the I&C system retirement scenarios. All parts of Clause 9.

6 Description of a typical NPP I&C system

The I&C system is a distributed computerized system, which provides the implementation of basic information management and the NPP control functions as:

- centralized collection and data storage about equipment's state;
- presentation of information about the plant to the operating personnel of the NPP;
- control of the NPP technological equipment.

Interaction between the I&C system and the NPP's equipment is carried out through gateways and controllers connected to the LAN. The structural diagram of a typical I&C system considered in the document is presented in Figure 1.

The components of I&C systems are:

- workstations (WSs);
- servers;
- gateways and controllers or field devices;
- network equipment.

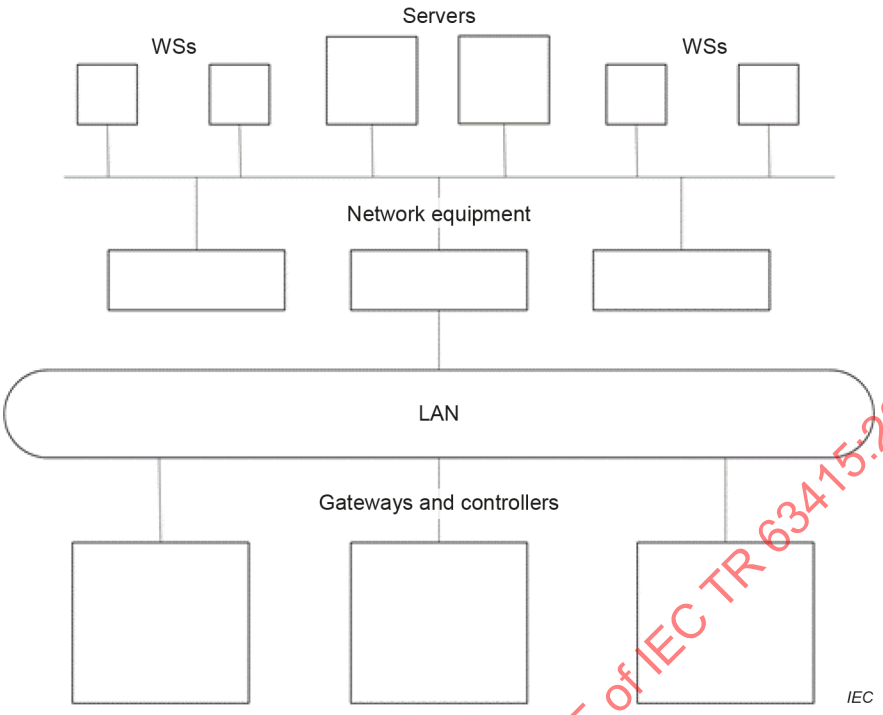


Figure 1 – Structure of a typical I&C system

NOTE The detailed structure of the real I&C system can be more complicated. The presented typical I&C system are simplified and omitting details as low level measurement transformers, actuators to avoid unnecessary complication in demonstration of the approach.

The WSs are implemented on the basis of graphical capable computers and are connected to specific server(s) via LAN. WSs connected to the same server form a single domain that is associated with a specific function being performed or a group of controlled equipment.

The servers process and archive the information received from the gateways. A server also implements automatic control algorithms that form operator-independent control instruction flow.

The information about the NPP technological equipment is received from the gateways (controllers) in the form of analogue or discrete variables characterizing the state of the equipment. Reverse flow of information from the server to the gateway forms flow of the control commands.

7 Security requirements and security architecture

7.1 General framework

Security policy is the starting point for understanding how various components involved in a security architecture are related to each other. The security policy is built on the risk analysis results and the level of risk tolerance held by the organization operating the nuclear facility. The security policy defines system's requirements to handle the cybersecurity goals inside and beyond the system. The risk analysis results and organizational risk tolerance will provide a bounding case for risk and help determine if the cybersecurity goals for the system are being met. The requirements might specify:

- allowed and forbidden system states;
- safety classification and security degree assignment for assets;
- grouping the assets by logical zones;

- referenced standards .

Therefore, the security requirements target the entire set of layers of the I&C system hierarchy: system, subsystems, and lower level elements and components like software and hardware elements, including but not limited to chips, standalone programs, and files. Security requirements also affect the personnel dealing with the I&C system: operators, engineers, security staff, contractors, etc. The security architecture depends heavily on appropriate security requirements. The security requirement additions or changes are reflected in system architecture.

A system designer establishes overall defensive security requirements where all identified assets are labelled with a security degree and implement security controls commensurate with the security degree. The requirements for defensive architecture include, but are not limited to, formal logical or physical boundaries like the security zones in which the defensive measures are deployed.

To ensure the defensive architecture remains effective, data flow is properly handled between security zones assigned to different security degrees and between individual I&C systems on the same security degree based on a risk informed approach.

During the security design process the goals postulated by the security policy are possibly mixed and heterogeneous. Input data used in the process of goals identification is probably weak and incomplete. That all makes the security requirements identification process time consuming, challenging and iterative.

Therefore, even the existence of the right security requirements in system's design specification does not guarantee that its realization in the I&C system will maintain the security risk for the I&C system at an acceptable level. Furthermore, when security requirements are mapped into security architecture the following problems arises:

- If the security requirement is formulated in a natural language, then a non-formal definition of the security requirement itself enables various interpretations of its implementation;
- Considerable complexity of the security requirements for I&C systems, involving a large number of assets and relationships between them, cause some aspects of the security requirements to be missed when defining the security architecture.

One possible solution to these problems is to set the security requirements in the form of formal (analytical) description which allows mathematical verification. This formal representation serves as input for other models describing components of the I&C security architecture. A systematic approach ought to be used to define requirements and trace though detailed design and into testing. Failure Modes and Effects Analysis is recommended at the requirements definition phase while a requirements traceability matrix is recommended thereafter.

In the general case, formal models of the I&C system reveal security requirements and identify important characteristics of environment at a sufficient level of detail. This combines the consideration of security issues with a common understanding of the context. The models used for cybersecurity requirements and security architecture representation might be very different and various but commonly all of them are known from computer system access control (DAC – Discretionary Access Control, MAC – Mandatory Access Control, Trust models, etc.) or system analysis (Markov networks, Petri nets, Failure trees, etc.) [8] through [15]. The DAC based model will be considered in the work. The reasons for selecting a DAC model are: considerable simplicity of the model and an existing well defined mathematical foundation and practice in information security. The limitations of the model are: the lack of flexibility and fast growth of the model size for large systems. In the case of I&C systems, the limitations are mitigated by the reasonable size of real I&C systems and fixed structure and functionality of the I&C system. The book by Bishop [11] gives more details of properties and algorithm behind the DAC model and Annex H contains the brief introduction to the mathematical notations used below.

7.2 Integrated security model

The mapping between security architecture and security requirements is provided by the integrated cybersecurity model (ICM) framework. The NPP I&C system ICM is the set of components $ICM = \langle SLM, DM, R \rangle$, where DM describes a model of information exchange between assets, the component SLM specifies general rules of access for the information, and the operator R specifies rules of matching between these two models.

It is evident that information exchange flows ought to not violate information security rules in a correctly designed system. Speaking in the model terms, the DM model ought to be in accordance with the SLM model.

In this TR we define I&C security architecture synthesis as bringing a DM model to correspond with a SLM model. How this can be done, the model properties, and the methods of architecture synthesis will be explained in detail below. Next, let us consider components of the model in detail.

7.3 Basics of the information exchange model (DM)

The component DM represents system assets and information transfer rules between them.

Formally, it is described by the DAC type model: $DM = \langle G^*, OP \rangle$, where $G^* = \langle \{ G_i \mid i = \overline{1,N} \} \rangle$ are all possible system states characterized by security graph G_i with assets as vertices A and with edges representing the binary relation of directed information transfer between assets in the frame of system operation, OP is a set of security graph transformations corresponding to the model (we call it allowed transformations) $G_i = \langle A, \{ |\!\rightarrow, \rightarrow \} \rangle$.

The model defines two types of the transfer (access) to the data: secure and simple. The information transfer between two assets is simple if there are no security barriers on the information path. The information transfer between two assets is secure if there is some security barrier on the information path. This barrier allows to achieve desired security property for an example maintaining the integrity of the asset.

The model does not specify the barrier internals because it depends on the implementation of the I&C system. There are two types of vertices in the security graph: the first corresponds to objects, the second corresponds to objects.

The detailed mathematical properties of the model are given in Annex A and [5].

7.4 Basics of the security model (SLM)

The security model is defined as a collection of classes (security degrees), relations between them and rules governing asset attribution to a degree.

Formally, it is described by the model $SLM = \langle SC, \rightarrow, \otimes, \twoheadrightarrow \rangle$, where:

- SC is a finite linearly ordered set of security degrees consisting of N_{SC} elements;
- $\rightarrow$ is the “simple” relationship defined on a pair of security degrees;
- $\twoheadrightarrow$ is the “secure” relationship defined on a pair of security degrees;
- $\otimes$ is the asset grouping operator.

Additionally, with the security degree, the notation of the security zone will also be used. A zone is a subset on the set of vertices (assets) in the security graph that form a strongly connected subgraph in the graph for the selected relation. All assets in the zone, respectively, belong to the same security degree.

The detailed properties of the used model are given in Annex B and [5].

7.5 Basic principles of the secure design

Secure by design is a method of the system software and hardware development that aims to implement the system in such a way that its architecture minimizes system vulnerabilities and reduces the size of the attack vector at each stage of the life cycle [4]. The principles of secure by design include:

- early detection and elimination of security vulnerabilities in the I&C system security architecture;
- definition of common information security measures between assets to reduce security implementation and maintenance costs.

The achievement of these principles is obtained through strict conformance between all parts of the integrated security model. The criterion is defined as follows:

A system described by an ICM model is cybersecure if the set of allowed operations (OP) on assets cannot result in a situation where the information flow between assets would violate the relations fixed in the security model. We say that for I&C system the DM model corresponds to the SLM model or the two models are coherent.

The sufficient condition for that if after ordering and grouping the assets into security degrees using group operator we get bijection between the resulted graph and a sub-graph of the security degree lattice.

A more detailed justification of the secure by design principle is given in Annex C and in Clause 8.

7.6 Asset ranking and ordering

Asset ranking and classification is an important part of the secure by design approach when it is necessary to provide defence in depth. In general, asset consists of “item important to safety” and “item not important to safety” from software aspect of viewpoint; when it comes to secure I&C architecture design, information classification (grouped and ordered)) is an important part of designing a security framework that can protect sensitive data and assets from cyber threats.

