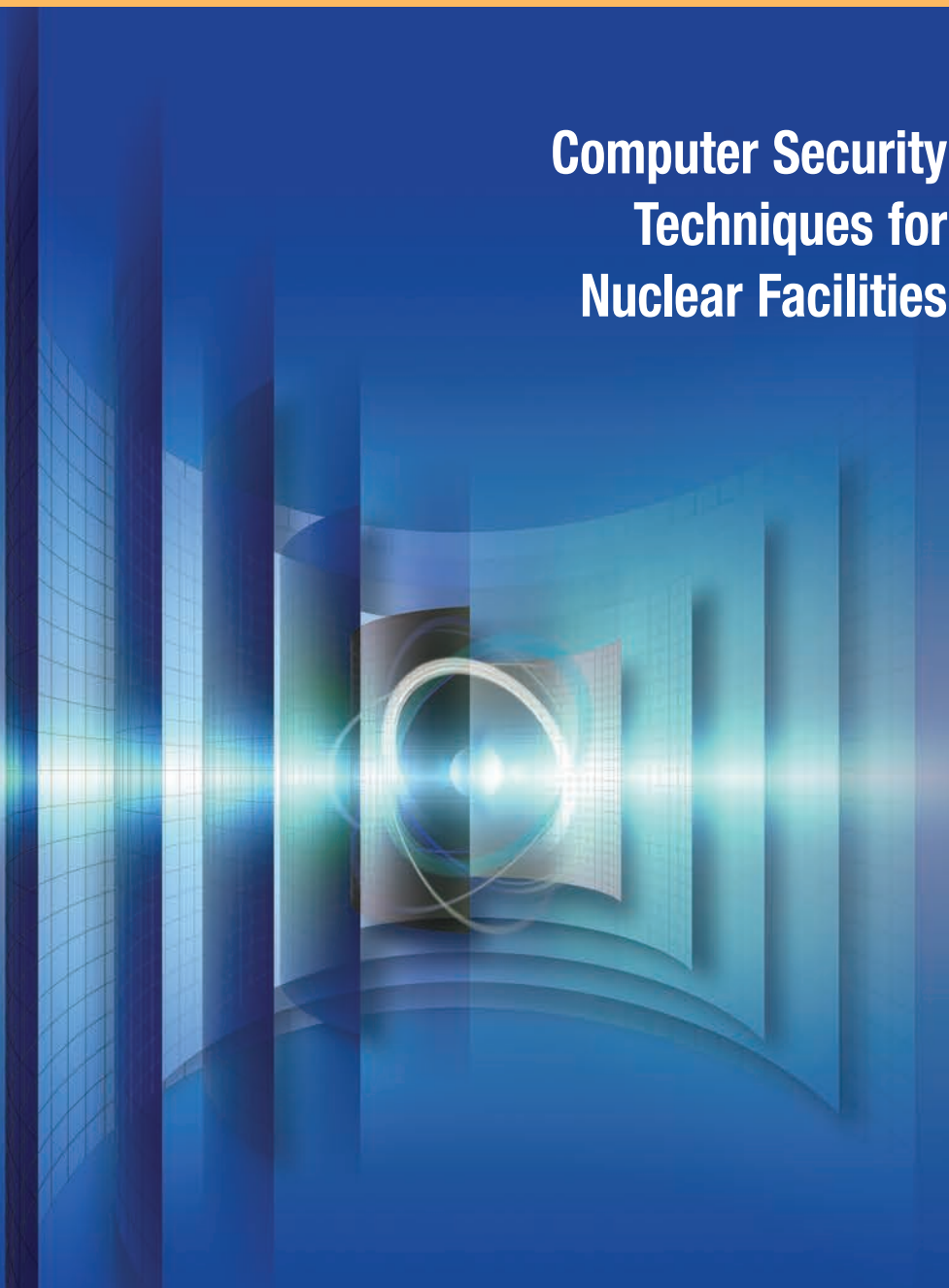
IAEA Nuclear Security Series No. 17-T (Rev. 1)

Technical Guidance

Computer Security Techniques for Nuclear Facilities



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

NUCLEAR SECURITY SERIES No. 17-T (Rev. 1)

COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
September 2021
STI/PUB/1921

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Computer security techniques for nuclear facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 17-T (Rev. 1) | Includes bibliographical references.
Identifiers: IAEAL 21-01393 | ISBN 978–92–0–123520–6 (paperback : alk. paper) | ISBN 978–92–0–123620–3 (pdf) | ISBN 978–92–0–123720–0 (epub)
Subjects: LCSH: Computer networks — Security measures. | Nuclear facilities — Security measures. | Computer security.
Classification: UDC 621.039:004.056 | STI/PUB/1921

FOREWORD

by Rafael Mariano Grossi
Director General

The IAEA Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The IAEA establishes and maintains this guidance as part of its central role in providing nuclear security related international support and coordination.

The IAEA Nuclear Security Series was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States. As Director General, I am committed to ensuring that the IAEA maintains and improves upon this integrated, comprehensive and consistent set of up to date, user friendly and fit for purpose security guidance publications of high quality. The proper application of this guidance in the use of nuclear science and technology should offer a high level of nuclear security and provide the confidence necessary to allow for the ongoing use of nuclear technology for the benefit of all.

Nuclear security is a national responsibility. The IAEA Nuclear Security Series complements international legal instruments on nuclear security and serves as a global reference to help parties meet their obligations. While the security guidance is not legally binding on Member States, it is widely applied. It has become an indispensable reference point and a common denominator for the vast majority of Member States that have adopted this guidance for use in national regulations to enhance nuclear security in nuclear power generation, research reactors and fuel cycle facilities as well as in nuclear applications in medicine, industry, agriculture and research.

The guidance provided in the IAEA Nuclear Security Series is based on the practical experience of its Member States and produced through international consensus. The involvement of the members of the Nuclear Security Guidance Committee and others is particularly important, and I am grateful to all those who contribute their knowledge and expertise to this endeavour.

The IAEA also uses the guidance in the IAEA Nuclear Security Series when it assists Member States through its review missions and advisory services. This helps Member States in the application of this guidance and enables valuable experience and insight to be shared. Feedback from these missions and services, and lessons identified from events and experience in the use and application of security guidance, are taken into account during their periodic revision.

I believe the guidance provided in the IAEA Nuclear Security Series and its application make an invaluable contribution to ensuring a high level of nuclear security in the use of nuclear technology. I encourage all Member States to promote and apply this guidance, and to work with the IAEA to uphold its quality now and in the future.

EDITORAL NOTE

This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Nuclear security seeks to prevent, detect and respond to criminal or intentional unauthorized acts involving or directed at nuclear and other radioactive material, associated facilities and associated activities. Nuclear security of nuclear material and nuclear facilities includes physical protection, personnel related security (e.g. trustworthiness determination, measures against insider threats) and information security.

1.2. Groups or individuals planning or committing any malicious act involving nuclear material or a nuclear facility might benefit from access to sensitive information and sensitive information assets related to the material, the facility or the security measures in place.

1.3. The Nuclear Security Fundamentals [1] and the three Nuclear Security Recommendations publications [2–4] all emphasize the importance of securing sensitive information. IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [5], provides guidance on appropriate measures for the identification, classification and securing of sensitive information to achieve effective information security within the State's nuclear security regime.

1.4. Cyber-attacks at nuclear facilities can contribute to causing physical damage to the facility and/or disabling its security or safety systems (i.e. sabotage), to obtaining unauthorized access to sensitive nuclear information, or to achieving unauthorized removal of nuclear material. Computer security is therefore vital at nuclear facilities to protect both nuclear security and nuclear safety.

1.5. The protection of sensitive digital assets[1] (SDAs) is recommended in para. 4.10 of Ref. [2], which states:

> "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*."

[1] Sensitive digital assets are sensitive information assets that are (or are parts of) computer based systems.

The specific need for protection of computer based systems from insider threats is recognized in Ref. [6].

1.6. General guidance on computer security for nuclear security is provided in IAEA Nuclear Security Series No. 42-G, Computer Security for Nuclear Security [7], and more specific guidance on computer security of instrumentation and control (I&C) systems in nuclear facilities is provided in IAEA Nuclear Security Series No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [8]. The current publication is intended to complement this guidance by providing details of computer security techniques for other systems at nuclear facilities.

OBJECTIVE

1.7. The objective of this publication is to assist Member States in implementing computer security at nuclear facilities with the aim of preventing and protecting against unauthorized removal of nuclear material, sabotage of nuclear facilities and unauthorized access to sensitive nuclear information. This publication addresses computer security for supporting activities and organizations such as vendors, contractors and suppliers. While the focus of this publication is on the security of nuclear facilities, application of this guidance may also benefit facility safety and operational performance.

1.8. This publication addresses the use of risk informed approaches to establish and enhance computer security policies, programmes and measures to protect SDAs and other digital assets. A nuclear facility relies on SDAs and other digital assets for the safety and security of the facility. This publication describes the integration of computer security into the management system of a facility or organization, and it includes guidance on defining policy and requirements and on activities to develop, implement, sustain, maintain, assess and continually improve the computer security measures that protect the facility from cyber-attacks consistent with the threat assessment or design basis threat (DBT) [9].

1.9. This publication also provides technical guidance on protecting other digital assets at nuclear facilities.

1.10. This publication is intended for regulatory bodies and other competent authorities and for operators of nuclear facilities and their vendors, contractors and suppliers.

SCOPE

1.11. The guidance in this publication applies to the implementation and management of computer security for nuclear security purposes at nuclear facilities. This publication is applicable to all stages in the lifetime of a nuclear facility [10].

1.12. Computer security at nuclear facilities is intended to protect a range of systems that contribute to different aspects of nuclear security, such as physical protection and nuclear material accounting and control systems. This publication does not address the design or operation of such systems, except as design or operation relates to the protection of those systems by computer security measures.

1.13. This publication addresses all digital assets associated with a nuclear facility, including the facility's I&C systems. Additional guidance on specific computer security considerations for the facility's I&C systems that provide safety, security or auxiliary functions is provided in Ref. [8].

STRUCTURE

1.14. Following this introduction, Section 2 introduces key terminology, basic concepts and relationships. Section 3 describes general considerations for computer security in nuclear facilities. Sections 4 and 5 present guidance on computer security risk management (CSRM) at the facility and system levels, respectively. Section 6 presents guidance on considerations for facility and system CSRM relevant to different stages in the lifetime of the facility. Section 7 presents an overview of a computer security programme (CSP). Section 8 presents an illustrative example of the implementation of defensive computer security architecture (DCSA) and associated computer security measures.

1.15. The Appendix provides specific guidance on selected elements of a CSP. Annex I provides example attack scenarios that can be used to evaluate computer security at nuclear facilities. Annex II provides an example of the assignment of computer security levels for a nuclear power plant. Annex III provides an example of the application of computer security levels and zones.

2. BASIC CONCEPTS AND RELATIONSHIPS

2.1. This section clarifies the meaning of important terms that are used throughout this publication.

NUCLEAR SECURITY AND COMPUTER SECURITY

2.2. The Nuclear Security Fundamentals [1] state that the targets with respect to nuclear security are the following:

> "*Nuclear material*, *other radioactive material*, *associated facilities*, *associated activities*, or other locations or objects of potential exploitation by a *nuclear security threat*, including *major public events*, *strategic locations*, *sensitive information*, and *sensitive information assets*."

As well as information stored on SDAs, sensitive information includes software on such SDAs, including run time software, embedded firmware, development tools, testing tools, maintenance tool software and operating systems.

2.3. Reference [1] states that a nuclear security system is "An integrated set of *nuclear security measures*." Nuclear security measures are defined as follows:

> "Measures intended to prevent a *nuclear security threat* from completing criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities*, or *associated activities* or to detect or respond to *nuclear security events*" [1].

2.4. The general guidance on computer security [7] states: "The State should develop and maintain a national computer security strategy as part of its nuclear security regime". As nuclear facilities are within the nuclear security regime, computer security at these facilities needs to be included in that national computer security strategy. Facility functions that support safety and security need to be protected from adversaries. When these facility functions make use of, depend on or are supported by digital technologies, computer security is needed to protect these functions.

2.5. Computer security is concerned with computer based systems, especially those systems that perform or support facility functions important or related to nuclear security and nuclear safety (i.e. digital assets). Computer security provides

techniques and tools to defend against cyber-attacks and against human actions or omissions that might affect security.

Facility functions, computer security levels and computer security zones

2.6. A standard approach to protect systems in a structured way according to a graded approach is to use the concepts of computer security levels and computer security zones. The computer security level assigned to a computer security zone is based on the highest degree of security protection required by any facility function performed by a system within that zone. The same computer security level is assigned to all systems within that zone. Typically, a nuclear facility zone model consists of many different zones, and several zones may have the same computer security level assigned.

2.7. A facility function is a coordinated set of actions and processes that need to be performed at a nuclear facility. Facility functions include functions that are important or related to nuclear security and functions that are important or related to nuclear safety (i.e. safety functions).[2] Facility functions are assigned to systems[3], each of which performs one or more of these functions.

2.8. A computer security level is a designation that indicates the degree of security protection required for a facility function and consequently for the system that performs that function. Each computer security level is associated with a set of requirements imposed by the operator to ensure that the appropriate level of protection is provided to digital assets assigned to that level using a graded approach. Each computer security level will need different sets of computer security measures to satisfy the computer security requirements for that level.

2.9. 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). The use of computer security zones is intended to simplify the administration, communication and application of computer security measures.[4]

---

[2] Facility functions also include operational and administrative (or organizational) functions.

[3] Systems may be on-site, off-site or cloud based.

[4] The concept of computer security zones may be applied to existing facilities and legacy facilities as well as to new designs.

2.10. Additional criteria for defining computer security zones may include the following:

(a) Organizational responsibilities, for example different computer security zones for systems that are the responsibility of different departments;
(b) The need to maintain separation, for example different computer security zones for redundant systems at the same computer security level performing the same facility function;
(c) Zones already defined for other purposes, for example a computer security zone defined for simplicity to be the same as a zone already established for administrative or communication purposes.

2.11. The idealized relationships between the concepts of facility function(s), computer security level(s), system(s) and computer security zone(s) are illustrated in Fig. 1.

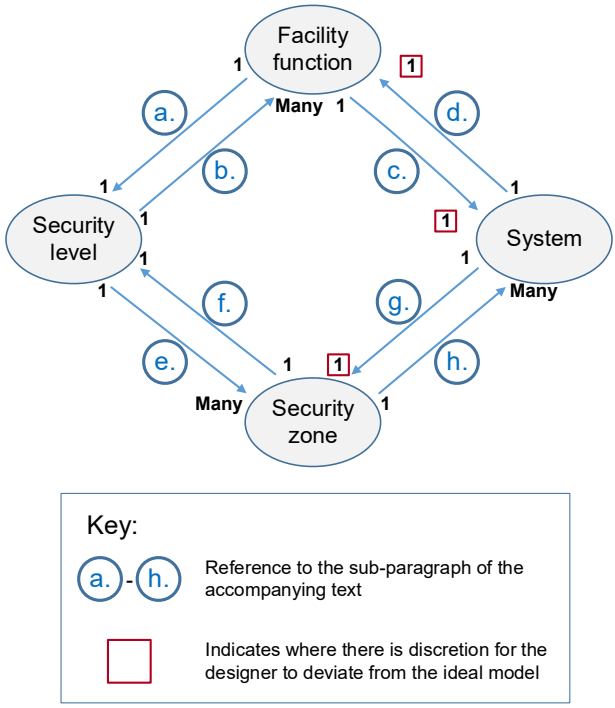


FIG. 1. Idealized relationships between facility function, computer security level, system and computer security zone.

2.12. Each of the idealized relationships is labelled in Fig. 1, and the labelled text below describes each relationship:

(a) Each facility function is assigned to a single computer security level.
(b) Each computer security level may be applied to one or more facility functions.
(c) Each facility function is ideally assigned to one system, where possible.[5]
(d) Each system ideally performs one facility function, where possible.[6]
(e) Each computer security level may be applied to one or more security zones.
(f) Each computer security zone is assigned a single computer security level.
(g) Each system is placed within a single computer security zone, where possible.[7]
(h) Each computer security zone may consist of one or more systems.

Computer security risk management

2.13. Facility CSRM (see Section 4) addresses facility functions and determines the assignment of these functions to computer security levels and to one or more systems. Systems inherit the computer security levels of the functions assigned to them.

2.14. System CSRM (see Section 5) is part of facility CSRM and addresses systems and determines (a) the boundaries of computer security zones according to the facility functions performed and system connectivity as well as (b) the computer security measures to be applied to meet the requirements for the computer security level of the zone.

2.15. Outputs of risk management processes typically rely on scenario development, analysis and, in some instances, performance to increase confidence

---

[5] For example, a function may be assigned to two independent, diverse shutdown systems.

[6] For example, a human–machine interface. Ideally, from a security perspective, a single system would perform a single facility function, but designers may assign more than one facility function to a system if deemed necessary to support human, operational or safety performance.

[7] Ideally, from a security perspective, each facility function would be performed by a single system that is within a single computer security zone and therefore assigned a single security level, but designers may deviate from the ideal owing to other considerations, for example fire protection or physical protection systems that span the entire (or a significant portion of the) facility and may therefore pass through physical areas that contain zones assigned to different security levels.

in the qualitative assessments. There are two categories of scenarios: functional and technical. Functional scenarios are generally used in the facility CSRM process, and technical scenarios are used in the system CSRM process.

Competing demands of simplicity, efficiency and computer security

2.16. The competing demands of simplicity, efficiency and computer security need to be balanced when considering the following:

(a) Identification and listing of facility functions;
(b) Assignment of facility functions to systems;
(c) Development of systems;
(d) Specification of requirements for computer security for different computer security levels based on a graded approach;
(e) Establishment of logical and/or physical boundaries for computer security zones.

2.17. Considerations of simplicity might lead to a preference to assign a single function to a single system. This might result in a DCSA that allows for the tailoring of efficient computer security measures within each zone for each facility function (assuming a one-to-one relationship between systems and functions). However, the systems would need interconnections to enable integration of separated facility functions, and therefore the system of computer security levels and computer security zones might become more complex owing to the larger number of computer security zones and interconnections between these zones.

2.18. However, considerations of efficiency in the performance of facility functions by systems might lead to a preference to assign multiple functions to a single integrated system. While this might result in a smaller number of computer security zones, the complexity of the system might increase, making it difficult to apply effective computer security measures throughout these zones. Additionally, assigning to the computer security zone a computer security level appropriate for the most important function of the system might further reduce efficiency because a higher level of protection than necessary might be applied to less important functions that have been integrated into the system.

2.19. The balance between efficiency and simplicity can also include balancing the performance of facility functions through systems, with the assignment of systems to computer security zones and computer security levels. Therefore, CSRM will typically involve a number of iterations of defining computer security zones and associated computer security measures to find the optimal balance

between simplicity and efficiency. Iterations will need to show that proposed modifications of computer security zone definitions will not allow a compromise of the facility functions that would lead to worse consequences.

Conceptual nuclear facility zone model

2.20. An example of a conceptual nuclear facility zone model is shown in Fig. 2, with the following characteristics:

(a) The example facility is associated with severe consequences in the event of unauthorized removal of material or sabotage.
(b) The number of computer security levels is limited to five, with level 1 having the most stringent demands for protection and level 5 having the least.
(c) Each system is placed within a computer security zone.
(d) Each zone (including its systems) is assigned a computer security level.
(e) One or more zones may be assigned the same computer security level.

2.21. Figure 2 illustrates a conceptual application of systems, computer security levels and computer security zones. The computer security level assigned has the following impact on the requirements for the facility functions, systems and computer security zones:

(a) The higher (more stringent) computer security levels are typically required for fewer functions (and consequently applied to fewer systems) than the lower security levels. In Fig. 2, security level 1 would apply to a minimal set of critical functions each ideally assigned to a single system, whereas security level 5 would allow for a single system to have many functions assigned to it.
(b) The higher (more stringent) computer security levels are generally simpler (i.e. less complex) than the lower levels. In Fig. 2, zone Z_{1A} contains a single deterministic system whose logical and physical interactions with other zones (and systems) are minimized to the greatest extent possible, whereas zone Z_{5B} has very little restriction on interactions with other zones (and systems).
(c) The complexity of zones is typically correlated with their physical and logical size. For example, in zone Z_{1A}, the physical locations of SDAs are likely to be restricted to a vital area, whereas in zone Z_{3C}, any digital assets might be anywhere within the protected area. The increase in physical area from vital area (Z_{1A}) to protected area (Z_{3C}) potentially increases both the number of access points and the number of authorized personnel requiring physical access and therefore having the potential to interact with the digital assets.

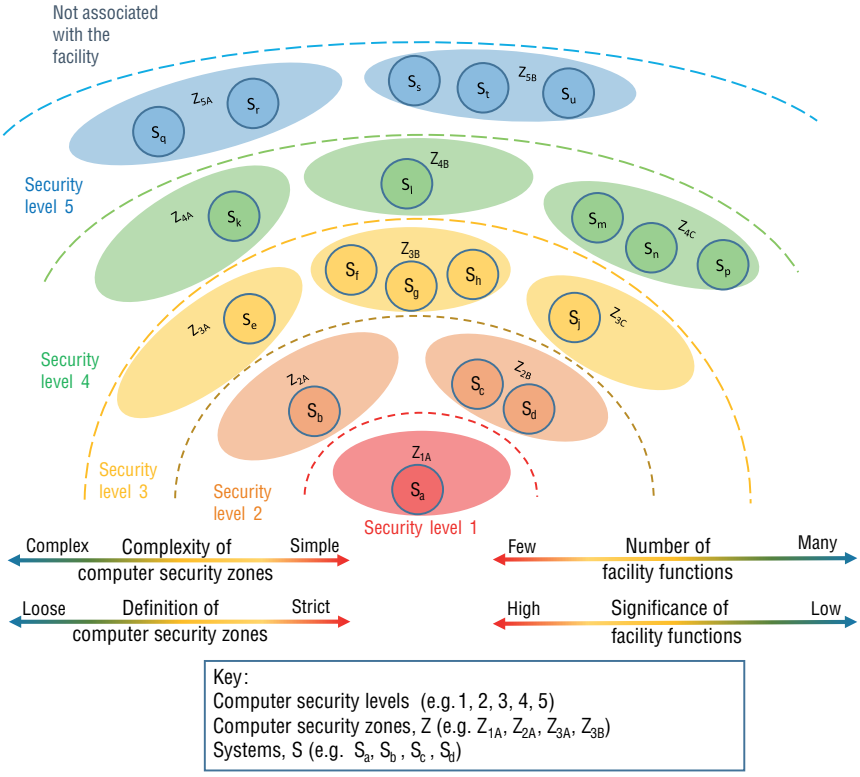


FIG. 2. Conceptual model of computer security levels and zones.

(d) The logical size of a zone may be expressed as the number of addressable, installed digital assets within a system. For example, zone Z_{3A} might be logically scoped to have a smaller number of assignable addresses for a limited capacity of digital assets, whereas zone Z_{5A} might have a broader scope with more available logical addresses for current and future digital assets.

(e) In these examples, the number of possible addressable digital assets increases in a manner similar to the example of physical zone size in para. 2.21(c). However, the installation of additional digital assets significantly affects the logical zone size but not the physical zone size.[8] This means that the number of potential logical interactions increases only when additional digital assets

[8] Typically, the physical size of a vital area will be several orders of magnitude larger than that of the digital assets located within its boundaries and is therefore not a constraint on the number of digital assets that might be potentially located within it.

are installed within a zone, thereby increasing the number and complexity of these interactions within the zone and its boundary.

2.22. The rigour with which computer security zones are defined may depend on the security levels assigned to those zones. For example, for zone Z_{1A}, both the physical and logical boundaries are strictly defined, whereas zone Z_{5A} might only need strict definition of the logical boundary, and the physical boundary might be more loosely defined (e.g. within a data centre, cloud service or corporate office).

2.23. System boundaries (logical and physical) can be useful in defining computer security zone boundaries. In practice, a zone may comprise one or more systems, each system comprising or supported by one or more digital assets to perform or support the assigned facility function.[9]

2.24. Computer security zone boundaries generally have physical access control (e.g. locked cabinets, barriers, port blockers) and decoupling mechanisms for data flow (e.g. packet filters, firewalls, data diodes) to prevent cyber-attacks or other forms of unauthorized access and to prevent errors propagating from one zone to another (especially from a zone with less stringent protection requirements to one with more stringent requirements).

2.25. The zone model provides for a graded approach and defence in depth. A cyber-attack originating outside the facility would need to defeat or bypass several layers of computer security measures before having the opportunity to compromise a system with computer security level 1, 2 or 3. The measures for computer security levels 4 and 5 can also contribute to the protection of the levels of higher protection.[10] For example, providing early detection capabilities within zones assigned security level 4 or 5 would be advantageous in providing an opportunity to contain and mitigate the cyber-attack before there is any impact on SDAs in levels 1, 2 or 3.

---

[9] Some analogue systems that perform facility functions (see para. 3.2) may require assignment to a computer security level and placement within a computer security zone. It is assumed that analogue systems are supported by digital assets, for example a digital tool for calibration of an analogue system.

[10] Some zones in Fig. 2 might be isolated, without a permanent network connection. Nevertheless, such zones with digital assets will always have some form of intermittent informational dependency — for example, updates by CD-ROM or USB — that represents an opportunity for the adversary.

COMPUTER SECURITY MEASURES

2.26. In a graded approach, the strength of computer security measures put in place to protect a facility function is in direct proportion to the potential worst case consequences of a compromise of the facility function.

2.27. Computer security measures are used for the following:

(a) To prevent, detect, delay and respond to criminal or other intentional unauthorized acts;
(b) To mitigate the consequences of such acts;
(c) To recover from the consequences of such acts.

2.28. Computer security measures may also be used for the following:

(a) To decrease the susceptibility of digital assets to malicious acts;
(b) To prevent non-malicious acts from degrading nuclear security.

2.29. Computer security measures can be assigned to one of three categories: technical control measures, physical control measures or administrative control measures (see Ref. [7]).

2.30. Computer security measures might also contribute towards or be supported by other measures implemented for physical protection, personnel related security and information security. Section 8 provides an example of the application of computer security measures within a DCSA that has five levels.

COMPUTER BASED SYSTEMS AND DIGITAL ASSETS (INCLUDING SDAs)

2.31. Computer based systems make use of, depend on or are supported by digital technologies. Computer based systems play an ever-expanding role in the performance of important facility functions at nuclear facilities and associated operations. Increasingly, computer based systems are integrated into new designs and may be introduced into existing facilities during modernization or to increase productivity or reliability.

2.32. Computer based systems are technologies that create, provide access to, compute, communicate or store digital information, or perform, provide or control services involving such information. These systems may be physical or virtual.

These systems include desktops, laptops, tablets, other personal computers, smartphones, mainframes, servers, software applications, databases, removable media, digital I&C devices, programmable logic controllers, printers, network devices, and embedded components and devices. Some computer based systems are programmable, which provides the option to modify processing steps without changing the hardware. Computer based systems are susceptible to cyber-attacks.

2.33. In the context of this publication, the term 'digital asset' refers to a computer based system that is associated with a nuclear facility. Any digital asset that has an important role in the safety or security of a nuclear facility will be considered an SDA[11].

2.34. Computer security is concerned with the protection of computer based systems against compromise.[12] Computer security is a subset of information security (as defined, for example, in ISO/IEC 27000 [11]) and shares many of the same goals, methodologies and terminology.

2.35. The relationship between information security, sensitive information, sensitive information assets, digital assets and SDAs is shown in Fig. 3.

CYBER-ATTACK

2.36. A cyber-attack is a malicious act with the intention of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible system [8]. A cyber-attack can be carried out by individuals or organizations and might target sensitive information or sensitive information assets. Cyber-attacks have the following special characteristics:

(a) They can be hidden.
(b) Their execution can be delayed, condition based or remotely initiated.
(c) Personnel (e.g. engineers, guards, operations and maintenance staff, contractors) can be deceived into unwittingly supporting the attack.

2.37. Compromise of digital assets might provide pathways for, facilitate or assist in cyber-attacks targeting SDAs, with a corresponding adverse impact on nuclear

[11] Some Member States use designations similar to SDA, such as 'critical digital assets' or 'cyber essential assets'. These terms might not be directly equivalent to SDAs.

[12] Terms such as 'IT security' and 'cyber security' are considered to be synonyms of 'computer security' and are not used in this publication.

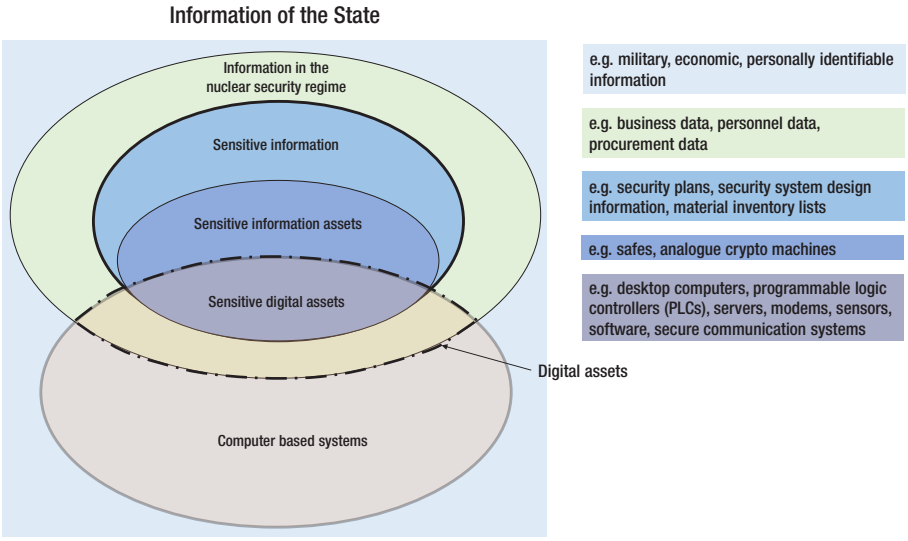


FIG. 3. Information and computer based systems in the State and in the nuclear security regime.

security and nuclear safety. Therefore, it is necessary to provide appropriate protection — based on a graded approach and defence in depth — to all digital assets associated with the facility to prevent their use in the compromise of SDAs. The compromise of an SDA degrades nuclear security and might result in a nuclear security event[13] with consequences ranging as follows (from best to worst case):

(a) No consequence;
(b) Negligible consequences;
(c) Limited consequences (including safety consequences such as an anticipated operational occurrence, and operational effects such as plant performance);
(d) Moderate consequences (e.g. degraded capabilities to prevent, detect and respond to nuclear security events);
(e) High consequences (e.g. unauthorized disclosure or loss of sensitive information);
(f) Severe consequences (e.g. unacceptable radiological consequences due to sabotage, unauthorized removal of nuclear or other radioactive material).