The ordering function P describes the process of asset ranking and the operator R arranges the ranked assets in security degrees (classification) and builds information links between the degrees according to the rule: if all relations between system assets from two different degrees are secure then the relation between the corresponding vertices of Λ are secure. Vice versa, if there is a simple relation between system assets from two different degrees then the relation between the vertices is simple, too.

A detailed description of asset ranking and ordering procedure is given in Annex D. Practical issues of the function P and the operator, methods of asset classification, are not discussed in this subclause (see Annex E,and Annex G).

7.7 Information property of the asset

The ranking and classification processes use informational properties of the asset $\boldsymbol{Q_j} = \{C_j, I_j, T_j\}$, where C_j, I_j, T_j are a set of some parameters of confidentiality, integrity and availability. In a simplified framework the properties related to confidentiality and availability are omitted and $\boldsymbol{Q_j} = \{I_j\}$. The main reason to concentrate on the integrity is that precedence order of these properties for I&C system (see [2]) as: availability integrity and confidentiality listed from most to less important. The DAC model used for security analysis doesn’t work with time characteristics of the system which is necessary for availability assessment. Some suitable approaches for availability assessment can be found in works [26],[27],[28].

NOTE 1 The detailed explanation of the integrity property is provided in Annex C.

NOTE 2 However, when considering characteristics of confidentiality the inverse nature of the models Biba and Bell LaPadula permits using the same approach.

Based on the Biba model [8], let us assume that assets having access to a greater number of other assets with respect to write are considered more important from the point of view of security. Then the task of finding important assets is largely similar to the problem of finding a leader (the most influential person) in social graphs (see, for example [12]) or using metrics of cyclomatic complexity (branch points) for software engineering when assessing its reliability when it is most critical [13].

For the system described by the security graph G_0, we define the quantitative characteristic of the information property of the asset for integrity as the output degree of the vertex computed on the transitive closure of the graph G_0 in the selected access relation (w).

In the general classification case other properties of assets, such as functional or technological properties, might be considered. The ranking function takes into account asset involvement in the performance of a particular safety function of the system when the safety classification is known (see Annex G).

7.8 Security degrees concept and security architecture

The whole design approach of the security architecture is based on a differentiated approach when degrees are assigned to the assets according to the asset's criticality for security provisions [2]. Appropriate barriers are implemented between classified assets to prevent the spread of an attack if any asset is compromised.

The security model SLM and the ranking model R use the concept of security degree. It is necessary to dwell in more detail on what meaning is embedded in security degree in each model. The approach presented in the work is based on the methodology introduced in IEC 62443-3-3 [14], where three different types of degrees are defined:

- Target security degree for asset. It is determined by the hierarchy of SLM access model levels. The target degree is assigned to the asset based on the results of the risk assessment, taking into account the functions performed by the asset in the I&C system. The target security degree ought to be changed only as a part of the redesign activity for the system.
- Achieved (real) security degree of the asset. It is determined by the I&C system network architecture, the internal properties of the asset and the implemented security controls that are involved to prevent security breaches. The achieved degree is a function of time and external conditions, under those the asset operates. It might change over time due to lowering efficiency of security measures, the appearance of the new vulnerabilities and evolution of the security threats. The achieved security degree, as well as target degree, assigned to the asset as a result of a risk assessment takes into account the functions performed by the asset and operating conditions for a real I&C system. The difference between target security degree and achieved security degree is that the target degree is determined at design stage while the achieved degree is determined based on operating conditions in later life cycle stages.
- Potential security degree. The degree of the security for the asset that is uniquely determined by the structure of information links existing in the system. The DM model and information properties of the asset uniquely define the potential security degree (7.7).

If necessary, we will designate the target, achieved and potential degrees by the superscript t, r, p, respectively in degrees definitions as: L_n^t, L_n^r, L_n^p, where n is the number of a degree.

7.9 Establishing a relation between the data model and the security model

Generally the term synthesis of security architecture means the process of bringing the model DM into line with the model SLM .

After the security degrees are defined, it is possible to define more precisely the task of the security architecture synthesis using the framework introduced in Clause 5.

The system described by the model ICM is secure if any sequence of permissible operations (OP) on the assets in data model cannot lead to an information flow that will violate the relations between security degrees defined by the security model. The violation means that no data flow is possible between assets in data model belonging to some security degrees if the flow is not allowed between the same security degrees in the security model.

This means that securely designed I&C systems ought to have the following relations between the potential, actual and target degrees: $L_n^t(a_i) \geq L_n^r(a_i)$, $L_n^r(a_i) \geq L_n^p(a_i)$, $a_i \in A$. Simply stated, for any asset the achieved security degree fulfils the security requirements given by the target security degree. The potential security degree defines the upper limit for security degree value that can be achieved according to security architecture integrity level.

NOTE Here the higher, more secure degree is expressed by a lower degree number (L).

It is obvious that the potential security degree in such system ought not to be lower than the target and actual degree.

One of the problems that has to be solved during the design of the security architecture of the NPP I&C system is to establish the correspondence between the actual (achieved) degree of cybersecurity and the target degree with due account for the restriction of capable security degree.

In this context, two main subtasks can be distinguished:

- coordination of the target and actual degree of the system;
- coordination of capable and target degrees.

The target degree for an asset is most often set by experts at the initial stage of system design and is not reviewed anymore. The actual and potential degrees of the system depend on the information links of the asset in the system (DM model) and can be changed during the design of the system, modifications in the links between assets or the application of protective measures.

8 Procedure of I&C security modelling

8.1 General

The synthesis of the desired security architecture for the I&C system consists of the following steps.

a) Set the target security model: Set the type of target architecture as a security model.

b) Set the level of the detail: Define the level of detail for consideration (subsystems, components, or components parts of I&C system).

c) Adopt the method of asset classification: Accept the method of asset classification.

d) Identify the assets.

e) Define target security degrees L^t to the assets: Define ranking and classification (grouping) of the assets and their assignment to one of the target security degrees. Optionally, along with

the target degree, a security zone can be assigned to assets for the purpose of simplifying their administration and management of the security.

f) Build the data model. Calculate the potential security degrees (L^p).

g) $L^t \geq L^p$: Compare the target and potential security degrees, if necessary, modify the system architecture and change the DM model. If zones are defined for assets, then the belonging of assets to certain security zones is also taken into account.

h) Modify the system: If the condition g) is not held necessary change properties of the system as barriers or information path.

1) Asset reclassification: Classify assets and assign to them the real security degree (L^r). This procedure can be considered as a repetition of the classification procedure when a real (modified) security architecture is used.

2) $L^t \geq L^r \geq L^p$: Compare the target and actual security degrees. If the result is not satisfactory, repeat steps d) through h) .

The procedures in items a) through c) are preparatory stages of the synthesis, steps d) through h)are the main ones. The whole process is iterative in its nature, when the result of the previous steps can be reviewed and changed according to the result of the execution of any next step Figure 2 provides the algorithm of the architecture synthesis.

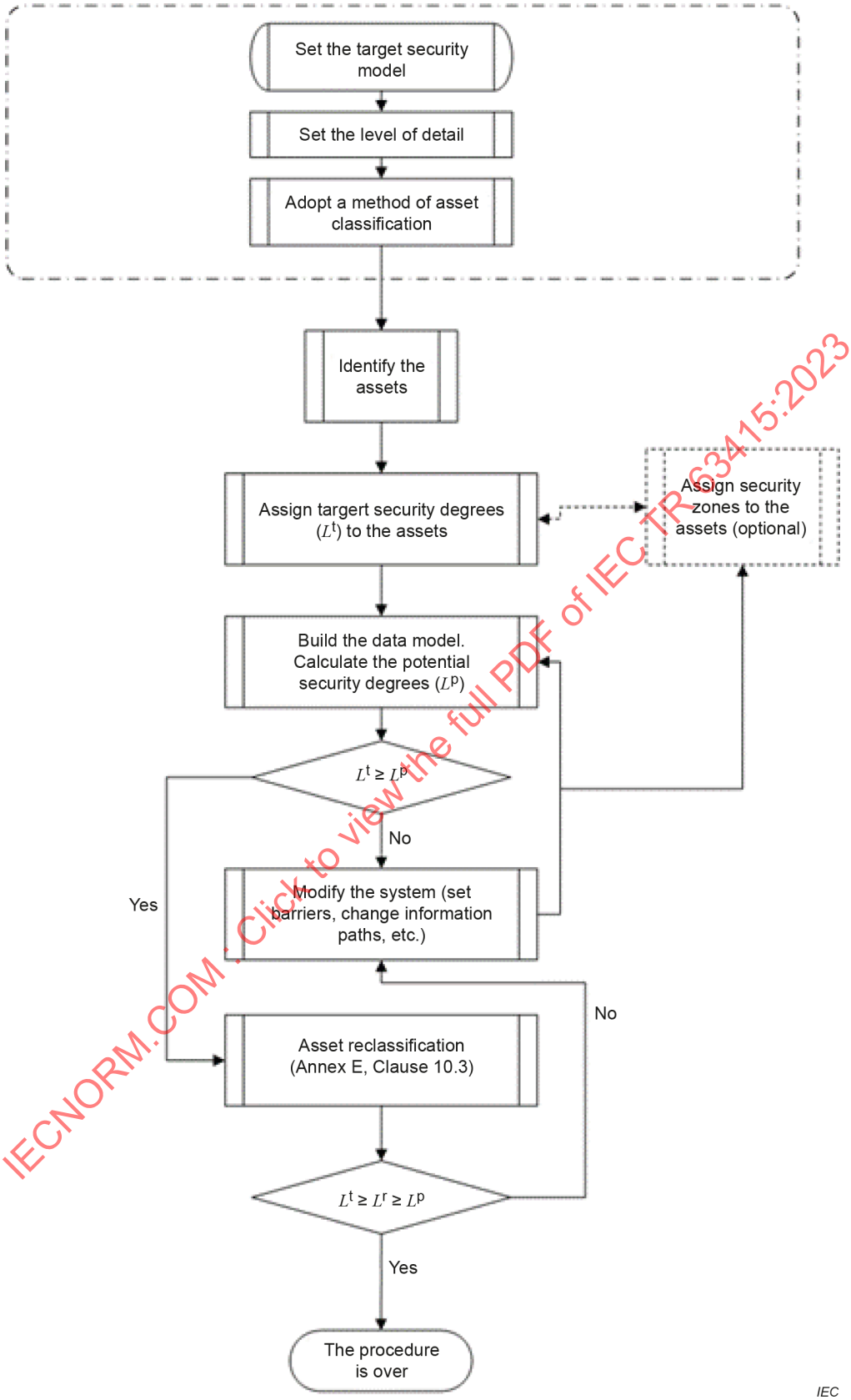


Figure 2 – Procedure of security architecture synthesis

The procedures of items a) through c) will be reviewed in a general form in Clauses 8.2-8.4 below, and the other steps will be analysed using a specific example (Clause 9).

Some algorithmic aspects of the synthesis procedure are given in Annex F.

8.2 General approach to asset classification

The ordering function P describes the process of asset grading and the operator R arranges the ranked assets in security degrees and builds information links between the degrees (Clause 7.6). But practical issues of the function P and the operator, which are methods of asset classification, have not been discussed yet.

This document considers the asset classification problem as a clustering problem [15], that is, identifying groups of objects to which the equal criterion could be applied. The presented method takes into account the established practice of cybersecurity asset classification stated in the field-specific publications [3] and IAEA [16].

The cluster analysis considers a cluster a part of the data, typically, a subset of objects which are characterized by a subset of variables, separated from the set by some uniformity of elements.

The problem can be divided into four sub-problems:

a) selection of the input data representation for the analysis;

b) determination of the cluster structure shape;

c) selection of the estimation criterion of the cluster structure;

d) selection of the procedure for constructing the cluster structure.

Annex E considers each of the sub-problems in the context of asset classification by cybersecurity.

8.3 Security degree assignment and the analysis of model conformance

The clustering technique allows the partitioning of a set of elements into a few groups according to given criterion of homogeneity of elements, but the technique does not specify an order relation between the resulting clusters.

We suggest building the order relation between the clusters empirically. First, select an asset $A_i \in \{A_i\}$ in every cluster and assign a rank to it. If needed, merge the ranked clusters into security degrees. It is expected that these actions will always be necessary, unless the number of clusters was equal to the number of degrees.

At this point all the assets A have been partitioned into ranked clusters.

Next, the link transformation rules (see Annex D) is applied to the resulting ordered set of clustered assets and thus obtain a cybersecurity level graph $\Lambda(l,D)$ for the calculated partitioning. Finally, comparing graph $\Lambda(l,D)$ with the security level lattice we get the answer to the question about correspondence between DM and SLM models in accordance with the conformance criterion stated in Clause 7.5 and Annex G.

Practically, the conformance means that the information workflow (DM model) does not violate the allowed information paths between different security degrees i.e. SLM.

8.4 Classification in hierarchical systems

All the above arguments did not take into account the hierarchical structure of NPP I&C systems. Real systems mostly consist of subsystems (the assets have its internal structure), which, in turn, include further subdivisions, etc. If the system of interest has no subsystems (the

assets are elementary or trivial) then the provided method gives a complete formal approach to the cybersecurity asset classification.

This reasoning is illustrated with an example of a system having one nesting level. In case of hierarchical systems, inductive method is used.

The structure of the subsystems is not developed yet at the design stage, but the set of subsystems is identified and the information flows between them are already known. One can build the security graph using the subsystems as assets and apply the presented formal method to classify the subsystems according to security degrees. After that, a cybersecurity class is assigned to each subsystem.

The developers of a subsystem face some issues. If a cybersecurity class is assigned to the subsystem, does it mean that all the elements of the subsystem are protected according to this class? For example, if a subsystem with high security degree contains an auxiliary element that has little influence on the system's functions is protected in the same way as the main elements of the system?

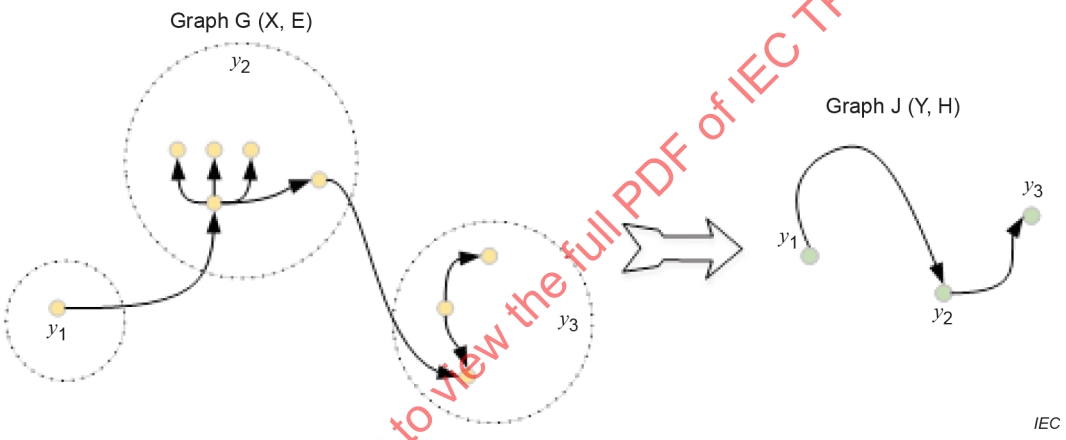


Figure 3 – I&C information model with subsystem hierarchy (left) and without it (right)

Let us consider two security graphs: the left one, $G(X,E)$, takes the structure of subsystems into consideration and the second one, $J(Y,H)$ isn't (see Figure 3). J is evidently a result of graph contraction G: $J = \mathbb{F}(G)$ that is not a one-to-one mapping. The formal classification method generally gives different results on the graphs $J(Y,H)$ and $G(X,E)$. Moreover, since the order function is constructed on the transitive closure of the security graph, it leads to a paradoxical conclusion: a developer of a subsystem knows the structure of the whole system and the information flows in the system. The direct implication of the formal classification method does not give any practical results.

The paradox is eliminated, if note that classifying the subsystems of the graph $J(Y,H)$ into security degrees adds an additional constraint onto the subsystem elements in the initial graph $G(X,E)$: and limited the maximal security degree for the internal assets of subsystems.

Let us propose the following algorithm for the classification of systems with arbitrary number of nesting degrees.

- First step: A system designer builds the security graph with subsystems as vertices and carries out the asset classification for this graph. Then, every subsystem gets a security degree. Optional barriers can be set between subsystems of the same degree; mandatory barriers ought to be set between the subsystems of different classes, and, on the part of the

system with a higher security degree. In the frame of the adopted model the installation of the barrier means transformation relations of the type $\mapsto$ into the type $\rightharpoonup$.

- Second step: Designers of subsystems build security graphs for their subsystems and classify the assets with additional constraints: maximum cybersecurity assets degrees within the subsystem equal to the subsystem security degree; the set of assets belonging to the maximum-security degree is not empty. After the classification, the barriers between asset groups are set as well: mandatory barriers if separated groups belong to different cybersecurity classes and optional barriers, if the groups belong to the same security degree.

The designer of a second level subsystem (a subsystem inside another subsystem) classifies its assets according to the second step, etc.

9 Case study of I&C security architecture synthesis

9.1 General

There is a practical technique of security architecture synthesis based on the principles presented above. The security synthesis architecture procedure is demonstrated for a subsystem of the typical NPP I&C system (Clause 6). The example uses the implementation of I&C system based on a platform Operator [17]. To analyse and synthesize the security architecture, Omole security designer program [18] is used. In the example, the actual security degree is not considered separately and it is silently accepted that actual security degree is equal to the potential degree $L_n^r(a_i)=L_n^p(a_i)$, $a_i \in$ A. This simplification is reasonable when it is not necessary to consider the exact details of the implementation of the I&C system. An example of a more detailed account of the real characteristics of the system during classification is given in Annex G and [5].

9.2 Definition of the security model

The security architecture defined in [19] is selected as the security model. The graphical representation of the architecture is shown in Figure 4. The architecture since the introduction has become de facto an international standard for the nuclear industry. Five degrees of the computer (cyber-) security are introduced in the model: 1 is the highest, 5 is the lowest. Information flow from a higher to a lower degree is allowed without restrictions; data transfer from a lower degree is allowed for the two lowest degrees only. The main goals of a cybersecurity system that is built on the architecture are to maintain the integrity of data and to prevent the change of information by low-degree systems in a top-degree system.

The security architecture impose that I&C systems requiring the highest degree of security (i.e. the most stringent security degree) is only connected to systems requiring lower degrees of security (i.e. weaker security degrees) via fail-safe, deterministic, unidirectional data communication pathways. The direction of data pathways ought to be limited to the transmission of data from devices requiring the most stringent security degree to the devices assigned to weaker security degrees.

The architecture includes series of concentric defensive degrees of security enhancements and considers both hardware and software components. While implementing such architecture, designers limit the dynamic elements of both the composite networks and their individual systems to increase the determinacy of their behaviour.

The security controls are implemented between I&C subsystems and components that have different security degrees.

Data flow from a top degree to a low degree is determined by the written access rule (w) granted by a subject of the top degree to a subject of the low degree.

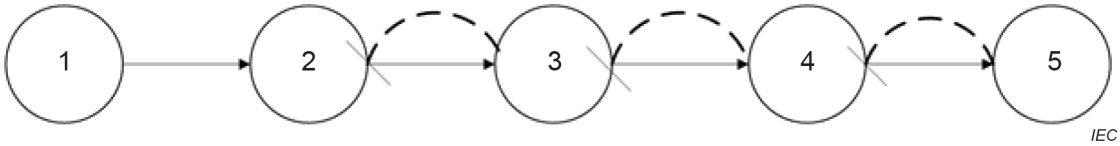


Figure 4 – Simplified information model of security.
(secure relation between degrees are shown by dashed lines)

In the framework of nuclear safety there is a limitation on the direct transfer of the information between assets, whose classes of nuclear safety differ by more than one. Accordingly, a similar principle is also applied to the exchange of information between assets classified by different security degrees.

9.3 Selecting the detail level in system analysis

In practice, I&C system is almost always constructed as a complex and has subsystems (assets have an internal structure), which, in turn, include components, etc.

Therefore, it is necessary to set the level of consideration of the system, or define assets which are considered atomic. For demonstration purposes, the assets listed in Table 2 are treated as atomic. Thus, the I&C system will be considered at the level of software and technical components. For hierarchical systems with a greater degree of nesting, it is possible to apply induction method and use the described methodology for other levels of detail of the system.

9.4 Asset classification

Let us consider the task of classifying assets and grouping them into security degrees as a typical clustering problem [25] by identifying groups of objects to which the same criteria are applicable. In many cases, for small systems and with adroit specialists, clustering and classification can be done by experts.