[13] Nuclear security events can have consequences affecting nuclear security or nuclear safety or both.

2.38. The capabilities of potential adversaries might include the effective use of cyber-attacks. Therefore, SDAs are targets both for their effect on facility functions and as a means for adversaries to facilitate and achieve their goals, and might be specifically targeted.

INTERFACE WITH SAFETY

2.39. A safety function is "A specific purpose that must be accomplished for *safety*" [12]. Safety functions are necessary "for a *facility* or *activity* to prevent or to mitigate radiological consequences of *normal operation*, *anticipated operational occurrences* and *accident conditions*" [12].

2.40. For example, the fundamental safety functions that are required for all plant states (Requirement 4 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [13]) are as follows:

(a) Control of reactivity;
(b) Removal of heat from the reactor and from the fuel store;
(c) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

2.41. Paragraph 3.46 of Ref. [2] identifies physical protection functions as detection, delay and response. Physical protection functions use defence in depth and apply a graded approach to provide appropriate effective protection.

2.42. Physical protection functions and safety functions are not necessarily inherently related to each other, making it difficult to treat safety functions and physical protection functions coherently in risk assessment methodologies. Therefore, describing and designating facility functions important or related to security in a manner similar to facility functions important or related to safety (i.e. safety functions) will simplify the determination of the significance of facility functions and will enable the equal treatment of safety functions and security functions of equivalent significance. Some examples of facility functions important to security are the following:

(a) Intrusion detection (including assessment) at a critical detection point;
(b) Control of access of persons and equipment to Category I material or vital areas;
(c) Communications to coordinate response forces during a nuclear security event.

3. GENERAL CONSIDERATIONS FOR COMPUTER SECURITY

IDENTIFICATION OF FACILITY FUNCTIONS

3.1. Reference [7] states:

> "The first step in a systematic process [for applying computer security measures for nuclear security] should be to identify the functions that directly support one or more aspects of nuclear security (e.g. physical protection, nuclear material accounting and control and sensitive information management and nuclear safety. The computer based systems and component digital computer based assets [i.e. digital assets] that support those functions should then be identified".

For a nuclear facility, these digital assets are the computer based systems that need to be protected against compromise, as recommended in para. 4.10 of Ref. [2], and are the SDAs addressed in this publication.

3.2. The operator should identify and list the facility functions for the entire facility in a consistent manner to ensure that the identified set of facility functions can be assessed holistically. The operator should provide the list of identified facility functions to the competent authority[14] consistent with national regulations. The computer security requirements[15] for these facility functions should be considered, whatever the means of performing the functions (e.g. the specific technology employed, whether analogue or digital).

3.3. The performance of facility functions will rely on or be supported by related sensitive information, sensitive information assets and other associated digital assets.

---

[14] In this publication, the 'competent authority' means the authority to which the State has assigned responsibility for computer security in the context of nuclear security. This may be the competent authority for nuclear security or the competent authority for computer security.

[15] In this publication, computer security requirements include specific written requirements imposed by the relevant competent authority or by the operator to comply with the computer security requirements defined by the competent authority or with regulatory requirements.

3.4. The operator should apply computer security measures to ensure the appropriate protection (including traceability) of sensitive information, sensitive information assets and SDAs. Computer security is provided by measures to ensure confidentiality, integrity and availability as well as to meet any other requirements specified by the competent authority.

3.5. The operator should identify sensitive information, taking into account the effects of its compromise and the State's requirements for the security of sensitive information. Reference [5] provides detailed guidance on the development of a State's requirements for sensitive information.

3.6. Sensitive information may be identified directly by considering the potential consequences associated with its unauthorized disclosure (as indicated in Ref. [5]), for example information on security arrangements, which an adversary might use in planning a malicious act. For this type of information, confidentiality is typically the attribute that most needs protection. Sensitive information may also be identified less directly by considering its functional significance (i.e. its importance to the provision or performance of a facility function), for example accurate and timely data on boiler pressure, which an adversary might be more likely to exploit by modifying or destroying. For this type of information, the integrity and availability of the information might be at least as important as confidentiality.

3.7. The information in the site security plan may be classified as sensitive information and measures may be implemented to protect its confidentiality for an extended period of time, since the information will remain sensitive throughout the period for which the site security plan is valid.

3.8. For an I&C system and its process data, an operator might give priority to those measures that ensure system availability and integrity over those that ensure confidentiality. In this case, the process data are important to the correct performance and availability of the function and are only sensitive during the very limited intervals when the I&C system is performing a control action based on the data. However, once the process data are no longer important to the performance and availability of the function (i.e. can no longer form the basis of a control action), the historical process data have value only based on their sensitivity. Therefore, the security benefit arising from the increased assurance of confidentiality (to protect information sensitivity) needs to be balanced against that from protecting integrity and availability.

3.9. While protecting the confidentiality of process data from these systems might not need stringent measures, the loss of confidentiality of other data related to the systems, such as administration passwords, source code and other key details, would provide the adversary with a significant benefit in the planning and execution of cyber-attacks targeting the system and might lead to a need for stronger measures. Additionally, classification of the historical process data (e.g. logs) to limit their distribution (e.g. application of administrative control) might be necessary to reduce the risk of unauthorized disclosure to an acceptable level.

RISK INFORMED APPROACH

3.10. Computer security should be implemented using a risk informed approach. Figure 4 of Ref. [7] provides an overview of a risk informed approach to computer security measures.

3.11. Risk, in the computer security context, is the risk associated with an adversary exploiting the vulnerabilities of a digital asset or group of digital assets to commit or facilitate a malicious act. This risk is expressed as a combination of the likelihood of a successful attack and the severity of its consequences if it occurs.

RISK ASSESSMENT AND MANAGEMENT

3.12. The operator should establish and implement a CSRM process (unless the management process is performed by the competent authority). The competent authority may specify policy requirements to be followed and may require that a specific risk assessment methodology be used, or it may agree to the use of an operator's methodology [7]. The assessment process for a facility may follow the example of the organizational computer security risk assessment as described in paras 7.10–7.16 of Ref. [7].

3.13. The CSRM process should include a cyclical process for continual improvement[16] in the management of risks associated with cyber-attacks on the facility.

[16] An example of a cyclical process for continual improvement is the 'plan, do, check, act' cycle.

3.14. Periodic and iterative risk assessments are used to support decision making within a risk management process. Computer security risk assessments are typically qualitative, involving relative metrics (e.g. high, medium, low), but could be quantitative if sufficiently reliable data were available.[17] The results of risk assessments will assist in determining appropriate computer security requirements.

3.15. The operator should perform CSRM for the facility to comply with regulatory requirements. Reference [7] indicates that this may include two complementary assessments, one at the organizational level and one at the system level, and such an approach should be adopted for complex, high hazard facilities, such as nuclear facilities. In the guidance in this publication, it is therefore assumed that CSRM for a nuclear facility (facility CSRM) includes a specific phase of risk assessment and management at the system level (system CSRM) (see Fig. 4). This implies two stages:

(a) Assess and manage aggregated computer security risks to facility functions for the whole facility. This will ensure that the operator performs a complete assessment of the facility and will provide the competent authority with the primary means to assess the overall effectiveness of CSRM at the facility. Section 4 provides guidance on performing facility CSRM.
(b) Assess and manage risks associated with each system that performs or supports those facility functions. This will ensure that the operator performs a detailed assessment of each system that performs or supports a facility function. The competent authority may require the detailed assessments as a means to review the effectiveness of specific instances of CSRM at the facility. Section 5 provides guidance on performing system CSRM.

3.16. The operator should ensure independence between the teams responsible for performing overall CSRM to set the computer security requirements for the facility, those implementing the requirements and those validating that the requirements have been met.

3.17. Risk management is relevant at all stages in the facility's lifetime and throughout the life cycles of systems to inform the development, implementation and maintenance of computer security measures. Section 6 identifies risk management activities throughout the lifetime of a facility.

[17] At the time of publication, there are no internationally accepted methodologies that apply quantitative values for security risk assessments.

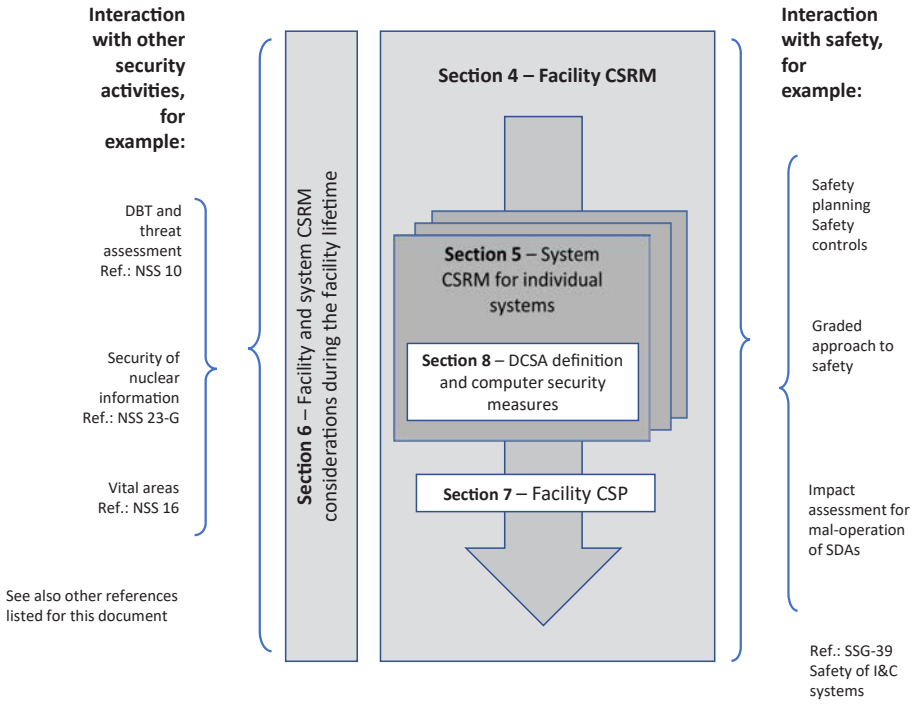


FIG. 4. Overall structure for guidance on computer security risk management (CSRM) in this publication. CSP: computer security programme; DBT: design basis threat; DCSA: defensive computer security architecture; I&C: instrumentation and control; NSS: Nuclear Security Series; SDA: sensitive digital asset; SSG: Specific Safety Guide.

3.18. A review of the risk assessment should be performed, and the risk assessment updated as necessary, in the following instances:

(a) New information or important findings emerge that could invalidate assumptions stated in the current computer security policy, CSP, DCSA, site specific threat assessment.
(b) A vulnerability is discovered that invalidates computer security measures or assumptions made in a system risk assessment.
(c) A computer security incident occurs at the facility.
(d) The national threat statement or DBT is modified (and the modifications are relevant to adversaries using cyber-attacks or blended attacks). This might reflect new threats or enhanced adversary capabilities or resources that might increase the likelihood of successful cyber-attacks.

(e) There is a change to a facility function, system, SDA or computer security measure. This should include the introduction of any new equipment, software or procedures or any major change in skill sets of operating personnel. The level of effort to update the risk assessment can be informed by the assigned level of protection of the SDA (e.g. computer security level).
(f) Regulatory requirements change.
(g) A periodic review is due according to the continual improvement process to ensure that the assessment remains valid.

3.19. Regulatory activities related to facility security, such as licensing, inspection and enforcement, should include appropriate consideration of computer security. Records from the risk management process and the resulting decisions and actions should be available for review by the competent authority on request to allow it to assess whether regulatory requirements are met.

3.20. The overall structure and approach for the risk management process should include the following:

(a) Facility CSRM:
    (i) Definition of the scope of CSRM;
    (ii) Characterization of the facility;
    (iii) Characterization of the threats;
    (iv) Specification of requirements;
    (v) Verification and validation;
    (vi) Acceptance by the competent authority.
(b) System CSRM:
    (i) Definition of system boundaries;
    (ii) Identification of digital assets (including SDAs);
    (iii) System computer security requirements;
    (iv) Verification.

3.21. Many methods exist for conducting risk assessment (see, for example, ISO/IEC 27005 [14]). Organizations need to choose a method and customize it to their specific organizational environment and objectives, while observing the need for separate facility and system level risk management.

COMPUTER SECURITY LEVELS BASED ON A GRADED APPROACH

3.22. Computer security requirements and the design and implementation of measures to meet these requirements should be based on a graded approach,

where computer security measures are applied in direct proportion to the potential consequences arising from compromise of the facility function. As indicated in Section 2, one practical way of applying a graded approach is to assign facility functions to computer security levels, where each computer security level is characterized by graded computer security requirements, and preventive and protective security measures can be selected to meet the requirements for the relevant level. Figure 5 illustrates the graded approach using computer security levels.

3.23. While the requirements (e.g. explicit restrictions on communication between SDAs assigned to different levels) are fixed by the computer security levels, security measures (e.g. the specific type of firewall used to restrict such communications) can be chosen to protect digital assets (including SDAs) according to the architectural environment of the computer security level and the technology of the specific digital assets (including SDAs).

3.24. In the computer security level approach, computer security requirements need to be defined for each level with the following considerations:

(a) Generic requirements should be applied broadly throughout the facility and operating organization and may be applied to all digital assets. Generic requirements provide for improved nuclear security culture through a greater awareness of computer security. They also improve the computer security resilience and might provide additional defence in depth. Generic requirements cannot be credited with providing benefit to a specific computer security level or system because generic measures typically apply

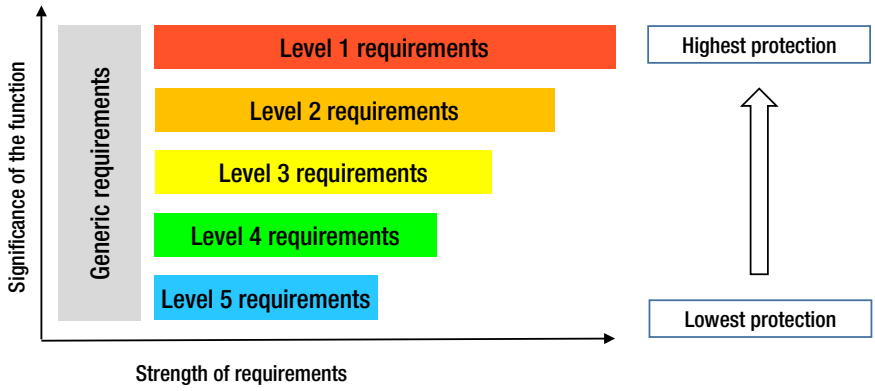


FIG. 5. Illustration of the graded approach using the computer security level concept.

to a wide range of digital assets and cannot be relied on to be operated consistently and effectively.

(b) Computer security levels are assigned, ranging from level 5 (least protection needed) to level 1 (most protection needed) (see Fig. 5). In this approach, systems containing SDAs would be in computer security levels 1–3, whereas systems in levels 4 and 5 contain other digital assets.

(c) Computer security requirements are specified and applied according to the computer security levels assigned, in accordance with a graded approach. Computer security requirements should be based on defence in depth, whereby digital assets assigned to security levels affording higher protection do not rely solely on or implicitly trust digital assets or computer security measures of security levels with lower protection.

(d) The computer security measures applied to meet the requirements for each computer security level should take into account the independence and diversity of the measures in order to reduce common vulnerabilities that could allow multiple layers of defence in depth to be bypassed or defeated. However, it might be necessary for some computer security measures applied in one computer security level to be repeated in other computer security levels.

(e) With the application of a layered approach and defence in depth, computer security measures on lower levels can help protect the higher levels, especially with regard to early detection of cyber-attack.

(f) Computer based systems that are outside the control of the CSP are unassigned and should not be trusted by any digital asset at any computer security level.

3.25. Section 8 provides guidance on computer security requirements for a graded approach using the example of five computer security levels plus generic computer security requirements.

4. FACILITY COMPUTER SECURITY RISK MANAGEMENT

4.1. Facility CSRM is a complex process that should be performed by a multidisciplinary team of people who have skills and competencies in nuclear security, nuclear safety, operations, maintenance, computer security and

engineering.[18] This team might have a composition similar to that proposed for physical protection evaluations (see Ref. [15]).

4.2. Facility CSRM is an iterative process that is conducted in phases. It might be necessary to review and modify assumptions, determinations or results from a previous phase on the basis of the results of a subsequent phase. Verification activities are expected to be performed between phases.

OBJECTIVE OF FACILITY COMPUTER SECURITY RISK MANAGEMENT

4.3. The objective of facility CSRM is to assess and manage risks associated with cyber-attacks that have the potential to degrade the nuclear security or nuclear safety of the facility.

4.4. Facility CSRM should ensure that the regulatory requirements regarding computer security are met.

4.5. Facility CSRM should take account of an assessment of identified adversaries who might attack the facility and their goals (e.g. sabotage, unauthorized removal of nuclear material or radioactive material, unauthorized access to sensitive information), including an evaluation of the attractiveness of targets[19] in the facility to these adversaries. The State's assessment of threats might be provided by the national threat statement or DBT[20].

4.6. Facility CSRM should include a determination of the significance of each facility function in accordance with that function's importance to the operator's objectives. These determinations may allow for the development of a hierarchical list[21] of potential nuclear security events (from most severe to no consequence)

---

[18] Some Member States may use designations such as 'cyber security team' to identify the personnel needed for computer security.

[19] Attractiveness of targets might be addressed in the threat assessment or DBT and may be augmented by information provided by the State via its competent authorities.

[20] A DBT is derived from the State's current evaluation of a threat and provides the basis for the development of nuclear security measures. The operator has the primary responsibility for providing nuclear security measures against the threat capabilities described in the DBT. Some Member States provide an alternative national threat statement instead of a DBT.

[21] An ordered list that places facility functions into groups of approximately similar consequence.

resulting from compromise of a facility function[22]. Figure 7 of Ref. [7] may be used in the development of such a hierarchical list.

4.7. Facility CSRM should include consideration of facility functions but not their technical implementation in systems and digital assets, which are considered in system CSRM (see Section 5).

4.8. The use of a consistent approach to facility CSRM across all facilities within a State may assist the competent authorities in providing effective oversight with respect to the application of computer security at nuclear facilities.

OUTLINE OF FACILITY COMPUTER SECURITY RISK MANAGEMENT

Inputs to facility computer security risk management

4.9. The operator should use the following as inputs to facility CSRM:

(a) The national threat statement or DBT, and associated analysis if available.
(b) Applicable regulatory requirements and other documents. These may include the State's information classification requirements.
(c) The safety analysis for the computer systems of the facility. This safety analysis may be used in defining computer security requirements, but it is not sufficient for this purpose as it does not address all mal-operations, notably those caused by malicious acts.
(d) The site security plan [15]. The site security plan may be used in identifying the facility functions important or related to security and their significance in meeting the operator's objectives. The site security plan may incorporate the facility's CSP or aspects of it.
(e) The facility computer security policy.
(f) Current and previous facility CSP documents, including details of the assignment of facility functions to systems and the facility specific threat assessment.

[22] The operator may also include other functions identified as having significance to the facility other than safety or security.

Phases of facility computer security risk management

4.10. The following are the phases of facility CSRM:

(a) Scope definition: Defining the scope of the risk assessment while taking account of the operator's objectives for the facility (e.g. safety, security, operations, emergency preparedness), the physical and logical boundaries, and the stage of the lifetime of the facility. The prerequisites for and inputs to the assessment should be identified in this phase.
(b) Facility characterization: Identifying facility functions and their interactions and interdependencies, identifying sensitive information that could be useful in planning an attack against the facility, and identifying targets on the basis of the identified facility functions and sensitive information.
(c) Threat characterization: Analysing the national threat statement or DBT and any other relevant information or analysis of threats to identify specific tactics, techniques and procedures, along with adversaries' skills, that could be used in cyber-attacks (including blended attacks) on targets at the nuclear facility. The threat characterization is a model, developed through analysis of applicable aspects of the threat information, to generate a representation of adversaries who pose the greatest risk. This threat characterization phase bounds the range of credible attack scenarios.
(d) Specification of computer security requirements: Generating facility level computer security requirements. The specification phase includes the following:
    (i) Developing and documenting a CSP;
    (ii) Recommending any necessary amendments to the computer security policy;
    (iii) Assigning the identified facility functions to computer security levels;
    (iv) Creating or amending requirements for the DCSA.

    This phase may include applying analysis techniques (e.g. vulnerability assessment, threat assessment) and evaluation methods (see para. 4.98) to develop requirements from the facility characterization and threat characterization phases, and from regulatory requirements.
(e) System CSRM: The CSP and the DCSA are applied to each system. System CSRM is described more fully in Section 5. Changes might be needed to the CSP and the DCSA in the light of the experience of implementing the CSP and the DCSA on each system.
(f) Implementation of systems and their integration into the facility: This phase is not covered further in this publication. Changes may be needed to the DCSA and the CSP in the light of the practical engineering experience of implementation and systems integration.

(g) Assurance activities: These are not strictly a phase of facility CSRM but rather a set of continuous activities that are also performed in each system CSRM process. Three types of assurance activity are used:
   (i) Evaluation of compliance with computer security requirements;
   (ii) Verification of each phase of CSRM;
   (iii) Validation of the computer security of the facility.
   Scenarios are a vital part of evaluation, verification and validation activities.

(h) Facility CSRM outputs: These outputs comprise the (revised) CSP, the DCSA, the site specific threat assessment and the facility CSRM compliance report. Some or all of these documents will be subject to review for acceptance by the competent authority. The output from CSRM may be an input to the further development by the State of its regulatory requirements.

4.11. The phases of facility CSRM are shown in Fig. 6, which provides an overview of the facility CSRM process. These phases are described in more detail in the remainder of this section.

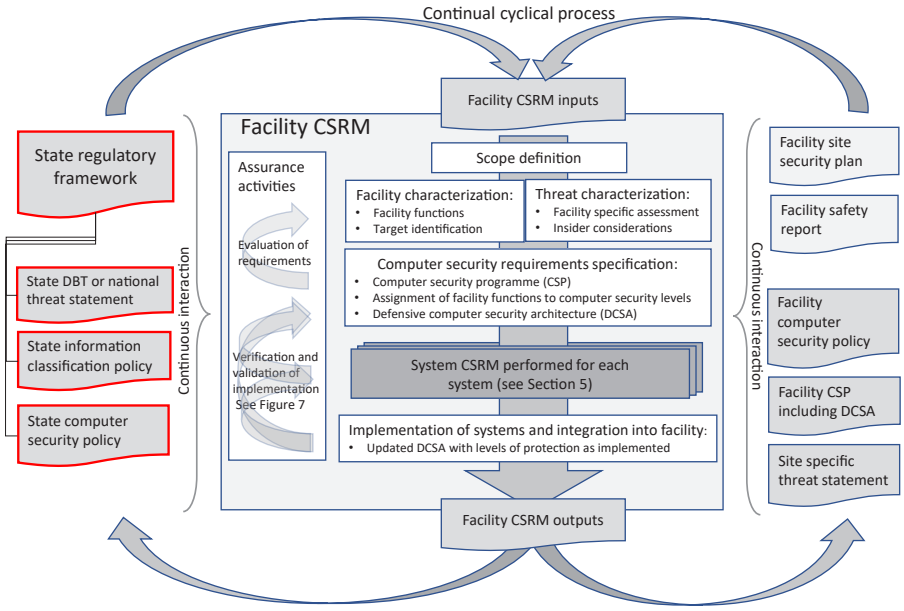


FIG. 6. Overview of facility computer security risk management (CSRM) process. DBT: design basis threat.

4.12. There is one facility CSRM process per facility, within which there is a separate system CSRM process for each system. For a site that contains multiple facilities or for an organization that operates multiple facilities, there may be one process for the whole site or whole organization, resulting in one or more sets of facility CSRM output. In this case, the operator may decide how many sets of output to generate but should ensure that the process is comprehensively applied to each facility.

SCOPE DEFINITION

4.13. The operator should identify the scope of facility CSRM, which will be the physical or logical extent of the facility functions and associated systems of concern for nuclear security. Considerations in defining the scope might include the facility's physical perimeter; the locations of approved vendors, contractors and suppliers; the operating organization's corporate offices; off-site data centres; and any other strategic locations. The scope of assessment might also vary depending on the stage in the lifetime of the facility or the capability and maturity of the operating organization (see paras 5.26–5.29 of Ref. [7]).

FACILITY CHARACTERIZATION

Identification of facility functions

4.14. The operator should identify all facility functions without consideration of how those functions are performed. The presence and use of digital assets throughout the facility and throughout its lifetime make it likely that digital assets will be used to perform or support the majority of key tasks and activities related to facility functions.

4.15. The stage in the lifetime of the facility [10] should be taken into account in characterizing the facility and identifying the facility functions. Different facility functions will be relevant at different lifetime stages, and their relative importance might change.

4.16. Facility functions are characterized by the following elements:

(a) Intrinsic significance: The importance of the facility function to nuclear security and nuclear safety and the potential consequences for the facility if the function is not performed correctly.[23] This is the primary characteristic.
(b) Potential effects of compromise: The manners in which the facility function could fail to be performed correctly.
(c) Interdependencies between functions: The significance of a facility function might arise from other functions that depend on it.
(d) The timeliness and accuracy with which the facility function needs to be performed.

Intrinsic significance of facility functions

4.17. The significance of all facility functions should be compared in order to group together those that have similar significance, if possible using a common scale that includes both security and safety considerations.

4.18. For facility functions important or related to nuclear security, a classification scheme based on consequences for nuclear security, such as that outlined in Fig. 7 of Ref. [7], should be used to determine the significance of the function.

4.19. For facility functions important or related to nuclear safety, an established safety classification scheme may be used to determine the significance of the function. However, security considerations may necessitate the assignment of higher significance than indicated by a function's safety classification.

4.20. The determination of the significance of facility functions should take into account that the performance of safety functions (by systems) may support security and the performance of security functions may support safety. As a result, the significance assigned to a safety function for computer security may differ from its safety class.

---

[23] The significance of the function to nuclear security can often be associated with the consequences of the function's not being performed correctly. For nuclear facilities, the consequences that are considered most significant are unauthorized removal of nuclear material and sabotage resulting in unacceptable radiological consequences. Other consequences, such as unauthorized disclosure of sensitive information, might be considered. Other possible consequences might be associated with other organizational objectives, for example maintaining reputation or remaining compliant with other environmental regulations. A list of possible consequences can be found in ISO 27005:2018 [14].

4.21. For example, a system providing a facility function of detecting radiation for the protection of personnel (a safety objective) may also provide for the detection of unauthorized removal of nuclear material (a nuclear security objective). Although the failure of the radiation protection function from a safety perspective might have limited consequences, the consequences of failure for nuclear security might be more severe. Therefore, the facility functions provided by the system in this example would be assigned a significance value on the basis of their importance to the nuclear security objectives. (Alternatively, the operator could choose to implement independent systems to separate the functions that support nuclear safety and nuclear security, and in this example the function supporting nuclear safety could be assigned lower significance.)

Potential effects of compromise of a system on facility function

4.22. In addition to considering the intrinsic significance of the facility function, the operator should consider the effects on facility function of compromise of the system intended to perform it. These effects are as follows (arranged from worst to best case):

(a) The performance of the facility function is indeterminate. This means that the function might be altered in any manner without the initial compromise being detected.
(b) The performance of the facility function changes in unexpected ways (and other actions can be performed), but these anomalies are observable to the operator.
(c) The performance of the facility function fails.
(d) The performance of the facility function is as expected, meaning the compromise does not adversely affect the facility function (i.e. the system is fault tolerant).

4.23. A system intended to perform a facility function might mal-operate in different ways when compromised, and the effects of this mal-operation depend on the circumstances and environment at the time of the compromise, the nature of the cyber-attack causing the compromise, and the significance of the facility function. For example, a system performing a less important facility function might, through interdependencies and interactions between the functions, be used to attack a system performing a more important function.

4.24. For each system and each type of effect of compromise (i.e. mal-operation), there will be different consequences for the facility. These consequences should be assessed, and the significance assigned to facility functions should

be based on these potential consequences. When assessing consequences, loss of confidentiality, integrity or availability of sensitive information should be considered, as well as consequences related to unauthorized removal of material or sabotage of the facility.

4.25. The significance assigned to a facility function should take into account whether the facility function can be defined in a way that is valid for all possible conditions or modes on which the facility function might depend. If the facility function cannot be bound in this way, the list of consequences might be incomplete and additional analysis or assignment of a higher significance value (using a conservative approach) may be needed.

Interdependencies between facility functions

4.26. The determination of the significance of a facility function should also take into account the potential consequences of compromise (or mal-operation) on other facility functions that depend on it. Examples of such functional dependencies include the following:

(a) Information dependency: A facility function provides information to another facility function. Examples of mal-operation include the following:
    (i) Interruption of the automated control instructions for a facility process;
    (ii) Compromise of alarms provided to security officers;
    (iii) Display of incorrect plant monitoring information to operating personnel;
    (iv) Failure to provide information for emergency responders or nuclear security officers;
    (v) Loss or manipulation of procedures or instructions, or of records that document the results of these procedures.

(b) Engineering or physical resource dependency: A facility function provides a physical resource to another facility function. This includes resources needed to sustain the other facility function directly and resources needed to sustain those resources. Examples of mal-operation include the following:
    (i) Interruption of the provision of water or power;
    (ii) Unanticipated ambient environmental conditions;
    (iii) Failure to schedule preventive maintenance tasks;
    (iv) Failure of physical protection systems (e.g. access controls, intrusion detection).

(c) Policy or procedural dependency: A change to one facility function necessitates a change to another facility function. For example, if policy demands that primary and secondary heat sink functions be provided when

a reactor is critical, then if one of those heat sinks becomes unavailable, the reactor has to be put into a subcritical state.

(d) Proximity effects: The effects on a facility function of mal-operation or physical failure of other systems physically near to those that perform the facility function.