This approach fully takes into account the current practice of cybersecurity assets classification for nuclear power plants [2].

In cluster analysis, a cluster is usually understood as a part of the data, in a typical case, a subset of objects characterized by a subset of variables, which is distinguished from the entire set by the presence of some uniformity of elements.

The clustering task can be divided into four subtasks:

- selection of the data representation for analysis;
- determination of the type of the desired cluster structure;
- selection criteria for evaluating the cluster structure;
- selection of a method for building a cluster structure.

The classification method taking into account the asset's functional, informational, technological, and other properties is given in Annex E.

The set of characteristics for describing each of the security properties can vary depending on the properties of the system being analysed.

In the example, we restrict ourselves to information properties of assets, i.e. characteristics reflecting the connectivity of an asset and possible ways of spreading an attack in violation of the integrity of information associated with an asset.

We set the information property of an asset as the value of integrity level I_j with respect to the write access relationship: $P(I(A)) = \{X : x_1,\ldots,x_M\}$, $M \le M_A$,.

9.5 Identification and initial classification of assets

The input data for this stage is data from Clauses 9.3,9.4 and additional information as:

- a list of identified assets;
- an assigned target security degree for assets $L_n^t(a_i)$, $a_i \in$ A;
- a zone assignment for assets (zone assignment is a result of asset grouping on logical or physical closeness and separation).

The input data are summarized in Table 2. To keep the example clear, only software modules are considered in the list of assets. Therefore, the list of assets does not contain auxiliary components of a real I&C system: network equipment, computer hardware or power supplies, physical access control devices, climate sensors, etc. The example also does not consider possible existence of redundant elements, since redundancy policy is system-dependent and tied to a specific implementation of the system. However, while modelling a real system, the redundancy of elements ought to be taken into account.

The assets are classified by assigning a target security degree.

Table 2 – List of assets of a typical control system channel and IS target characteristics

Asset name	Description	Target security degree (L_n^p)	Zone(S_n)
Workstation software			
Operator	A human	5	1
IZ	The module that provides a graphical interface with an operator	5	1
Ab	The module that provides a logical interface with the operator	5	
WWW	Web browser with access to data archive via a web server	5	
OS WS	Operating system	4	2
Server software			
DB	Database server	3	3
Archdb	The part of the database that is responsible for storing the data	- not set for assets of type object	
WWWServ	Web server with access to the archive of equipment status data	not lower than 4	4
OS_SERV	Server operating system	2	5
Gate	Equipment controller	3	3

In the example only four of five possible security degrees are used.

9.6 Data model

The I&C subsystem implements the following procedure of interaction between components.

Operator, via the workstation human-machine interface (IZ and AB components), can change control's records in the server's database (DB component).

AB regularly requests the state of the equipment (reads the record to and from the database) and displays it to the Operator via the computer graphical interface (IZ).

The server's database asset (DB), when the state of the records changes, initiates the transfer of commands to the controllers (Gate). In addition, DB queries the equipment status from the controllers and stores them in the database (ArchDB asset).

The algorithm module (ES asset) implements automatic control procedures.

The Operator also has the ability to get the history of the equipment state using the Web-interface for database access (WWW, WWWServer).

All assets operate on computers under the control of an operating system (OS_SERV, OS_WS).

All assets except ArchDB are subjects in the terms of the model.

The security graph for the I&C subsystem is shown in Figure 5.

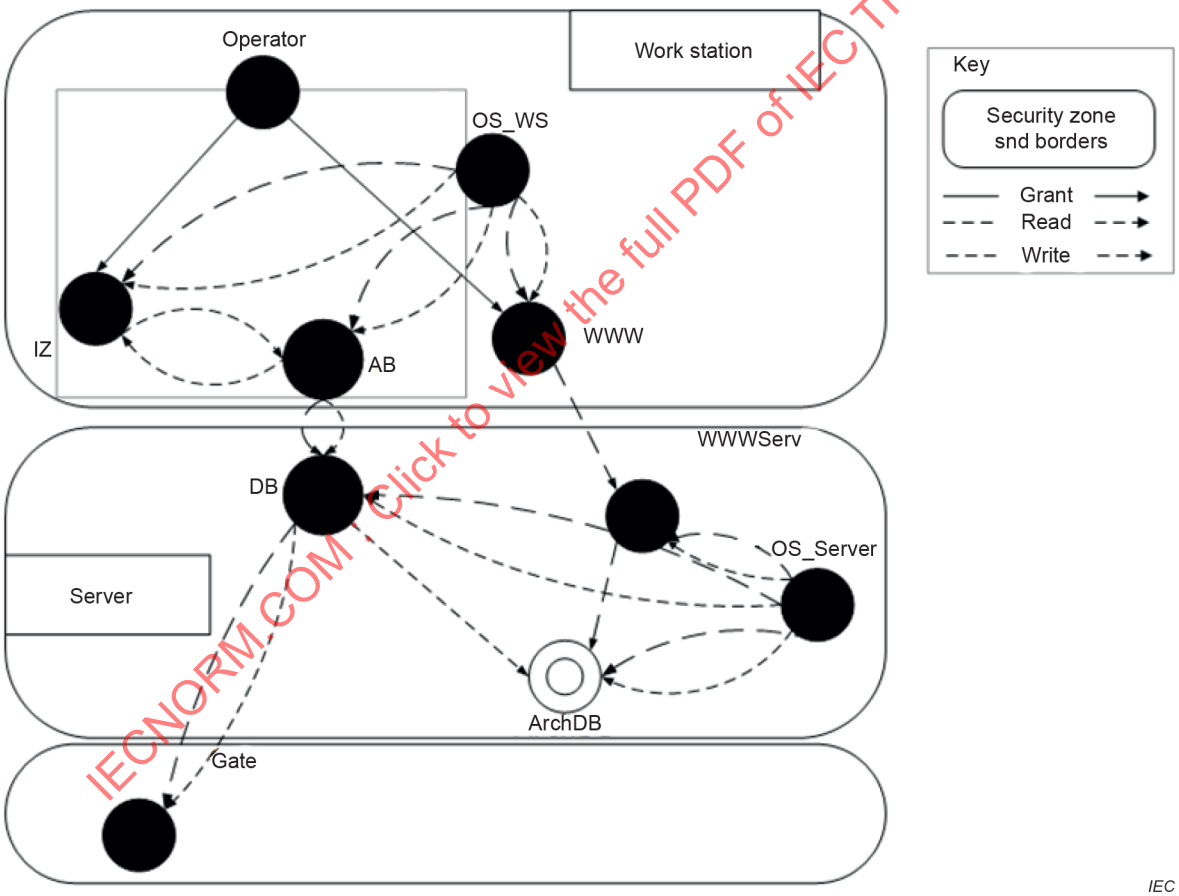


Figure 5 – General security graph for I&C subsystem without taking into account security controls. The borders show boundaries for workstation server and gate subsystem.

9.7 Analysis of the model and synthesis of architecture

The analysis starts with the calculation of the potential security degree for asset basing on their information properties (Clause 7.8). In the initial architecture version (without the use of any security controls), all assets (Figure 5) are at the same security degree and logically belong to a single security zone, because all vertices in the security graph (assets) are strongly connected by the following relation:

$S_0(a_i)$, $a_i \in$ A,

$L_0(a_i)$, $a_i \in$ A.

It means that the data DM model does not match the SLM, and a synthesis of the cybersecurity architecture needs to be carried out.

The procedure of the synthesis will start with allocating asset OS_WS in a separate security zone in accordance with the security requirements defined by Table 2. To do that we will consider the write relations to the direction of the asset (implicit reading) and separate the OS from other assets. To minimize changes in the existing communication between assets in the system, we will use the methods of the minimal edges cut-off [20]. The modified security graph is shown in Figure 6.

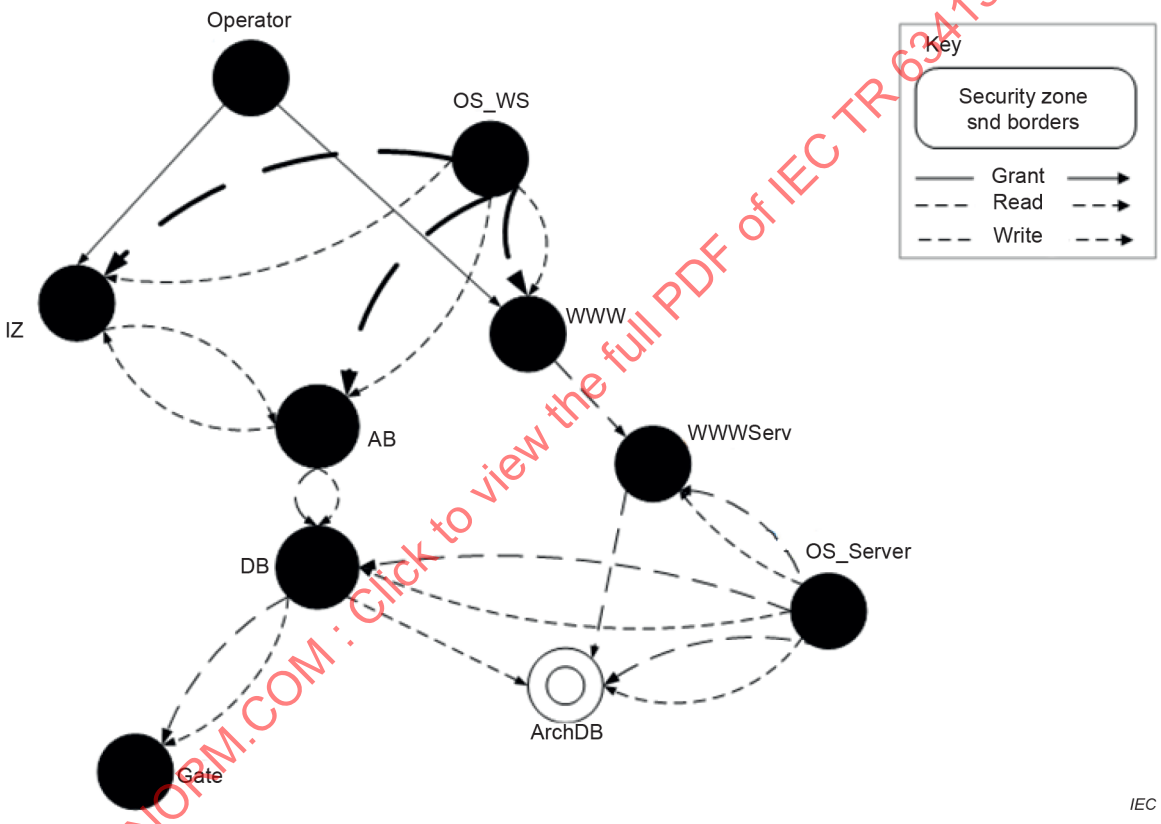


Figure 6 – Changes in the security graph for I&C subsystem when OS_WS asset is targeting allocation to a separate zone. The edges belonging to the minimal cut are shown with bold lines.