4.27. Analysis of interactions and interdependencies between facility functions might reveal that an important facility function has been omitted from the scope of the assessment. Dependencies might extend beyond the facility, for example the supply of water or power to the facility. Some functions provided by external organizations may need to be considered in the analysis of facility function dependencies. In this case, it may be necessary to revise the assessment scope to include those dependencies or to make changes at the facility that remove the dependencies.

4.28. Segregation of systems performing facility functions to limit the interactions and interdependencies between them might simplify the specification of computer security levels and requirements and might improve the effectiveness and efficiency of computer security measures.

Necessary timeliness and accuracy for facility function interdependencies

4.29. The determination of the significance of facility functions may also take into account the timeliness and accuracy with which one facility function needs to respond to another facility function. Timeliness can be considered in terms of requirements for the availability of sensitive information, and accuracy can be considered in terms of requirements for the integrity of such information:

(a) Availability of information implies that, for example, alerts provided by one facility function are provided promptly to allow other facility functions such as assessing the alert and responding to the alert to be performed.

(b) Integrity of information implies that, for example, a facility function provides accurate data on environmental variables (e.g. temperature, pressure, frequency, level) on which other facility functions depend.

Target identification

4.30. A target is defined in Ref. [1] as follows:

> "*Nuclear material, other radioactive material, associated facilities, associated activities*, or other locations or objects of potential exploitation by

a *nuclear security threat*, including *major public events*, *strategic locations*, *sensitive information*, and *sensitive information assets*."

4.31. Some systems performing facility functions will be targets and should be identified from the list of facility functions produced during facility CSRM, using the definitions of vital areas [16] and sensitive information [5]. Whether such a system is considered a target does not alter the significance of the facility function, but it is an additional consideration when determining computer security requirements.

4.32. Targets that are associated with important facility safety and security functions should be identified as SDAs through the process described in paras 3.6–3.9. These SDAs should also be analysed for the potential value of any associated sensitive information. This will ensure that the SDAs and their associated information are considered within the facility's information security programme and CSP and are afforded the appropriate level of protection.

Documentation of facility functions

4.33. The operator should document all facility functions identified and assessed during facility CSRM.

4.34. Identification of all the functions within the facility depends on having complete and accurate records describing the interactions and interdependencies between functions. These records will allow for the assessment of those functions that could have a negative impact on other functions if not performed correctly.

4.35. The interactions and interdependencies of a facility function might be internal or external and might be permanent or temporary. For example, during the development of systems, interaction might be needed between the development and operational environments through the physical transport of new software, data or devices, but these interactions could be removed when the systems are operational.

4.36. The operator should consider, when analysing the consequences of an attack directed at one facility function, the possibility that it could be part of an attack affecting multiple facility functions or part of a blended attack (i.e. combined cyber-attack and physical attack).

4.37. The analysis may need to include an iterative assessment of each facility function, whereby one assessment is performed to determine the function's

intrinsic significance, and another is performed to determine the significance on the basis of interactions and interdependencies with other facility functions. The higher of the two levels of significance from these assessments should be used.

4.38. Those facility functions that have a direct relationship between the function not being performed correctly and the most severe consequences (e.g. those facility functions closely related to the three fundamental safety functions of controlling criticality, removing heat and containing material [12])[24] should be assigned the greatest significance. In these cases, the assignment of significance should not take account of other parameters or factors.

THREAT CHARACTERIZATION

4.39. Threat characterization depends on two separate continuous processes, which are interrelated:

(a) The State's assessment of threats and the development and maintenance of the national threat statement or DBT using intelligence sources;
(b) The facility specific threat assessment, taking account of analysis of facility specific information and information on specific adversaries.

Sources of threat information

4.40. Paragraph 3.34 of Ref. [2] states:

> "The appropriate State authorities, using various credible information sources, should define the *threat* and associated capabilities in the form of a *threat assessment* and, if appropriate, a *design basis threat*. A *design basis threat* is developed from an evaluation by the State of the threat of *unauthorized removal* and of *sabotage*."

Additional information on the DBT can be found in Ref. [9].

[24] See also table 1 of Ref. [17] for relationships between functions credited in the analysis of postulated initiating events and safety categories.

4.41. The operator should put in place measures to identify, retain and manage specific information[25] related to potential cyber-attacks and adversaries (e.g. phishing emails, malware samples) to allow follow-up analysis to support threat characterization. The operator should ensure that these measures are implemented in a manner that does not adversely affect nuclear security or nuclear safety.

4.42. The operator's threat characterization might include elements of threat assessments performed by other organizations (e.g. the operator's own assessments, open source intelligence reports).

4.43. The relevant competent authority is encouraged to provide an analysis of the specific information captured by the operator in a timely and cooperative manner and to support the exchange of this analysis and other important information, consistent with the State's requirements for sensitive information [5]. Periodic reporting of incidents to the relevant competent authority by the operator may be valuable as threat analysis, and characterization is a continual activity that demands up to date information.

4.44. During the development of the national threat statement or DBT, the competent authority and other relevant State authorities should have (or should have access to) expertise and knowledge regarding potential computer security incidents (e.g. cyber-attacks) on nuclear facilities.

4.45. Reference [7] provides guidance on the assessment of cyber threats to a nuclear security regime as well as detailed descriptions of potential sources of attack and associated attack mechanisms relevant to nuclear facilities, and of methodologies used to evaluate and identify threats.

Facility specific threat characterization

4.46. The operator should develop and maintain a facility specific threat characterization to support the evaluation of computer security risk to the facility. This should include an analysis of the national threat statement or DBT to characterize the specific nuclear security threats to the facility that contribute to the computer security risk. The analysis should describe the potential objectives, capabilities, tactics and techniques of relevant threats, providing the basis for

[25] This specific information may be specified by the operator, a competent authority or other State organization. This information may be classified and therefore needs to comply with the State's identification of and handling requirements for sensitive information.

formulating or validating the effectiveness of the facility computer security policy and CSP.

4.47. The operator should perform the threat characterization in the following instances:

(a) The operator performs a facility computer security risk assessment. This may sometimes be a less intensive analysis to check the previous analysis and assumptions.
(b) The competent authority issues a new DBT or national threat statement.
(c) The operator receives information that potentially invalidates assumptions made in the current analysis.

4.48. The threat characterization done by the operator should describe the knowledge, capabilities and funding, as well as the possible campaigns, targets, tactics, techniques and procedures of identified potential adversaries, and any additional attributes of particular relevance. Paragraph 5.19 of Ref. [9] provides a list of possible additional attributes for threat characterization.

4.49. The threat characterization done by the operator should identify potential combinations of tactics and techniques that might be used in an attack, such as coordinated remote and local actions, use of insiders and external adversaries, or blended attacks combining cyber-attacks and physical attacks. The threat characterization should include the possibility of sequential or parallel cyber-attacks with cumulative consequences, involving one or several adversaries, as well as cases where there are no indications of collusion between different adversaries (non-collaborative attacks).

4.50. The threat characterization done by the operator should allow for listing and assessment of credible types of attack. This list will form the basis of the computer security requirements and specification of the DCSA.

4.51. The threat characterization should indicate whether the adversary has the capabilities to carry out a particular type of attack and whether the adversary can compromise a system performing a facility function in such a way that its behaviour is indeterminate (i.e. outside its design basis).

Additional considerations for insider threats

4.52. The threat characterization should include consideration of insider threats. Specific guidance is provided in Ref. [6]. For computer security, insider threats can be categorized as follows:

(a) Passive insider: An insider with the motivation to enable but not initiate malicious acts. The computer security measures to counter a passive insider might rely on preventive measures, including having a strong security culture. Typically, a passive insider will not be deterred by detection measures, because their access to information and systems is legitimate, but will seek to avoid being identified as acting maliciously.
(b) Active insider: An insider with the motivation to initiate malicious acts. There are likely to be fewer active insiders than passive insiders. The computer security controls to counter an active insider need to be more comprehensive than those to counter a passive insider and should include protective measures such as separation of duties and compartmentalization of information, physical access or system privileges.
(c) Unwitting insider: An insider without the motivation to commit a malicious act and who is unaware of their exploitation by an adversary. For example, in a cyber-attack, an unwitting insider might not be aware that certain actions can provide information or authenticated access to an adversary, such as by clicking a malicious link in an email disguised as being from a trusted source.

4.53. Adversary paths and the associated timelines for insider threats differ from other threats owing to insiders' authorized access. This access allows insiders, for example, to use a non-continuous series of tasks performed over an extended period of time. For example, the gathering of administrative credentials (through either social engineering or compromise of systems) to defeat measures such as access controls or segregation of duties could take place over several weeks, months or years.

SPECIFICATION OF COMPUTER SECURITY REQUIREMENTS

Computer security policy and computer security programme

4.54. The operator's computer security policy[26] specifies the objectives and high level requirements for computer security of the facility, applying a graded

[26] Some organizations may refer to the computer security policy as the 'computer security strategy'.

approach and defence in depth. These high level requirements are specified by the operator, in compliance with applicable regulatory requirements, and are applicable without exceptions. The computer security policy is an input to facility CSRM, and facility CSRM may expand on and refine the facility computer security policy.

4.55. The operator should develop and document its CSP[27] as part of facility CSRM. The CSP is a framework for implementation of the facility computer security policy that will be used throughout the lifetime of the facility. The contents of a typical CSP are described in Section 7 and include the set of specific computer security requirements of the facility, in addition to those requirements identified by a risk informed approach.

4.56. The operator should define computer security requirements in the CSP for the following, which are described in more detail in Section 7:

(a) Organizational roles and responsibilities;
(b) Risk, vulnerability and compliance assessment;
(c) Organizational security procedures;
(d) System security design and management;
(e) Asset and configuration management;
(f) Personnel management.

4.57. The operator should specify within the CSP those baseline computer security measures that are mandatory for each computer security level. These measures are likely to consist of requirements that represent organizational policies and processes and will translate into procedures.

4.58. Requirements for the strength of computer security measures should be identified and defined for each computer security level, consistent with regulatory requirements (if applicable). Exceptions to the application of a specific measure within a computer security level are strongly discouraged, and any such exceptions should be justified and documented within facility CSRM.

4.59. The principal outputs from the specification phase of facility CSRM are the documentation of the CSP (or revised CSP) and a compliance report for the competent authority indicating how implementation of the CSP will ensure

[27] Some organizations may refer to the CSP as a ‘computer security plan’.

that regulatory requirements are met. The CSP documentation may be a single document or a collection of separate documents but should include the following:

(a) A statement that indicates the level of computer security protection to be provided for each computer security level. This statement could be qualitative or quantitative, but should be verifiable.
(b) A requirement to perform and document periodic computer security reviews and risk assessments in each stage of the lifetime of the facility.
(c) A definition of the roles and responsibilities needed to support computer security.
(d) A specification for the DCSA, combining the computer security requirements derived from the operator's application of a risk informed approach and any such requirements imposed on the facility by national law or regulations. The DCSA specifications should include the following:
    (i) The requirements for applying a graded approach (e.g. the number of computer security levels);
    (ii) The requirements for defence in depth;
    (iii) Any additional requirements (e.g. for authenticity, non-repudiation and traceability) necessary to meet the necessary level of protection for each computer security level;
    (iv) Requirements that will provide and maintain the capability to prevent, detect, delay, mitigate the effects of and recover from cyber-attacks;
    (v) The specific requirements for computer security measures for each computer security level to be applied to the respective computer security zones.
(e) A record of the functional scenarios or other evaluation methods used in the analysis to develop requirements. It is important that other scenarios be developed independently to provide greater assurance in the requirements (i.e. increased confidence). Use of scenarios for raising confidence in the output of the specification phase is described in more detail in paras 4.116-4.122.

4.60. The operator should provide its CSP documentation for review by the competent authority, along with the compliance report.

Assignment of systems performing facility functions to computer security levels

4.61. Facility CSRM should include or make use of a prioritized list of facility functions, arranged in order of the significance of the facility function, as the basis for the application of a graded approach to provide the highest level of assurance

of protection to those functions that have the highest potential to lead to the most severe consequences.

4.62. The aim of the computer security level approach is to simplify the application of a graded approach. Computer security levels determine which set of computer security requirements are implemented to provide the appropriate level of protection to the system performing a facility function.

4.63. The operator should identify the number of computer security levels to be used, taking account of applicable regulatory requirements. For example, an operator could choose to apply a different computer security level for each facility function. However, the complexity of applying the approach increases with the number of computer security levels. Limiting the number of computer security levels allows for common approaches and methods to be applied to different systems. Therefore, the facility may choose to use a smaller number of levels. The benefit of simplicity in reducing the number of levels should be balanced against the cost in resources and efficiency of applying more stringent measures to facility functions than absolutely necessary in all cases.

4.64. The operator should ensure that each facility function is assigned to a single computer security level.

4.65. In some cases, facility functions important or related to security might not be sufficiently demarcated to allow them to be clearly distinguished from other functions. The inability to separate facility functions from one another increases the complexity in assigning the significance of the facility functions. Facility functions should therefore be distinct and independent from one another to the extent possible. The operator may consider modification of the facility functions with the aim of simplifying the application of the graded approach, which in turn might also be of benefit in applying defence in depth.

4.66. The operator should include the following in the CSP documentation:

(a) The number of computer security levels and the requirements for their associated computer security measures;
(b) The ordered list of facility functions, indicating how the functions have been assigned to computer security levels.

Defensive computer security architecture specification

4.67. The operator should design and implement a DCSA in which all systems performing facility functions are assigned to a computer security level and protected according to computer security requirements specified for that level.

4.68. The operator should specify those baseline computer security measures that are mandatory for each computer security level within the DCSA. These baseline measures may include technical, administrative and physical control measures.

4.69. The DCSA should be designed to eliminate or limit the possible routes for cyber-attack (as identified in the threat characterization) that an adversary could exploit to compromise systems performing facility functions. Similar processes for reducing physical pathways available to the adversary are detailed in Ref. [16].

4.70. Computer security boundaries[28] should be established between systems performing facility functions that have different computer security levels.

Requirements in the DCSA specification to apply a graded approach

4.71. The DCSA specification should express the overall requirements (including the number of computer security levels) and should include the strength of measures for each computer security level, the strength of measures between different computer security levels and the rules for communication between zones at different computer security levels.

4.72. The DCSA specification should ensure that facility functions with the highest significance are assigned to the most stringent computer security level. Requirements for communications between systems assigned to different facility functions should be defined. Data flow should be controlled between facility functions of different computer security levels in accordance with a risk informed approach.

4.73. The DCSA specification should ensure that system design complexity is reduced where possible to simplify implementation of computer security measures. Decreasing the complexity of computer security measures can increase both performance and reliability.

---

[28] 'Computer security boundaries' are defined in this publication as the logical and physical boundaries of a system or a set of systems at the same security level, which therefore may be secured by the application of common security measures (e.g. computer security zones).

Requirements in the DCSA specification to apply defence in depth

4.74. The DCSA specification should require the application of defence in depth through successive layers[29] of computer security measures that have to be overcome or bypassed by an adversary in order to compromise systems performing facility functions.

4.75. The DCSA specification should require a designed mixture of technical, physical and administrative control measures to provide defence in depth.

4.76. The DCSA specification should require a design that ensures that a compromise or failure of a single computer security measure does not result in unacceptable consequences.

4.77. The DCSA specification should require the use of independent and diverse measures to ensure that a common vulnerability cannot allow an adversary to compromise or bypass multiple layers of defence in depth with a single tactic.

4.78. The DCSA specification should require the application of defence in depth between layers and within each layer. Layers of defence may use a combination of measures applicable to different computer security levels and apply them to different computer security zones. For the most severe consequences (i.e. high radiological consequences due to sabotage or unauthorized removal of Category I nuclear material), computer security measures should be implemented in multiple independent layers with the aim of providing deterministic and fail-secure[30] behaviour of systems in the event of cyber-attack.

4.79. The DCSA specification should be supported by an analysis report to identify computer security measures that are fail-secure and deterministic within the application of defence in depth. This report may be requested by the competent authority to be submitted for review.

---

[29] The term 'layers' in this publication refers to layers of defence in depth. For computer security, this is typically achieved through the arrangement of computer security zones (including computer security measures) constructed in compliance with the requirements of the computer security levels and the DCSA.

[30] The term 'fail-secure' means that failure of a measure results in a condition that maintains the security of the function that the measure is intended to protect.

Defence in depth between layers

4.80. The DCSA specification should require each layer of defence in depth to be protected from cyber-attacks originating in adjacent layers. Layers and their associated computer security measures should prevent or delay advancement of attacks.

4.81. The DCSA specification should require that the computer security measures used in a layer be selected and operated in a diverse and independent manner from those computer security measures used in an adjacent layer in order to mitigate common cause failures of protection mechanisms used for isolation between layers. In accordance with the principle of a graded approach, these requirements should be more stringent for those layers requiring the most stringent protection (i.e. computer security levels 1 and 2).

Defence in depth within a layer

4.82. The DCSA specification should require that a combination of computer security measures be employed within each layer to minimize the potential for a single compromise to overcome or bypass multiple measures. In accordance with the principle of a graded approach, these requirements should be greatest for those layers requiring the most stringent protection (i.e. computer security levels 1 and 2, with level 1 having the highest level of protection).

Trust model

4.83. The application of a graded approach and defence in depth should be consistent with an applicable trust model. Trust models that may be applied include the following:

(a) Personnel trustworthiness (i.e. protection against insider threats) [6];
(b) Sensitive (i.e. classified) information protection (e.g. Bell–LaPadula[31]);
(c) Integrity protection (e.g. Biba, Clark–Wilson[32]).

[31] The Bell–LaPadula model enforces confidentiality: for a person or process to access information, they should have a clear need to know and should be authorized to have access to at least the classification of the sensitive information.

[32] Biba and Clark–Wilson models protect the integrity of information: Biba prevents data modification by unauthorized parties but does not prevent unauthorized modification by authorized parties (i.e. insiders), whereas Clark–Wilson prevents both.

RELATIONSHIP WITH SYSTEM COMPUTER SECURITY RISK MANAGEMENT — PERFORMED FOR EACH SYSTEM

4.84. After specification of the computer security requirements, the implementation of those requirements proceeds as illustrated in Fig. 6 (see also Fig. 7). The implementation of requirements demands understanding of the ways in which facility functions are performed by digital assets.

4.85. The risk management processes in facility and system CSRM have significant interactions (see Figs 6 and 7). Facility CSRM includes the assignment of one or more facility functions to individual systems and thus sets the scope for each system's CSRM, but facility CSRM might also be affected by the outputs of system CSRM in an iterative process. For example, in physical protection systems, multiple facility functions may be assigned to a single system owing to the unavailability of systems with segregated functions. This restricts the ability to segregate the system into separate zones, thereby limiting the zone model to either a physical boundary or a logical boundary.

4.86. For legacy facilities or systems, some structures, systems and components might not be modifiable or alterable. This might mean at the system CSRM phase that some requirements defined in facility CSRM cannot be met, and the operator might need to revise facility CSRM to determine a suitable CSP and DCSA specification that meets the security requirements.

4.87. Facility and system CSRM should be reviewed and might need to be revised in the following instances:

(a) The facility CSRM or facility safety analysis is revised.
(b) The system cannot fully comply with requirements identified in the facility CSRM output.
(c) System modifications are made that have the potential to affect facility CSRM.
(d) Relevant security events or incidents occur.
(e) New or changed threats or vulnerabilities are identified.

4.88. The review of both the facility and system CSRM processes needs to be included in the facility change management process to ensure that they are consistent with one another and are kept up to date. These analyses also assist in setting the requirements (e.g. defining the computer security levels) for new systems or implementations.

4.89. Trends in successive iterations of facility and system CSRM should be periodically assessed to identify the following types of adverse pattern:

(a) A risk showing a clear pattern of increasing towards or beyond the unacceptable risk threshold. In this case, consideration should be given to ways to prevent the risk threshold being exceeded.
(b) A risk reaching or exceeding the threshold. In this case, appropriate actions will need to be taken (e.g. reporting to the competent authority, implementing compensatory measures consistent with the urgency identified from risk trend data).

4.90. Trends associated with individual systems should be analysed to ensure that the trend has not invalidated the facility CSRM output. For example, system surveillance assessments may be performed continually, and system performance monitoring reports may then be approved periodically. Outputs from the corresponding systems' CSRM should be reviewed in the facility CSRM process to ensure there is no change in the overall facility risk.

ASSURANCE ACTIVITIES

4.91. There are three types of assurance activity:

(a) Evaluation, which provides confidence in the outputs of phases where verification is not possible (e.g. the threat characterization and computer security requirement specification phases). Owing to the nature of the information on which the computer security requirements are developed (e.g. estimations of the threat, assumptions about facility function failure modes due to compromise of systems), the operator cannot be certain that the requirements are correct. Therefore, evaluation is needed to give the operator confidence in the outputs of the computer security requirement specification phase, namely the CSP and the DCSA.
(b) Verification, which provides confirmation that the results of a phase meet the objectives and requirements defined for that phase. Where possible, verification activities occur between successive phases of facility and system CSRM. This may involve a number of performance based methods or analyses to verify the outputs of each phase prior to their use as input in a subsequent phase.
(c) Validation, which is the process of determining whether the computer security of the facility provides appropriate protection against the threat (as defined in the threat characterization) and complies with regulatory requirements.

Evaluation

4.92. The operator should evaluate the CSP and the DCSA to verify that their implementation will be effective in reducing the opportunity of adversaries to compromise systems performing facility functions, specifically through the following:

(a) Identification and assignment of functions to computer security levels;
(b) Assignment of computer security measures to those levels;
(c) Specifications for computer security measures.

4.93. The evaluation of the CSP and the DCSA should include functional and performance testing in a manner that meets regulatory requirements. The evaluation should include consideration, as appropriate, of both facility and system CSRM and of the whole lifetime of the facility.

4.94. The operator should consider using independent experts to review its CSP and DCSA.

4.95. The operator should justify all assumptions about the likelihood of attacks or their success (e.g. vulnerability, exposure, opportunity) that are used in evaluation. The likelihood should be assumed to be 1 for postulated scenarios that can result in unacceptable radiological consequences[33] or unauthorized removal of nuclear material (i.e. compromise of SDAs).

4.96. The national threat statement or DBT and the facility specific threat assessment provide the basis by which the operator can conduct an analysis to confirm the assumptions made during the assignment of facility functions to the appropriate computer security level. The use of credible functional scenarios (para. 4.120(a)) may allow for a greater level of assurance in the quality of the assessment (see Annex I for example scenarios).

4.97. Computer security measures based on the CSP and the DCSA provide detection, delay and response functions through physical (e.g. structure), technical (e.g. firewall) and administrative (e.g. personnel, procedures) control measures. The interaction of these computer security measures with the facility functions important to safety and security, and their assigned systems, makes the evaluation of the CSP's effectiveness a challenging task.

[33] Guidance on the definition of unacceptable radiological consequences is provided in Ref. [8].

4.98. A number of evaluation methods are available, including the following:

(a) Attack tree analysis (also referred to as ‘attack vector analysis’ and ‘attack graph analysis’). This involves postulating a set of different possible adversary paths to determine whether there is high assurance that each attack will fail (i.e. that the adversary can be prevented from following the path) or be detected and responded to before the adversary reaches the objective. Attack tree analysis can be used, with the threat characterization, to assess whether the measures based on the CSP and the DCSA are effective in eliminating or minimizing the potential for an adversary to make the postulated attacks successfully.

(b) Simulation. This includes computer based simulations of elements of the CSP (including the DCSA) and tabletop exercises that allow consideration of security and contingency plans as well as decision making by the adversary and computer security incident responders. These tools are used to judge the overall performance of the CSP, taking all measures into account. For example, tabletop exercises might assist in determining the opportunities available to an adversary on the basis of their capabilities and characteristics (e.g. whether they are insiders), or the vulnerabilities of the function.

(c) Exercises. These can include both facility level and system level performance testing (e.g. penetration tests) as well as force-on-force exercises (e.g. for blended attacks) in either field conditions or test conditions. These exercises can address the effectiveness of the CSP in providing protection to the entire facility, parts of the facility, specific sets of systems or sets of measures against a simulated adversary attack. In this evaluation activity, data concerning the performance of computer security measures are collected and used to evaluate the overall effectiveness of the CSP.

4.99. Simulation and exercises are typically performed as part of scenario based analysis, in which postulated attacks (scenarios) are specified in detail and simulated or used as a basis for exercises. Scenario based analysis typically builds on attack tree analysis by considering specific adversary tactics and techniques for defeating computer security measures.

4.100. The effectiveness of the CSP, the DCSA or individual computer security measures can be evaluated quantitatively or qualitatively or both. The competent authority may prescribe deterministic evaluation methods to be used for different types of target, threat and scenario. It is suggested that the overall effectiveness of the CSP and the DCSA be conservatively defined as the lowest effectiveness that still meets regulatory objectives when all adversary tactics and techniques and credible scenarios have been considered.

Verification

4.101. The objective of verification in this context is to evaluate the quality of outputs from one phase against the specifications before that output is used in a subsequent phase.

4.102. Verification should, where possible, occur between successive phases of facility or system CSRM.

4.103. The results of verification might lead to the following actions by the operator:

(a) Addressing any deficiencies in design or implementation of computer security measures to meet the requirements;
(b) Identifying, analysing and implementing upgrades that might be necessary to address identified deficiencies and improve performance.

4.104. These verification activities might involve evaluation methods, including exercises, performance testing, simulation or analysis (e.g. vulnerability assessment) (see para. 4.98).

4.105. For example, evaluation of outputs based on attack tree analysis includes consideration of the flow of information between systems, devices, networks and locations. The exchange of information between systems can allow adversaries to exploit these pathways, potentially leading to compromise of systems and thereby of facility functions. Attack tree analysis at this stage considers generic pathways with the aim of minimizing or eliminating the possibility of an adversary gaining access to these pathways.

4.106. The operator should use a graded approach when determining the level of effort to be applied to verification and validation. The greatest level of effort should be applied to those functions or systems assigned to the most stringent computer security levels (i.e. those requiring the greatest level of protection).

4.107. Verification should be repeated on a regular basis (e.g. annually) or as needed to take into account any changes in targets or in the nuclear security programme requirements.

Validation

4.108. The operator should validate that the systems, when integrated together, have the appropriate level of protection to meet computer security requirements as expressed in the CSP and the DCSA. Figure 7 illustrates the verification and validations activities within the CSRM process, CSP and DCSA.

4.109. The operator should validate that the systems, as they are installed at the facility level, have the appropriate level of computer security protection to perform their facility functions to meet requirements as expressed in the facility security requirements.

4.110. The operator should validate that the level of computer security protection is sufficient to ensure that the operation of the facility meets regulatory requirements or operator requirements as expressed in the facility security requirements.

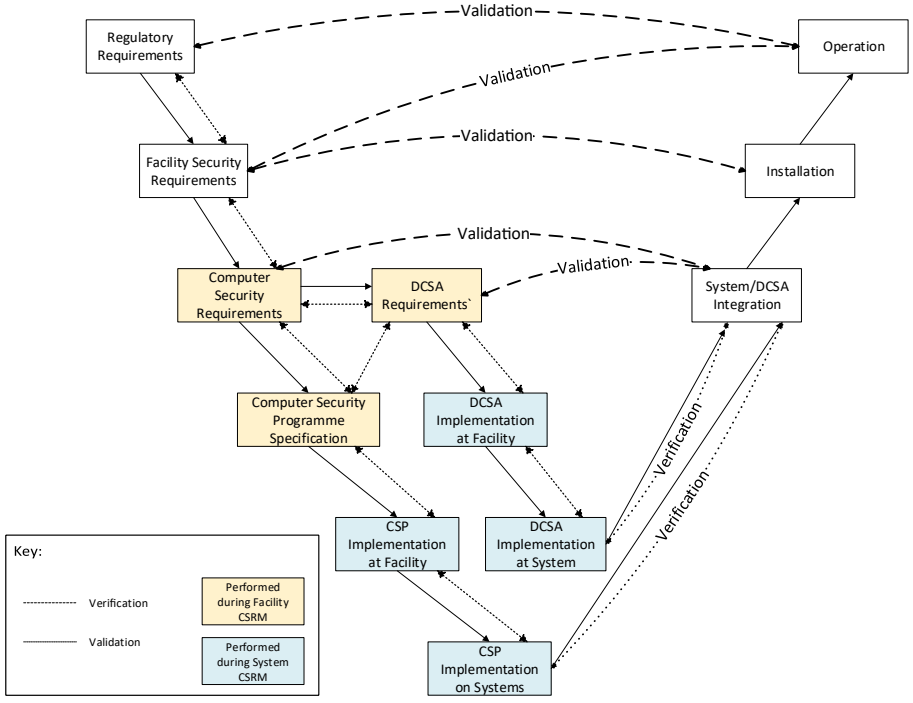


FIG. 7. Overview of verification and validation activities within the computer security risk management (CSRM) process. CSP: computer security programme; DCSA: defensive computer security architecture.

4.111. Where the validation indicates that the level of protection is not sufficient, the operator should revise its CSP and DCSA to increase protection. The operator may not reduce the level of protection without the agreement of the competent authority.

4.112. The operator should validate the outputs of both the facility and system CSRM processes. The facility CSRM outputs should be validated against the operator's and regulatory requirements. The system CSRM outputs should comply with the CSP and DCSA requirements.

4.113. The operator should aggregate facility risk level, including reference to applicable regulatory and design requirements. This should also include the system risk level for each individual system that contains an SDA.

4.114. The operator should validate the facility and system level risk assessments against the national threat statement or DBT using scenarios that involve attacks affecting multiple systems and the overall architecture. These scenarios differ from those used in system CSRM (para. 5.5(j)) and those specified in the national threat statement or DBT. They might include blended attacks involving compromise of a number of separate systems with the aim of identifying vulnerabilities somewhere in the facility.

4.115. Full validation of the results of both facility CSRM and system CSRM should include consideration of both technical and functional scenarios as described below.

Scenario identification and development

4.116. The operator should identify and develop scenarios based on the State's assessment of the threats as detailed in the national threat statement or DBT and, where appropriate, the facility specific threat assessment. Operators are strongly encouraged to include experts in cyber-attacks and related threat capabilities in the development of these scenarios. This expertise can be found in competent authorities, intelligence services and law enforcement agencies. The operator might be required to provide these detailed scenarios to the competent authority for review and acceptance.

4.117. Analysis of scenarios might provide insight into the most vulnerable points within the facility, processes, system architectures and procedures. Further analysis might be needed to identify computer security measures already in place or those that need to be added to address the identified vulnerabilities.