Evidently, simply by breaking the write relation to the direction to OS_WS assets, we solve the problem of allocating the asset in a separate zone, but, most likely, it makes the I&C system inoperable since the OS ought to receive information from application programs (IZ, AB assets). In order to enable OS assets to receive information from other assets in the computer but to preserve the integrity of the OS asset, we change the simple read relations to secure. The similar work is done with server OS assets. It means that we put a security barrier between the OS and other assets. The barrier implementation is the developer decision. Some examples of barriers are: access right hardening, resource isolation, containerization, etc. The resulting security graph with security degree structure is shown in Figure 7.

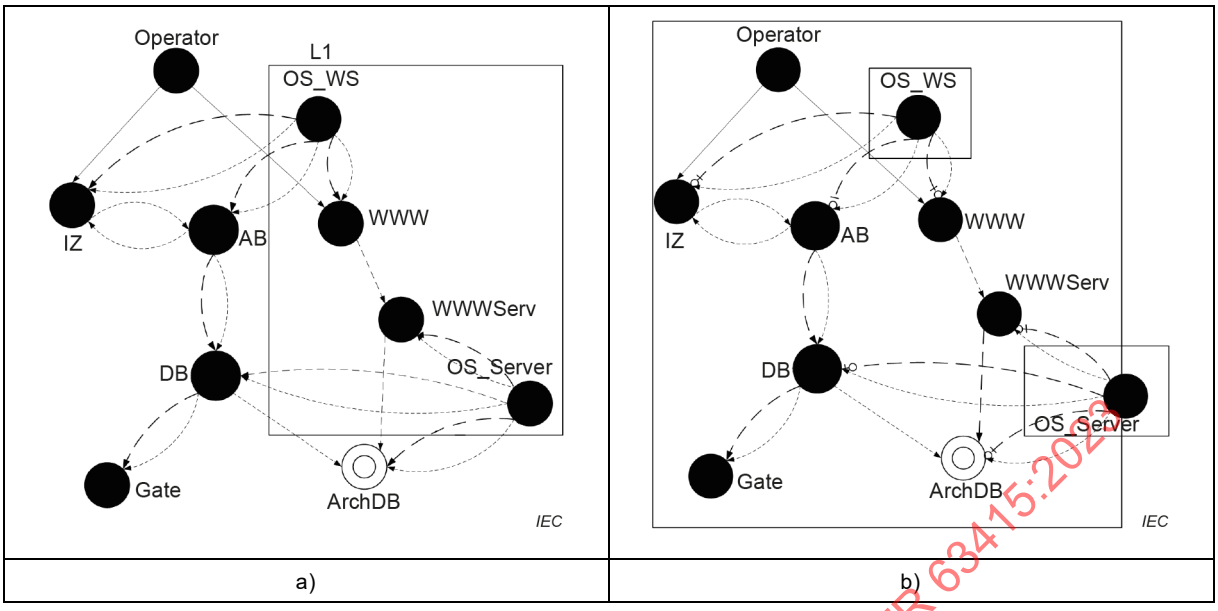


Figure 7 – General view of the security graph for I&C subsystem, taking into account security controls for OS assets. The security degree structure is shown in a) and the zone structure is shown in b). Degrees and zones are shown in a solid rectangle. The degree is numbered.

A partial result of architecture synthesis is the separation of OS assets from others within a separate security degree and zone.

At the next step of the security architecture synthesis, we will solve the problem of separating the server's application assets (DB, WWW server) into their own security zone (see Table 2). For that purpose we are considering options for separating these assets from the workstation's assets (Figure 8).

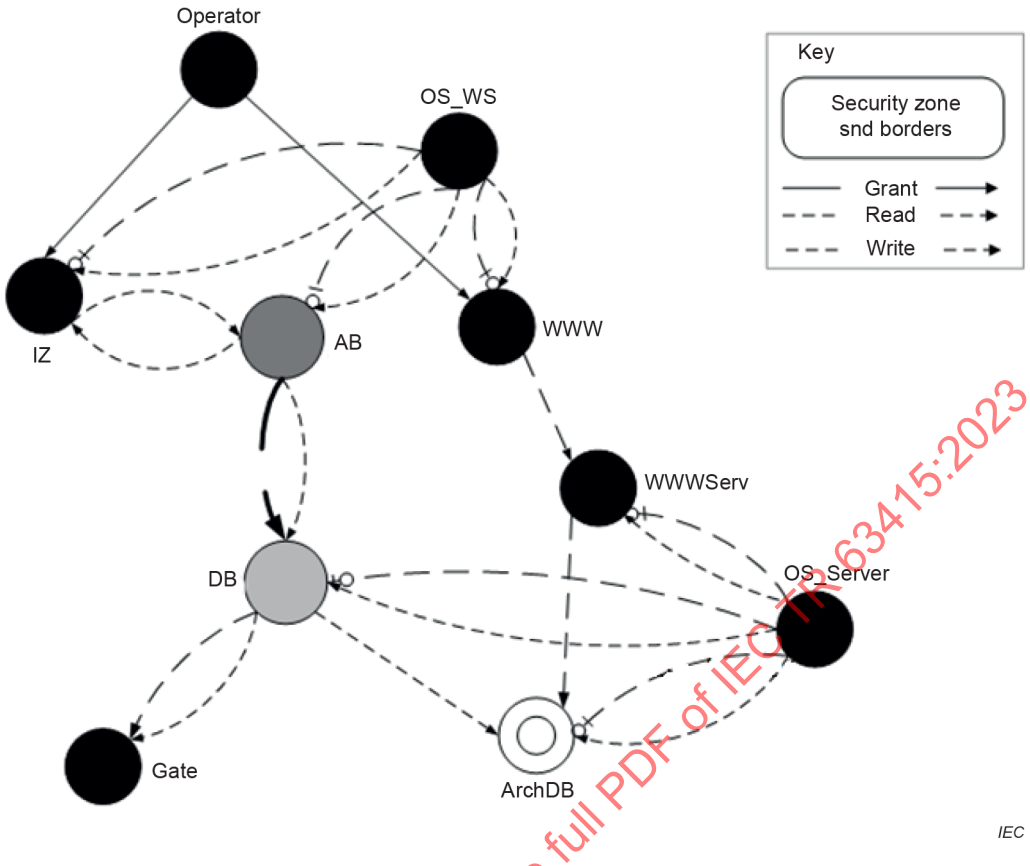


Figure 8 – Changes in the security graph for I&C subsystem when server assets are targeting allocation to a separate zone from the workstation. The edges belonging to minimal cut are highlighted with bold line.

In order to allow the asset DB to obtain information from the asset AB in the workstation, but keep the integrity of the asset DB, we change the simple write relationship belonging to the cut-off to the secure reverse reading relationship between assets AB and DB. For the resulting modified security graph, we again calculate the potential security degrees and security zones taking into account the write relationship (Figure 9).

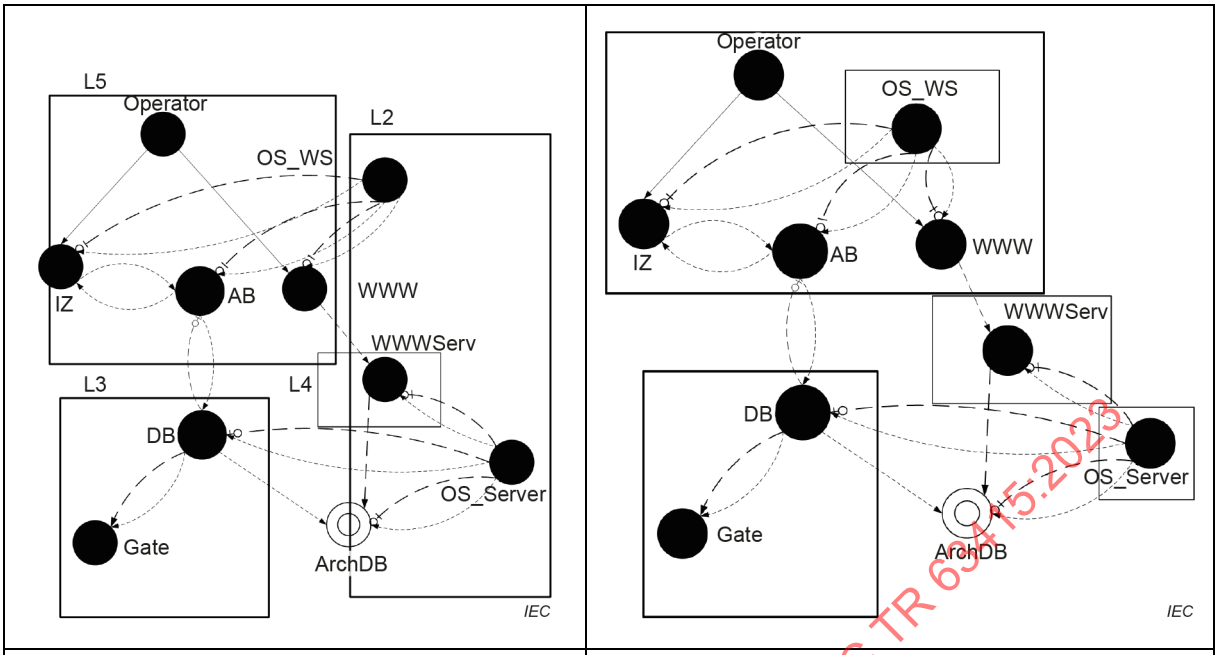


Figure 9 – General representation of the security graph for practical I&C subsystem, taking into account all assigned security controls for the assets. The security degree structure is shown in a) and zone structure is shown in b). The degrees and zones are shown in solid rectangle. The degrees are numbered.

9.8 Assessment of the modified security architecture

The initial security architecture of the I&C subsystem from the point of view of information exchange is a monosystem where each identified asset has complete information about the others. That architecture has no obvious advantages in a sense of functionality but from the security point of view it is extremely vulnerable. Any security violation of one asset, e.g. hacked functionality of a software module, disrupts any function within the subsystem.