4.118. Scenarios should be used in verifying the results of the facility computer security risk assessment, including the analysis of possible adversary tactics, likelihood of attack and potential consequences.

4.119. The scenarios should be reassessed periodically to ensure that they remain sufficient to meet security objectives in the light of changes in the threats.

4.120. There are two categories of scenario:

(a) Functional scenarios, which are scenarios based on the threat assessments and which reflect the potential effects on facility functions of the compromise of systems performing those functions. These scenarios include those involving sabotage resulting in unacceptable radiological consequences and unauthorized removal of nuclear material. Functional scenarios can also be used to identify critical dependencies between functions or systems.
(b) Technical scenarios, which are scenarios based on the specific technical implementation of computer security measures and which involve detailed information about the actual or potential implementation of digital assets. These scenarios can be assessed through performance based or tabletop exercises, typically as part of the verification and validation of both the facility and the system CSRM outputs.

4.121. These scenarios are developed and analysed between facility CSRM and system CSRM phases, and within elements of facility CSRM if needed for analysis. These scenarios are necessary to raise confidence in the outputs of the requirement specification phase but can also be used to develop these requirements. The set of scenarios used for analysis to develop the requirements cannot be identical to the set of scenarios used in assurance activities.

4.122. Scenarios considered should include multiple attack routes (e.g. via different networks and local systems), attacks involving insiders and blended attacks. They should also include the potential for sequential cyber-attacks that multiply the consequence but that show no indications of collusion between different adversaries (non-collaborative attacks).

4.123. Scenarios can include the following:

(a) Stand-alone attacks by a single adversary;
(b) Coordinated attacks by a group of adversaries working together;
(c) Opportunistic attacks, in which independent adversaries effectively create a combined attack. For example, a vulnerability is publicly disclosed by one

adversary, which allows other adversaries to target the facility systems and equipment;
(d) Specific threat capabilities [9];
(e) Blended attacks with coordinated cyber and physical elements;

Attack tree analysis can help in identifying threat scenarios as well as in identifying protective strategies.

4.124. Scenarios should be periodically reviewed and updated in the following instances:

(a) When the national threat statement or DBT is updated;
(b) When significant modification of the facility is undertaken;
(c) When changes are made to security processes, critical countermeasures and architectures;
(d) When new credible attack routes are identified;
(e) When new regulatory requirements are introduced;
(f) When new critical vulnerabilities[34] become known, especially those involving important computer security measures;
(g) When the threat characterization changes.

4.125. For the most significant scenarios, specific attack vectors and components should be identified and their risks documented.

FACILITY COMPUTER SECURITY RISK MANAGEMENT OUTPUT

4.126. The facility CSP documentation should describe the computer security measures required to maintain protection against adversaries analysed during the assessment.

4.127. The output of facility CSRM should comprise the facility CSP documentation and a determination of the aggregate facility risk based on an evaluation of the effectiveness of those measures identified in the CSP as providing protection against adversaries described in the national threat statement or DBT.

[34] For example, the Common Vulnerability Scoring System, version 3.0, identifies as being ‘critical’ (i.e. score of 9.0–10) those vulnerabilities that are network exploitable; have low attack complexity; and result in complete compromise of confidentiality, integrity and availability.

4.128. The facility CSRM report should include a high level review and analysis of security system design and configuration management as detailed in the CSP. A more detailed analysis should be performed during system CSRM.

4.129. Facility functions and their corresponding systems in the facility CSRM output should be addressed in comprehensive system level risk assessments as described in Section 5.

4.130. The operator's assessment of risk associated with different functions and aggregate facility risk should be provided to the competent authority.

5. SYSTEM COMPUTER SECURITY RISK MANAGEMENT

GENERAL CONSIDERATIONS

5.1. The operator should establish a systematic and periodically reviewed process for managing the computer security risk to digital assets, including SDAs, within the systems that perform the facility functions identified in the facility CSRM process[35]. Compromise of SDAs typically has the potential to lead to very high, high or medium severity consequences (as described in Ref. [7]). Facility CSRM should include system CSRM for each system, as described in this section. System CSRM should consider all digital assets in the system, including SDAs.

5.2. System CSRM should be performed by a multidisciplinary team similar to that for facility CSRM. However, the composition of the system CSRM team may be tailored to address specific considerations associated with each system.

5.3. The operator should use a graded approach when determining the level of effort to be applied to risk management for each system. The greatest level of effort should be applied to those systems that perform or support the facility functions assigned to the most stringent computer security levels (i.e. those requiring the greatest level of protection) as determined in the facility CSRM process.

---

[35] It might be justified to extend this analysis to include other systems excluded from the scope of the facility computer security risk assessment that are not directly relevant to nuclear security objectives.

OVERVIEW

5.4. The primary objective of the system CSRM is to evaluate and manage the computer security measures to ensure that they provide the appropriate level of protection for the specific system (i.e. that required for its computer security level) according to the requirements defined in the facility CSRM output.

5.5. To meet this objective, system CSRM includes the following steps:

(a) Assessing each facility function, the systems assigned to perform the function and the computer security level applied to those systems — taking account of other facility functions that have interactions and interdependencies identified in the facility characterization phase of facility CSRM — to define the functional boundaries of the systems.
(b) Identifying the scope of each system, including those systems that support other facility functions that interact with and depend on the function performed by the system. This can include analysis of the overall system architecture to identify the locations, boundaries, interfaces and communication paths of systems containing digital assets, including SDAs.
(c) Identifying (and creating an inventory of) digital assets within those systems.
(d) Defining and establishing computer security zones on the basis of the requirements identified in the facility CSP and the DCSA.
(e) Identifying SDAs and other digital assets within the zone boundaries by asset analysis, which is an assessment of the digital assets to determine whether they are vital to the performance of the facility function.
(f) Assigning digital assets, including SDAs, to the computer security level assigned in the facility CSRM output to their facility security or safety function.
(g) Applying to the whole zone the most stringent computer security level assigned to any of the functions provided by digital assets within the zone, and assigning all of the digital assets within the zone to that level.
(h) Applying baseline computer security measures (see paras 4.58 and 4.68) and additional computer security measures to the SDAs and other digital assets (including at the zone boundaries), taking into account the specificities of the identified systems to meet the requirements of the assigned computer security levels.
(i) Providing a process to determine the technical control measures, administrative control measures or physical control measures that can be applied to meet the baseline computer security measures.
(j) Analysing specific attack routes, scenarios and vulnerabilities to verify the effectiveness of the applied computer security measures.

(k) If the analysis shows that a system is not sufficiently protected by the baseline computer security measures, applying additional or compensatory measures to reduce the risk to an acceptable level.
(l) Developing a system CSRM report for the identified system.

5.6. This process may result in the identification of other digital assets that were not part of the systems assigned to facility functions during facility CSRM, or were identified as being outside a system or zone boundary during system CSRM. In such cases, additional analysis should be performed to ensure the inclusion of all associated digital assets in the assessment and the CSP.

5.7. The outputs of system CSRM should include the prioritization of risks within the system to determine the appropriate implementation of computer security measures. The process should include consideration of the location of the components that make up the system, vulnerabilities, and computer security levels and zones if defined, as well the significance of SDAs and other digital assets within the system under assessment.

SYSTEM COMPUTER SECURITY RISK MANAGEMENT PROCESS

5.8. The operator should perform system CSRM in the following instances:

(a) When a facility is first constructed (for every system);
(b) When a facility is modified (for every system);
(c) When a new system or digital asset is deployed (for every affected system);
(d) When a system or digital asset is modified (for every affected system);
(e) When the facility CSRM process is revised (for every system).

5.9. The following inputs should be identified and made available for use during system CSRM:

(a) Facility CSRM outputs (e.g. the CSP and DCSA specifications);
(b) The safety analysis report;
(c) The site security plan;
(d) The computer security policy.

Overall defensive computer security architecture requirements for computer security

5.10. The operator should use the requirements for the DCSA set out during facility CSRM to design, implement and maintain computer security measures for systems and digital assets to prevent, detect, delay, mitigate and recover from cyber-attacks.

5.11. Computer security measures should be effective throughout the lifetime of the facility, for example during periods of maintenance and decommissioning, when significant configuration changes may be made. Monitoring, maintenance and recovery activities should not provide means by which an adversary might bypass computer security measures, for example bypassing the protection on communication pathways between facility functions that have different computer security levels.

5.12. Computer security boundaries[36] should be applied between computer security zones and should be protected using different computer security measures.

5.13. Data flow should be controlled between zones of different computer security levels and between zones of the same computer security level, using a risk informed approach, to ensure that the DCSA remains effective.

Definition of system boundaries

5.14. The system boundary defines the scope for each system's CSRM and encompasses the systems identified as providing a particular facility function on the basis of the facility characterization. This should include considerations of interdependencies between facility functions and their systems.

5.15. System CSRM should include identifying and documenting the system boundaries. These include all the components, subcomponents, interfaces and environments of the system in question during all stages in the lifetime of the facility, as well as those other systems that provide support or auxiliary functions.

[36] 'Computer security boundaries' are defined in this publication as the logical and physical boundaries of a system or a set of systems at the same security level that therefore can be secured by the application of common security control measures (i.e. computer security zones).

5.16. The following steps can be used to define the boundaries of the system under assessment:

(a) Identify all the interfaces of the system.
(b) Identify all the points at which data enter and leave the system (points at which an adversary might be likely to attempt to inject malicious code). Any means of injecting malicious code into the system should be considered in the system security risk assessment. For example, malicious code could be injected via communication connections, supplied products and services, or portable devices that are temporarily connected to target equipment.
(c) Identify the procedures that involve interaction with the system in normal operation and in specific circumstances (e.g. patching).
(d) Identify which data pathways (if any) are not used by any procedures during system operation and maintenance. Unused data pathways represent a significant vulnerability.
(e) Identify the assigned computer security level of the system (from the facility CSRM output).
(f) List the computer security measures applied to the system or its environment.

Definition and construction of computer security zones

5.17. The CSP and DCSA specifications produced during facility CSRM place computer security requirements on the implementation of the zone model. The CSP will also include a list of facility functions and the systems assigned to them.

5.18. The operator should implement computer security measures to meet the requirements set out in the DCSA specification. In doing so, consideration should also be given to achieving the following [8]:

(a) Systems belonging to the same zone form a trusted area for internal communications between those systems, and the computer security level applied throughout a zone that has such a trusted area is the most stringent level of those assigned to the systems involved.
(b) Safety architecture requirements (e.g. redundancy, diversity, physical and electrical separation, single failure criterion) are maintained.
(c) Defence in depth is applied both within each computer security zone (by using diverse, independent and overlapping administrative, physical and technical control measures) and between computer security zones.
(d) Technical control measures to provide continuous or automatic preventive or protective actions (i.e. requiring no human intervention) complement

physical or administrative control measures (i.e. requiring human intervention) where appropriate.

(e) All connections between zones have decoupling mechanisms for data flow, operating according to zone dependent rules to prevent unauthorized access and undesired interactions between the zones. This includes continuous network connections and intermittent connections, for example using removable media.

(f) The level of decoupling between zones is dependent on the computer security levels of the two zones. Decoupling measures include technical control measures, such as packet filters, firewalls and data diodes, at zone boundaries to restrict data flow and communication between different zones.

(g) Permitted communications between zones at different security levels follow requirements specified for the levels involved in the CSP. The development of requirements for permitted communications may include consideration of trust models (see para. 4.83).

(h) If the requirements in the CSP permit SDAs from zones assigned to different security levels to communicate, the connection is allowed to be initiated only by the SDA assigned to the higher (more stringent) computer security level. SDAs performing sensitive information management functions typically do not allow for communication from higher to lower levels (i.e. information flows in the opposite direction), in accordance with the Bell–LaPadula trust model (see para. 4.83).

(i) If communication initiated by the SDA subject to the lower computer security level[37] is unavoidable and in violation of its trust model, exceptionally stringent decoupling mechanisms are used.

(j) Logical or physical access to digital assets in a zone by permitted mobile devices or other temporary equipment is treated as a form of intermittent connection to that zone and is subject to computer security measures for both the established zone and the temporarily connected devices. Such devices are subject to additional computer security measures if they connect to more than one zone.

(k) Zones can be partitioned into subzones to improve the configuration and to prevent undesired interactions with other systems.

[37] Some Member States do not permit this direction of communications from lower levels to the highest levels for high or very high consequence facilities. In other types of facility (e.g. nuclear fuel cycle facilities, small modular reactors), the competent authority may allow for operator discretion in the application of bidirectional pathways.

5.19. Digital assets should be considered for separation into distinct zones when any of the following conditions are met:

(a) The digital assets belong to systems that perform different facility functions.
(b) Systems contributing to the same facility function are assigned different computer security levels.
(c) Systems contributing to the same facility function and assigned the same computer security level are managed by different organizational units.
(d) Servers communicate with multiple clients (e.g. those used with distributed control systems and programmable logic controllers). The zone requiring the most stringent protection should contain the minimum possible number of unique assets.
(e) Systems need to communicate with common infrastructure components used by multiple systems (e.g. directory services, time servers, security log collectors) but not with one another. Communication between zones containing these types of system and zones containing the common infrastructure components needs to be monitored and controlled.
(f) The systems are administration systems (especially when the same systems are used to administer several functional systems).
(g) Regulations require distinct zones.

5.20. Digital assets may be considered for assignment to different zones, despite being assigned the same computer security level, in the following cases:

(a) The digital assets are in systems performing different facility functions. In such cases, assignment of digital assets to different zones may improve the separation of the zones and systems that contribute to a facility function.
(b) Different organizational units are responsible for different digital assets.
(c) There are isolated digital assets, or several digital assets of the same functional system are hosted on an isolated network.
(d) Separate redundant systems performing the same facility function need to be assigned to individual zones.
(e) Regulations require separation of the digital assets.

5.21. Network connections and local exchanges (e.g. via removable media or mobile devices) of data between systems in different zones should be limited to only those that are essential. Where network connections across zone borders are essential, they should be established from the zone with the higher computer security level to the zone with the lower computer security level. Restrictions can be applied using technical control measures (e.g. filtering devices) or administrative control measures (e.g. rules for the use of removable media on a specific system).

Network connections and methods that are permitted for disconnected exchange of data should be documented.

5.22. A specific zone can only include systems (and digital assets) of the same computer security level. The zone is assigned the computer security level of the systems within the zone. A given computer security level can and should apply to different zones. However, in some specific cases it might be difficult to separate systems assigned to different computer security levels into different zones. In such cases, some systems could become part of a zone assigned a more stringent computer security level than they need.

5.23. Communications should be allowed only between zones of the same computer security level or adjacent levels. Communications between zones with different computer security levels should be limited to specific zone entry points (e.g. one entry point filtering connections between zones with computer security level 2 and zones with computer security level 3). Security measures for all entry points should be defined in an efficient and consistent manner to enforce a secure overall architecture. Specific checks should be applied at a zone entry point, for example on the content of data (e.g. acceptable ranges of parameter values) entering or leaving, or the data's digital signature. Zone entry points should also have specific event log monitoring.