Therefore, one of the goal of the security architecture synthesis is reducing the risk of such incidents – dividing the system into security zones with the establishment of security barriers between assets. The barriers and more generally security controls defined in zone target two goals:

- the barriers defend the assets inside zone from external threats;
- the zone encapsulates any compromised asset and prevents the spread of the consequence of an attack out of zone. This assumption prerequisites that the attack is discovered by additional means (security controls) implemented at boundaries or inside the zone. Just encapsulation might not be enough.

In case of the “flat” system without security degree differentiation, the assets which have different importance, value and functionality are equally protected and that can increase the cost of designing and maintaining the system. A differentiated approach, in which the degree of protection is correlated with the degree of importance of the function, can reduce the cost of providing information security for real industrial control systems.

In the example, different target security degree has been assigned to the assets according to their functions. This assignment is the input data for the architecture synthesis.

Finally, the obtained security architecture is the result of the coordination of the target architecture defined by security model and the real information structure of the system; the assets are separated into four security degrees and are located in five security zones. The OS

assets are at the top security degree, the server assets are at the next (lower) degree, and the application software (assets AB, IZ, WWW) of the workstation are at the last security degree.

The synthesis ensured the alignment $L_n^p(a_i) \le L_n^t(a_i)$, $a_i \in$ A, and ensured the alignment of the data and security models. For the asset "OS workstation" $L_n^p(\text{OS\_WS}) < L_n^t(\text{OS\_WS})$, a direct information exchange between the assets, belonging to the security degrees differing by more than one is not allowed in the security model. To take that into account, the actual degree of security $L_n^r(\text{OS\_WS}) = 3$ ought to be assigned.

The initial and final security architecture properties, security degrees and zones are shown in Table 3.

Table 3 – Information security characteristics for assets in the architecture of a I&C subsystem

Asset name	L_n^t	$L_n^{p'}$ The potential security degree in initial (not modified) security architecture.	L_n^p The potential security degree in final security architecture.	S_n	S_n The security zone in initial (not modified) security architecture.	$S_n^{''}$ The security zone) in final security architecture
IZ	5	1	5	1	1	1
AB	5	1	5			
WWW	5	1	5			
OS_WS	4	1	2	2		2
DB	3	1	3	3		3
Archdb	-	1	-			
WWWServ	3	1	3	4		4
OS_SERV	2	1	2	5		5
Gate (Gateway, Repeater)	3	1	3	3		3

The evaluation of a modified security architecture leads to the conclusion that it fully meets the requirements for information security defined by target architecture, while preserving information links required to perform system's functions.

10 NPP cybersecurity simulation for security assessment of I&C systems

The cybersecurity problem has two different dimensions; one is information, the other is technologically (physically)-oriented.

The use of integrated security model does not consider all security aspects completely. The fact that pure digital models in many practical cases are not sufficient for precise evaluation of the technological object characteristics and properties is well known [23]. The reason for that is difficulties in emulation of analogue parts of the object with discrete digital means tools or in nonlinear behaviour of the objects in specific operation modes. The solution for that the problem seems to be in development of a "hybrid" digital twin as a model for real cyber-physical system (CPS), which combines the pure digital simulation and real components [25]. The digital twin co-evolves with the real I&C system during the life cycle starting from a very high-level representation and abstract approximate model to the very detailed representation and

comprehensive, precise model. An example of a hybrid model which combines the real network equipment with hardware-in-the-loop (HIL) components of the real object is the Asherah NPP Simulator [24].

The scenarios and usage models of the digital twin also evolve during the life cycle.

A possible scenario of the digital twin application is shown in Figure 10. An assessment of the impact of an external event imposed on the digital twin is used to investigate and test the behaviour of the actual CPS without endangering the physical counterpart of the twin. Any scenario of a cyber-attack which needs accurate reproduction of a compromised control system performance or coupling dynamic effects of the plant equipment will require hybrid digital twin with HIL [24].

On the other hand, the comparison and analysis of the real data from real CPS and observation of the digital twin behaviour are able to improve estimation and prediction of the external stress consequences for the real CPS.

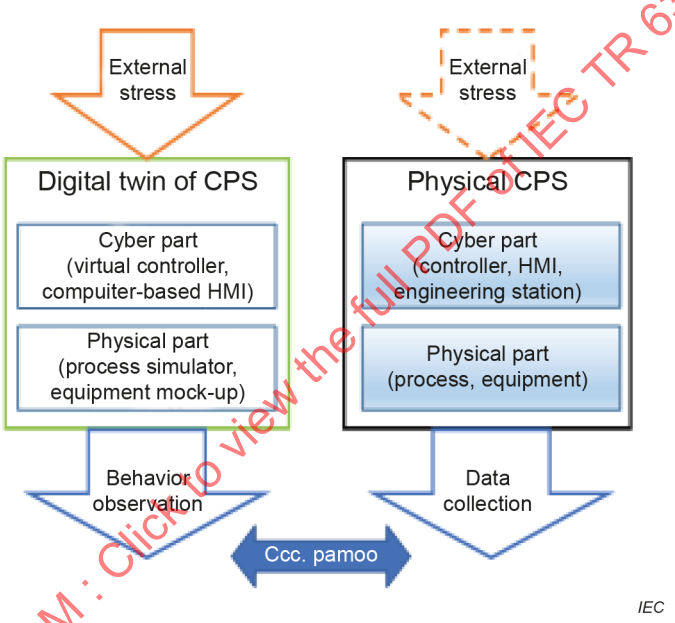


Figure 10 – General scenario of use of the digital twin for stress tests

The considered example shows a possible usage of digital twin in I&C system assessment, but the other crucial part of the assessment of any object is the estimation of object's performance and timing characteristics. The use of digital twins for cybersecurity is challenging. The main challenges are that exploitable vulnerabilities require implemented and therefore susceptible systems. Therefore, the digital twin is designed with knowledge of the implementation of the system (e.g. software, hardware, components, and networks). The problem arises not only for the analogue part of the object but also for digital (computer) components. The difficulty for the analogue part of the object is often caused by the lack of the system mathematical model, effect of the time discretization in computer model or incomplete input data for the model. The problem for the digital component is based on dependence of the model time characteristics on the performance of the components of the computational system and the load balance for software modules running on the same computer.

11 Conclusion

The solution of the problem of ensuring the secure design of the I&C system architecture for NPP is still under development. Allocating requirements as the part of a system specification does not guarantee maintaining security in an actual commissioned I&C system while there are

no strict procedure of reconciliation between security requirements and final architecture of the I&C system and implementation of the security measures.

This document presents a method of verifying the conformance between the security requirements and system architecture, if necessary, proposing changes in the system's architecture to meet the requirements.

The basis of the method is an integrated security model for NPP process control systems. The model consists of two main components: the security model describes the security requirements, and the DAC type data model describes the information exchange in the I&C system, respectively.

The realization of the integrated model provides the procedures for:

- asset classification,
- a mapping between data and security models,
- assigning security barrier measures between assets.

The procedures can be used for verification and design of the I&C system's architecture that meets security requirements.

It is worth mentioning that reconciliation of models (synthesis of the architecture) is, generally speaking, an ill-posed problem at least because the number of assets is usually greater than the number of degrees, and the systems differing in both asset number and relations between the assets conform to the same model of access rules. Sometimes it occurs that the security architecture synthesis problem for a system and given security requirements does not have a solution.

Still, the integrated model, being a purely abstract approach, does not entirely solve the security problem for the I&C system. For example, it does not take into account the dynamic behaviour of the system or unsatisfactory implementation of the security measures that could make the system vulnerable. For the final stage of verification and assessment of the cybersecurity, it is necessary to use a full-size simulator of the system or digital twin of the system with elements of a real system.

Annex A
(informative)

Data model

Let us represent an information model of a system as a graph (security graph) reflecting the real (physical) matter of the described I&C system. The properties of a graph of that sort are shown in Table A.1. Denote a security graph as $G = G(X,E)$ where X is the set of vertices, E is the set of edges.

The model works with the discrete model of rule propagation also known as the “take-grant” model [17]. It uses the graph theory to describe access relations between subjects and objects during performing their functions. The variant of the “take-grant” model considered in this technical report is based on the approach described in [18]: in the frame of the model the security graph is a finite labelled directed weighted multigraph describing the system properties.

Table A.1 shows the correspondence between the properties of the I&C system and security graph in DM. Some properties seem evident, but they are still presented in the table for clarity.

Table A.1 – Correspondence of the physical properties of I&C systems with the properties of the security graph

Physical property of the system	Property of the graph
The processes of information transfer has a source and a recipient.	The graph is directed.
There are different types of assets (active and passive).	The vertices can correspond to both objects and subjects, therefore, in the general case, the vertices are coloured.
There are different types of relationships between assets.	Edges can be of different types, for example: transfer of rights to control an object, transfer of information between assets, receipt of control commands. Therefore, the edges of the graph are generally coloured.
In the general case, I&C system is a hierarchical system. It has various layers like operators, subsystems, elements of subsystems: computers, equipment controllers, separate processes, files, etc. in computers.	There is a subset of vertices in the graph where an order relation can be established.
The presence of security barriers to the transmission of information (software and hardware firewalls, data diodes etc.) in the I&C system	The graph, generally speaking, is not transitive, i.e. the existence of an order relation between the vertices does not mean that these vertices are connected by an edge.
I&C system contains a finite number of elements.	A graph is finite.
Duality, symmetry of relations between assets.	The model supports a graph with cycles.
In the general case, the I&C system can be changed as a result of repair, modification or reconfiguration.	The graph is dynamically updated.

Two types of vertices are presented in the graph: the first corresponds to subjects, the second corresponds to objects.

An edge directed from the vertex a_1 to the vertex a_2 shows that a_1 has a right (or rights) on a_2. Normally the following rights are considered as typical ones: read (r), write (w) (with regard to information transfer), take (t), grant (g) (with regard to right transfer). Relations dealing with access rights transfer $\mathcal{R} = \{r_1, r_2, \ldots, r_n\} \cup \{t, g\}$ are commonly called “de jure” relations, while $\mathcal{R} = \{r_1, r_2, \ldots, r_n\} \cup \{w, r\}$ are called “de facto” relations. To describe information transfer the model introduces a number of atomic transformations (Post, Pass, Spy, Find) as well as graph

modifications: adding and removing vertices and edges (Create, Delete). The advantage of the “take-grant” model is its computational efficiency [11].

The initial security graph G_0 determined in the frame of a formal security model can be transformed to a new graph G' by successive applications of the elementary rules (the transformation is designated as $G_0 \mid\!\rightarrow G'$). The cybersecurity system is considered in the context of the possibility that a subject can obtain access rights to a certain object (initially the subject does not have the rights) after a co-operation of subjects by successive system state change by the execution of elementary commands. Situations of authorized (i.e. “legal”) acquisition of the access rights as well as “stealing” the rights are considered.

The publication [17] states the conditions under which a subject can get access $\boldsymbol{e} \in \{\boldsymbol{r}, \boldsymbol{w}, \boldsymbol{t},\}$ to an asset with the aforementioned set of the access rights and elementary rules of the graph transformation.

In the TR, the main attention is paid to the application of the discretionary model to the analysis of information security properties associated with the transfer in the form of reading and writing information between assets in a system (de facto relationships), rather than the rights to it (de jure relations).

In the standard "take – grant" model all operations between the subjects [13] are inversely symmetrical operations. The conjugate second part of such symmetrical relationships is called implicit relationships. In this model, the information can be obtained in two ways: either if the subject a_1 who is interested in the information contained in subject a_2, has a relationship of type r with the a_2 or if the a_2 has a relationship w with the a_1.

Implicit writing means that if the subject a_1 has a reading-to-subject relationship with a_2, then reading information from a_2, can be considered as transmitting (writing) information from a_2 to a_1. Implicit reading is somewhat the same but more abstract. Let us illustrate it with the following example: imagine that an asset a_2 does not contain any information before a_1 writing to it. After the writing to a_2 is completed, it will contain only the information that has been transmitted to it from a_1, since a_1 obviously knows that the info was transmitted, consequently, a_1 will have full knowledge of the information in a_2, as if it read it.

Sometimes it would be useful to break this feature, the rationale for this step will be given below. Let us introduce an extension of the standard model with a new type of relationship with antisymmetric transmission of information. In this extended model, the edges r, w in the access graph belong to one of two types: simple information transfer $\mapsto$, and antisymmetric information transfer $\rightharpoonup$, respectively.

We will call the read ($\frac{r}{\mid\!\rightarrow}$)and write ($\frac{w}{\mid\!\rightarrow}$) relations antisymmetric if $a_1 \frac{w/r}{\mid\!\rightarrow} a_2 \not\Rightarrow a_2 \frac{r/w}{\mid\!\rightarrow} a_1$, in other words, if the write/read operation from a_1 to a_2 does not lead to the ability to read/write a_2 from a_1, such relations will be denoted by $\rightharpoonup$.

The entry $a \mid\!\rightarrow b$ means simple information transfer from the asset a to the asset b.

The entry $a \rightharpoonup b$ means secure information transfer from the asset a to the asset b. In that case transfer of information between assets a and b belonging to different security degrees $L^a < L^b$ does not violate integrity of the asset b.

An example of a secure transmission is the replacement of data writing to b by the asset a by data reading from a by the asset b, provided that some actions are taken to destroy the symmetry of r and w operations.

NOTE $a \multimap b \not\Rightarrow a \mid\!\!\rightarrow b$, and vice versa, $a \mid\!\!\rightarrow b \Rightarrow a \multimap b$, $L^a > L^b$, and $a \mid\!\!\rightarrow b \not\Rightarrow a \multimap b$, $L^a \leq L^b$.

Annex B
(informative)

Security model definition (SLM)

Access rules model is defined as a collection of classes (degrees of cybersecurity) and relations between them and rules governing asset attribution to a degree:

$SLM = \langle SC, \otimes, \rightarrow, \nrightarrow \rangle$, where:

SC is a finite linearly ordered set of security degrees consisting of N_{SC} elements.

Let us define that secure information transfer means that there are some security barriers on the information path between security degrees. If there are no barriers on the information path we will call it simple information transfer.

Let us introduce the following notations:

- $\rightarrow$ is the relationship defined on a pair of security degrees; for any two degrees L_1 and L_2 : $L_1 \rightarrow L_2$ means that information could pass in a simple way from L_1 to L_2 (subscript is the sequence number of a degree).
- $\nrightarrow$ is the relationship defined on a pair of security degrees; for any two degrees L_1 и L_2: $L_2 \nrightarrow L_1$ means that information passes securely from L_2 to L_1.

Note that the secure information transfer in this work will be understood in that sense that the information on the transmission path has certain security controls in act. The security controls prevent the violation of the normal system operation. If the information received was determined to be harmful for the I&C system it ought to be discarded. We do not specify the exact security controls, as it depends on the implementation of the real I&C system.

- The direction of transmission of “secure information” in the model SLM is indicated $L_n \nrightarrow L_m, n \geq m.$
- $\otimes$ is the grouping operator.

Paper [10] shows that elements $SC, , \vee \nrightarrow$ compose a lattice of security degrees. It is convenient to depict the lattice as directed acyclic graphs $G_{SLM} = \langle SC, E \rangle, E = \{e_1, e_2, \ldots, e_n\} \cup \{, \nrightarrow\}$.

Definition 1: The security degree L is a set of vertices of a security graph G, such that for every pair of the vertices in the set $a_i \in$ A , $a_j \in$ A, i ≠ j $L_l(a_i) = L_l(a_j), l = const \in SC$.

The $L_n(a_i)$, means that the asset $a_i \in$ A belongs to a particular security degree n, $a_i \in$ A. The security degree is defined on a certain type of relationship $\mathcal{R}$.

Definition 2: Security zone S is a set of vertices of a security graph G, for every pair of vertices in the set $a_i \in$ A , $a_j \in$ A, i ≠ j $\exists G', a_i \mid\!\rightarrow a_j, a_j \mid\!\rightarrow a_i$.

The $S_n(a_i)$ means that the asset $a_i \in$ A belongs to a particular security zone n, $a_i \in$ A. The security zone is defined on a certain type of relationship $\mathcal{R}$.

NOTE The presented security zone definition clarifies the term "security zone" as defined by IEC 62645:2019 Clause 3.2.

Annex C
(informative)

Justification of the secure by design principle

The symmetry of de facto relations in the DAC model leads to the fact that it is impossible to organize the exchange of information between assets without violating the integrity of receiver asset or writing data without violating confidentiality on source assets (Biba model and Bell–LaPadula model, respectively, [8],[9]) if only subjects take part in the process of information transfer.

In some cases, this restriction can be circumvented by introducing asymmetric relations or using intermediate objects in the path. Further in this annex, we will carry out the discussion within the framework of the Biba model, since in general the security of I&C systems is aimed at maintaining integrity rather than confidentiality (see, for example, 5.2 of IEC TS 62443-1-1:2009 [21] for reason and justification).

An analysis of the Bell–LaPadula model can be carried out in a similar way, with the replacement of integrity by confidentiality and write to read.

The Biba model determines that an access graph is safe if an asset with a lower security degree cannot write to an asset with a higher security degree and change information in it.

Accordingly, if we need to maintain the integrity of assets located at the upper security degree, then in the model, it is necessary to allow only relationships by write with asset on the lower degree. However, in real I&C systems, often there is also a reverse flow when it is necessary to transfer information between assets from bottom to top (diagnostic signals, confirmations, etc.). To indicate such information in the model, we introduced a relation of “secure transfer” of the information (see Annex A and Annex B). To understand the practical meaning of the introduced relationship, it is necessary to discuss the meaning of the term “integrity”. Historically, the most commonly used definition of integrity in the context of industrial control systems is the definition given in IEC TS 62443-1-1 [21]. The technical specification has two definitions of the integrity:

The first of them is: “data integrity property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner”. This definition, similar to the approach of the ISO 27000 standard [29], narrows the security problem to the issue of data integrity in information systems. This assumption is reasonable for systems whose main function is the storage and processing of data.

For control systems of physical objects, the main function is to control the object itself. It is advisable to extend the concept of integrity to equipment and methods. In this form, this term is interpreted in the second definition in IEC TS 62443-1-1 and more precisely in IEC 62443-3-3 [14]: “property of protecting the accuracy and completeness of assets”.

Unlike the definition of “data integrity” IEC TS 62443-1-1, a definition of this kind extends the concept of integrity to tangible assets, including their protective mechanisms and data processing methods, which, unlike the data themselves, are internal properties of the protected system, which allows the owner of the I&C system to implement effective security measures to preserve the integrity of methods. In this context simple data corruption is not critical, if it does not violate the critical properties of the object.

The main property of I&C systems is the system ability to perform its functions to control the industrial objects. Suppose, for example, that a system receives corrupted data from a compromised asset and as a result of this an incorrect control command is generated, but the system remains in a physically safe state. Then, basically, from safety point of view this incident might be considered as insignificant violation of information integrity. In the definition of “secure

information” the word “secure” is interpreted as information the processing of which does not lead to a breach of the safety of the NPP.

Therefore, in this "narrow" sense, information is considered "secure" if it does not violate the integrity of the destination asset. The term integrity is interpreted in the above sense.

An example of the secure transfer of information is the replacement of a write of information by asset a into asset b with a read operation by asset b from asset a, i.e. replacement of the transfer initiator, provided that measures are taken to ensure that the symmetry of the r and w operations becomes broken with respect to the required cybersecurity property.

Extending the take-grant model with asymmetrical de-facto relationships allows us to simulate cases of secure information transfer, provided that the priority is to maintain integrity in a real system, when in addition to the main “direct” flow of commands between assets at different security degrees in the “top to bottom” direction additional there are "reverse" data streams in the form of diagnostic information, acknowledgment signals, and so on.

We provide a rule connecting the types of relationship $\nrightarrow$ and $\rightharpoonup$ in models SLM and DM, respectively.

Rule: The secure information transfer between security degrees $L_n \nrightarrow L_m, n \le m$ is organized using asymmetric access in security graph G', $G_0 \vdash\!\!\rightarrow G'$, $\forall a_i \in L_n$, $\forall a_j \in L_m$, $a_i, a_j \in A$ and $a_i \rightharpoonup a_j$, or a_i, a_j are not connected.

Annex D
(informative)

Mapping of security and data model

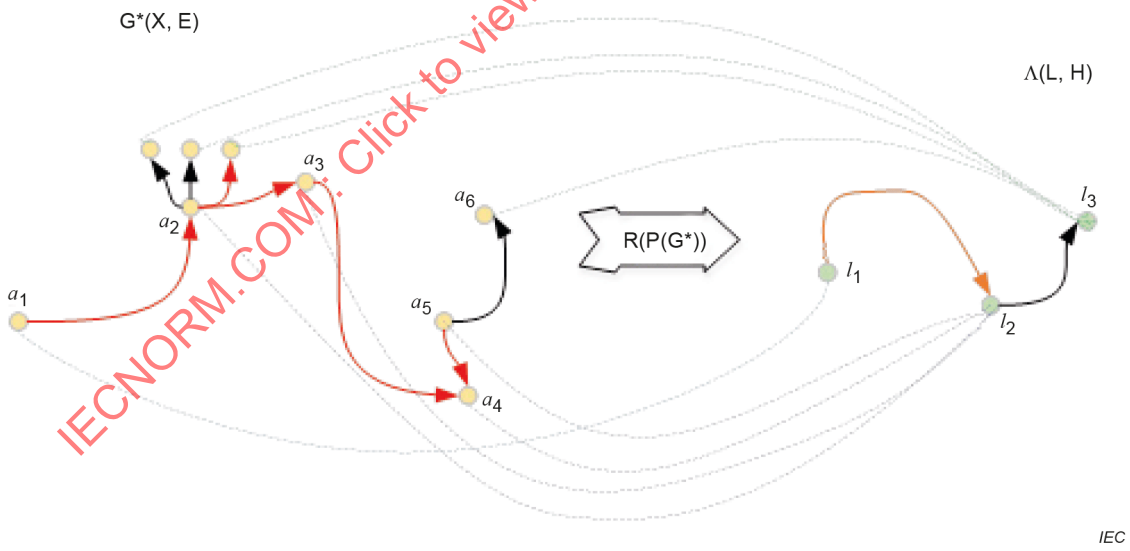
To simplify asset ranking reasoning, suppose that the set of security graphs G^* contains a graph G_i which is, at least weakly connected; that is, there are no isolated islands in the graph. Let us introduce an ordering function on vertices of G^*:

$P\left(G^*\right)=\{X: x_1,\ldots,x_M\}$, $M \le M_A$, where M_A is number of assets. Then let us introduce the operator R performing the transformation

$$R\left(P\left(G^*\right)\right)=\Lambda(l,D).$$

Here $\Lambda(l,D)$ is a directed graph; M vertices of the graph correspond to the points of the set $\{X\}$.

The example shown in Figure D.1 illustrates the rule of link transformation for the mapping from G* to Λ. Let the ordering function groups vertices of graph G* into three degrees, and R maps G* to the graph Λ with three vertices. Here the vertex a1 maps to l1, and vertices a2, a3, a4, a5 map to l2. Since all the links between {a1} and {a2, a3, a4, a5} are secure then (l1,l2) is a secure link, too. On the other hand, since there is a simple information transfer (a5, a6) then the arc (l2, l3) is simple.



Red and orange arrows mean secure information transfer, black arrows mean “common” information transfer.

Figure D.1 – Sketch of link transformation

Now we provide a rigorous description of the transformation rule.

Let us name vertices of graph G* that are mapped to the related vertices {L} of graph as “original vertices”: a1 is the original vertex for l1; a2, a3, a4, a5 are the original vertices for the vertex l2 etc. Now we define the following rule(s): if information between all “original” vertices is transferred securely then the related arc in graph L represents secure information transfer. And

conversely, if there is at least one arc of simple information transfer between “original” vertices then the related arc in the graph L represents simple information transfer.

Denote the sets of all assets that go to the vertices l_k and l_m of the graph Λ as $A_k \subset A$ and $A_m \subset A$ respectively. Then the rules of edge composition are:

- if $\exists a_i \in A_k$ and $a_j \in A_m : (a_i a_j) \in \mapsto (A)$ and $P(a_i) \neq P(a_j)$, then $(l_k l_m) \in$
- if $\forall \ a_i \in A_k$ and $a_j \in A_m : k \neq m, (a_i a_j) \notin \varnothing$ the condition $(a_i a_j) \in \rightarrow$ is valid, then the edge $(l_k l_m)$ of the graph Λ exists and also $(l_k l_m) \in \nrightarrow$

If G^* breaks down to a few domains of connectivity (see an example in Figure G.3) then:

$R(P(G^*)) = \bigcup_i R(P(G^{*i}))$, where G^{*i} are the domains of connectivity.

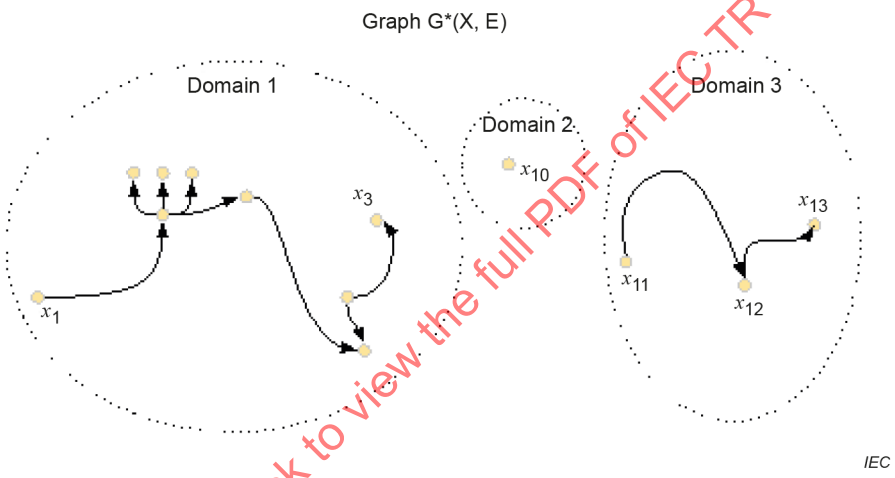


Figure D.2 – Example of domains of connectivity in a graph – Here the graph splits into three domains

Let us define an operation of degree grouping, $\oplus$, that shrinks the graph $\Lambda(l, D)$ to a graph $\Lambda'(l', D')$ whose number of vertices does not exceed N_{SC}.

The ranking (degree) of the new vertex derived as an aggregation of vertices $l_1, l_2, \ldots, l_n$ is given by the expression $L = L^{l1} \oplus L^{l2} \oplus \ L^{l3} \ldots L^{ln}$ = inf($\{L^{l1}, L^{l2}, L^{l3} \ldots, L^{ln}\}$) and

Edges of the graph $\Lambda'(l', D')$ are generated according to the rule:

- If all $l_k \overset{\oplus}{\rightarrow} l'_q$ and $l_m \overset{\oplus}{\rightarrow} l'_p$, where $l'_q \neq l'_p$ and $(l_k, l_m) \notin \varnothing$ fulfill the condition: $(l_k l_m) \in \nrightarrow$, then the edge $(l'_p, l'_q) \notin \varnothing$ and $(l'_p, l'_q) \notin \nrightarrow$.
- If there are some $l_k \overset{\oplus}{\rightarrow} l'_q$ and $l_m \overset{\oplus}{\rightarrow} l'_p$, where $l'_q \neq l'_p$ and $(l_k, l_m) \notin \varnothing$ for which $(l_k l_m) \in$, then the edge $(l'_p, l'_q) \notin \varnothing$ and $(l'_p, l'_q) \notin \rightarrow$.

Let us have some two models SLM and DM. The operator $\mathrm{R}\left(P\left(G^{*}\right)\right)$ performs mapping (surjection) of graph G^{*} vertices onto a set of graph $\Lambda(l,D)$ vertices.

The sufficient condition that a DM model corresponds to a SLM is: if the graph obtained by mapping $\mathrm{R}\left(P\left(G^{*}\right)\right)$ is isomorphic, after applying the grouping operator $\oplus$, to a minor G_{SLM}^{m} of the graph G_{SLM}, i.e. $\Lambda(l,D)\overset{\oplus}{\rightarrow}\Lambda'(l',D')\simeq G_{SLM}^{m}$, then the DM model corresponds to the SLM.

The proof follows from the definitions of the functions P and operators $\mathrm{R}\left(P\left(G^{*}\right)\right)$ and $\oplus$, and as well from the above definition of cybersecurity for the ICM model.

In practice, the sufficient condition corresponds to the following statement: if we have a designed system then the information access rules between different degrees ought not to be violated after the degree assignment to assets.

NOTE Additional conditions can be imposed on $\mathrm{R}\left(P\left(G^{*}\right)\right)$ and G_{SLM}. For example, for nuclear safety ensuring direct transfer of any information between assets whose nuclear security classes differ by more than one; a similar approach is used for information exchange between assets classified by security degrees that imposes restrictions on adjoined assets in G^{*}.

Annex E
(informative)

Formal approach to asset clustering and classification

E.1 Input data types and the choice of data representation for the analysis

We propose using the “asset–attribute” table to specify the relations between attributes and assets. According to this method, assets are identified, the attribute values and measurement scales are determined for the choice of the data representation. Different types of scales are used for the attribute description: rank scale (dealing with ranks), quantitative scale (applied to measurable properties), nominal scale (applied to qualitative properties)

The number of attributes can be arbitrary but here, for clarity, we provide an example with three attributes:

a) Nuclear safety (NS) class of the object (from 1 to 3) to which the asset belongs. The nuclear safety class assigned to a system appreciably determines the system’s importance because the class is unequivocally related to the damage due to the system failure. To assign the attribute we use the rank scale reduced to a quantitative one with the ordering function $R_1(x) = \{1,2,3,4\}$ (1, 2 and 3 are for the 1st, 2nd and 3rd safety classes respectively, and 4 is for unclassified assets).

b) A functional property (or properties) of the asset (the asset is considered as a “gray box” having some intrinsic properties).The properties could include, for example, physical links and dependencies, power, water, spatial, environmental, etc. For further calculations the property is to be reduced to a qualitative kind with the ordering function $R_2(x) = \{0,1,2,3,\ldots\}$;

c) Asset informational properties (see Clause 7.6) are the attributes presenting information links of an asset with other assets.

Note: All formulae and reasoning in this clause are applicable to the arbitrary number of attributes.

Asset cybersecurity information properties are mostly determined by the impact on the system in case of violation of confidentiality, integrity and availability of the information associated with the asset. The classical approach for information property estimation is expert ranking technique bringing them to fixed degrees [14]. We consider an analytical way to quantify the attributes.

We will consider the integrity only because according to the common approach [5] I&C systems focus on securing the integrity.

The table of properties are presented in Table E.1.

Table E.1 – NPP I&C asset properties

Asset	NS Class	Functional property (properties)	Asset informational property

E.2 Order relation on a security graph

The existence of an order relation on a subset of vertices implies that we can introduce an order function $R(x)$ on this subset. The value of asset order function can be used as a quantitative characteristic of asset informational properties.