Identification of digital assets

5.24. The following records should be consulted when identifying a system's digital assets:

(a) System asset database (of all digital components);
(b) Software and firmware inventory;
(c) Lists of sensitive information relevant to the system [5];
(d) System network and architecture diagrams;
(e) Facility design documents such as the safety analysis report or test reports;
(f) Data flow diagrams;
(g) List of user and system accounts and privileges;
(h) Procedures related to the identified system.

5.25. The list of digital assets may include their identifiers, key technical specifications and data, descriptions of their interfaces, references to facility level and system level risk assessments, and their assigned owners.

5.26. The list of digital assets should be maintained during the lifetime of the facility and periodically reviewed. The list should also be reviewed and updated if necessary whenever a system level risk assessment is performed.

5.27. Digital assets that are also sensitive information assets should be designated as SDAs. Digital assets that might facilitate or contribute to an adverse effect on the function of SDAs should also be identified and considered in the digital asset analysis to determine, consistent with the CSP, whether they should be designated as SDAs.

5.28. The list of SDAs should be classified and protected as sensitive information.

System computer security architecture, including digital asset analysis

5.29. The operator should identify key tasks and activities necessary to provide computer security for the facility. These tasks and activities should be associated with computer security levels and their corresponding computer security measures. The operator should ensure that the necessary resources and capabilities are available to perform those tasks and activities.

5.30. The system CSRM process should identify all SDAs. Digital assets that are not SDAs may also need to be considered in the analysis of specific threats or types of attack if their compromise could adversely affect an SDA. The level of effort associated with the system level risk assessment should be graded to ensure that those systems assigned the highest computer security level are also subject to the most robust assessment.

5.31. In general, systems that perform the same facility function should be assigned the same computer security level, including independent, diverse and redundant systems. The assignment of a less stringent computer security level to any such systems is strongly discouraged and may be considered only on a case by case basis if supported by a specific justification and security risk analysis.

5.32. Asset analysis of SDAs should include consideration of information about the hardware, firmware and software of the SDA, which can be used as input to a vulnerability analysis. The vulnerability analysis may lead to a recommendation to perform procedures to identify, disable or remove unneeded services, ports or interfaces on the system (or network) of the SDA to reduce attack surface (i.e. system hardening; see para. A.64).

5.33. The interfaces of each system (including its digital assets) should be analysed and categorized with respect to the zone boundary. The following categories may be used:

(a) Trusted internal communications: This category would include communications within and between systems or within a zone or between digital assets within a system, including internal pathways to devices at the zone boundary (e.g. firewalls, data diodes). There are no computer security measures that can effectively monitor or protect internal trusted communication pathways against cyber-attack.
(b) Authorized external communications: This category would include connections between zones via authorized permitted pathways and boundary devices. Such communications are normally between separate systems performing different facility functions. Computer security measures in the form of boundary devices ensure that all communication pathways, whether digital or analogue, are continually monitored and only those that are authorized can be used.
(c) Potential unauthorized communications: This category would include the capability to make unauthorized connections between zones, for example using network cables, wireless connections or removable media. Such unauthorized communication pathways could be made between systems or digital assets that are in different zones but in physical or logical proximity, for example systems that are physically located in the same area with no physical barriers controlling access between them.

5.34. All digital assets with trusted internal communication pathways within a zone should be assigned to the same computer security level, namely that of the zone.

5.35. Zone boundary devices should be assigned to a computer security level equivalent to the highest (most stringent) level applied to the equipment for which they are intended to provide protection. For example, a firewall between two zones of different computer security levels may have a trusted internal communication pathway with the zone assigned the higher computer security level but only an authorized external communication pathway with the other zone.

5.36. Another example of a zone boundary device may be a malware detection kiosk, or antivirus scanner, which is used to scan removable media and mobile devices before entering and exiting a zone. This kiosk would be assigned the highest computer security level applied to anything in the zone for which it is

intended to provide protection.[38] In this case, the operator needs to ensure that the kiosk does not provide a common route for the compromise of different systems in different zones (e.g. by providing a common vulnerability that can be exploited to compromise different systems).

5.37. All digital assets, including SDAs, that are connected via a trusted internal communication pathway should comply with the overall DCSA requirements. Permitted external communications need additional computer security measures (see para. 5.33(b)).

5.38. SDAs may be allowed to be in proximity (logical or physical) to other SDAs provided that computer security measures are in place to ensure that these systems cannot interact though potential unauthorized communication pathways. These measures might be solely administrative control measures. Typically, SDAs are assigned to the higher computer security levels (e.g. levels 1–3).

5.39. Digital assets that are not authorized to communicate with SDAs should not be allowed to be in logical or physical proximity to SDAs where there is the potential to have unauthorized communication pathways. The DCSA should provide for the design and maintenance of robust computer security measures to eliminate such pathways or create compensatory measures to reduce the potential for them to be used.

5.40. Unassigned digital assets (i.e. those not assigned to a computer security level) should never be in proximity to SDAs. For example, a vendor's equipment or personal mobile devices that have not been evaluated and assigned should be treated as potentially malicious devices to SDAs and should not be allowed in logical or physical proximity to facility SDAs.

5.41. Asset analysis should include assessing the effects of credible scenarios of cyber-attack on the system and the risk to the facility. The assessment should take account of the possibility that cyber-attacks might occur during any stage of the lifetime of the facility or any phase of the system's life cycle.

5.42. Cyber-attacks might affect an individual system or multiple systems and could be used in combination with other forms of malicious act causing physical

[38] Such kiosks might be unsuitable to protect level 1 or level 2 systems owing to difficulties in applying computer security requirements to a stand-alone kiosk. Additionally, kiosks using malware detection that relies solely on 'blacklisting' or signature approaches cannot provide a high level of protection.

damage. These potential specific component level interactions should be listed within the assessment report and assessed.

5.43. The assessment should include consideration of malicious actions that could change process signals, equipment configuration data or software.

5.44. The asset analysis should include identifying the locations at which information is stored and the pathways by which information flows within the system (including its digital assets). The analysis should also identify and justify the measures in place to protect the necessary data flows and communications and to identify any possible remaining vulnerabilities. The analysis could be supported by the following:

(a) Analysing or testing the effectiveness of the security measures;
(b) Documenting the status of the measures, including defining possible improvement points;
(c) For identified systems, ensuring that the software has been subject to a vulnerability assessment.

5.45. For example, consider the exchange of software (e.g. source code, object code) between a development environment and a security system. If no computer security measures are in place, then the compiler (hardware and software) will be assigned to the same zone (and computer security level) as the security system itself, since no boundary exists. However, if security measures are applied at the boundary between the compiler and the system — for example, testing the integrity of data and identifying any vulnerabilities in the code coming from the compiler — the compiler could be placed in a separate zone and assigned to a computer security level different from that of the system itself. The measures applied to the compiler's output are accredited with protecting the system and so would be assigned the same level as the system to which they are providing the protection.

5.46. The analysis of digital assets should produce a list and description of the specific computer security measures that are implemented for each system. The measures should be a combination of technical, administrative and physical control measures.

5.47. The analysis of digital assets should provide a qualitative or quantitative value of the acceptable risk threshold.

Verification of the system computer security risk assessment

5.48. The operator should verify and validate the system computer security risk assessment for each system as defined by the scope of the assessment. The verification of system CSRM outputs may use the evaluation methods outlined in para. 4.98 for facility CSRM.

System scenario identification and development

5.49. The national threat statement or DBT provides a basis for the generation of credible scenarios based on the motivation, capabilities, intentions and opportunity of potential adversaries (including adversaries using cyber techniques).

5.50. The operator should develop credible scenarios for each system on the basis of the threat characterization as a basis for the validation of the computer security measures that provide protection to the system. The credible scenarios should include potential sequences of adversary actions that might result in compromise of SDAs.

5.51. Scenarios should include common attack routes and techniques. These may include the following:

(a) Social engineering, including phishing attacks;
(b) Malicious emails;
(c) Malicious web sites;
(d) Infected mobile media devices;
(e) Compromised maintenance and inspection equipment;
(f) Remote access;
(g) Insiders (witting and unwitting);
(h) Compromise of the supply chain.

5.52. Scenarios should be developed consistent with the national threat statement or DBT that applies to the facility to identify those SDAs that might be exposed to such attacks. It may be beneficial to start scenario development by considering the most likely or the highest consequence cases.

5.53. The development of scenarios should have the following aims (in order of significance):

(a) To determine the highest consequence scenarios involving SDAs;
(b) To determine the most likely scenarios involving digital assets, including SDAs.

5.54. Evaluation methods para. 4.98) should use credible scenarios (paras 4.116–4.125) to verify the effectiveness of implemented computer security measures.

5.55. The operator should verify that digital assets, including SDAs, are appropriately protected against the adversaries identified in the national threat statement or DBT that applies to the facility.

System computer security risk management report

5.56. The output of system CSRM should be documented in a report that includes the following:

(a) Identification of all SDAs, including (as far as possible) all hardware and software components of each SDA.
(b) Identification of digital assets that are components of, interface with, support or have the potential to access communication pathways connected to SDAs. These might include components of systems assigned a computer security level.
(c) Identification of known vulnerabilities, deficiencies or weaknesses in the systems or components, for example potential procurement issues (e.g. supply of counterfeit or substandard parts), or human actions or omissions that might affect security.
(d) Identification of technical, administrative and physical control measures.
(e) Recommendations for implementation of countermeasures.
(f) Recommendations for improvements to countermeasures (i.e. additional technical, administrative or physical control measures).
(g) Identification of deficiencies in facility documentation or records.
(h) Classification of sensitive information.
(i) Access control lists for personnel and services.
(j) Corrective actions, when adverse conditions appear.
(k) Assessment of the residual system level risk.
(l) Identification and description of other indicators that will assist in the evaluation of computer security (e.g. mean time between failures, mean time to repair, mean time to detect, mean time to recover, security quality metrics).

5.57. The system CSRM report should be classified as sensitive information and protected accordingly.

6. FACILITY AND SYSTEM COMPUTER SECURITY RISK MANAGEMENT CONSIDERATIONS DURING SPECIFIC STAGES IN THE LIFETIME OF A FACILITY

6.1. This section provides guidance specific to the different stages in the lifetime of a facility.

PLANNING

6.2. The operator should review its plans for the facility against the regulations of the competent authority and identify issues that need to be addressed to meet regulatory requirements.

6.3. The operator should ensure that it has a formalized methodology to perform a detailed facility CSRM process.

6.4. The operator should develop the facility CSRM process as described in Section 4.

6.5. The operator should verify that, provided that the DCSA specification can be met, the residual risk will not exceed the acceptable levels.

6.6. The operator should plan the development of the competencies needed to support computer security during all stages in the lifetime of the facility.

6.7. The planning stage may include activities in locations away from the intended facility site. The operator should apply computer security measures to the information used in these activities, and to other inputs to and outputs from the planning life cycle, that is sensitive information or makes use of sensitive information assets.

SITING

6.8. The operator should include computer security considerations in the siting stage of the facility, because some activities supporting computer security can only be performed in relation to the specific site, not remotely or generically (e.g. establishment of isolated networks, access for computer incident response

teams, identification of the availability of expertise in computer security in the local workforce).

6.9. In its siting plans for the location of major equipment, the operator should take into account the need to allow for operation of physical control measures that will be necessary to complement computer security measures.

6.10. In siting, the operator should consider the availability of local infrastructure to support computer security measures (e.g. emergency communications networks).

DESIGN

6.11. The operator should use the output of the facility CSRM work conducted during the planning stage to ensure that the facility design process provides for computer security requirements for facility functions (expressed in the DCSA and the CSP) to be met as an integral part of the system engineering activities for the facility. This applies to the design of a new facility or to the modification of the design for refurbishment or modification of the facility during the operation stage of the facility.

6.12. The design process should take into account computer security requirements that arise owing to the dependencies between facility functions, as identified during the facility CSRM process.

6.13. Computer security requirements should be provided in sufficient detail to allow design decisions to be made, the design to be verified and design changes to be evaluated.

6.14. The operator should perform system CSRM for each system, including verification at each step of the design of the computer security measures.

6.15. Physical and remote accessibility of the SDAs within vital areas by an insider should be considered at the design stage.

6.16. The operator should develop computer security validation criteria for the commissioning stage. Systems performing facility functions assigned the highest computer security levels should be independently validated.

6.17. Staff knowledgeable in computer security from different parts of the operating organization should be involved in the design process to ensure the following:

(a) Appropriate computer security requirements are included.
(b) Design changes improve and do not degrade computer security.
(c) The changes, as implemented, meet the defined computer security requirements.
(d) The effectiveness review includes computer security.

6.18. The design should include the necessary directions for implementation of the computer security requirements. Design information, such as analysis reports, should be retained so that it is available in the future to authorized users of the design.

6.19. Because design documents might contain sensitive information related to computer security, all design documents should be classified according to the information classification scheme and protected accordingly.

6.20. The operator should ensure that any computer security requirements that need to be followed by vendors, contractors and suppliers are specified in their contracts[39] [19]. Vendors, contractors and suppliers should be required to have computer security management systems and secure engineering environments in place and to apply security by design to the SDAs that they produce or supply.

CONSTRUCTION

6.21. The operator should ensure that physical, administrative and technical control measures are established during the construction process to maintain the preventive and protective measures required by the CSP and the DCSA. For example, if lockable doors are to be installed on an enclosure, the locks should be installed and placed under control before installing SDAs within the enclosure, or appropriate compensatory measures should be put in place.

[39] The International Organization for Standardization and the International Electrotechnical Commission 'common criteria' standard ISO/IEC 15408 [18] is one possible tool to inform potential security requirements.

6.22. The operator should ensure that the following computer security actions are performed as required by the CSP and the DCSA during the construction stage:

(a) Assurance activities (i.e. testing, assessments, audits);
(b) Use of staging areas, with process and security controls to verify that SDAs have not been tampered with;
(c) Management of staff and verification of products of vendors, contractors and suppliers (both on the site and working remotely), from fabrication to installation;
(d) Supply chain evaluation and management, ensuring that the verified procurement process is followed consistently and is not tampered with.

COMMISSIONING

6.23. The operator should include the testing of computer security measures in its acceptance testing for the delivery of systems to the facility from the system provider.

6.24. The operator should perform configuration and testing activities during system and DCSA integration (see Fig. 7) to meet computer security requirements. For example, the following activities should be performed:

(a) Passwords and secondary authentication methods for digital assets should be changed according to approved procedures.
(b) Development and construction accounts for digital assets should be removed, and technical control measures should be enabled.
(c) System support tools (software and hardware) should be submitted for testing and evaluation using appropriate computer security measures.

6.25. The operator should perform validation testing of the computer security measures. Validation of computer security measures and physical protection measures should be conducted jointly to ensure appropriate integration.

6.26. If there is a conflict between safety measures and security measures, then the measures to ensure safety should be maintained and the operator should find a solution that also meets computer security requirements. Until such a solution is in place, compensatory computer security measures should be implemented to reduce the risk to an acceptable level and should be supported by a comprehensive justification and security risk analysis. The compensatory measures should not

rely solely on administrative control measures for an extended period. The absence of a security solution should never be accepted.

6.27. Review and approval of applicable CSP documents and supporting materials (required for system operation) should be completed prior to operation.

OPERATIONS

6.28. The operator should assign continuing responsibility for design change, management, maintenance and operations of the entire CSP to an individual (supported as necessary by others with appropriate skills and knowledge).

6.29. The operator should maintain documentation that describes how computer security measures are implemented, in compliance with the CSP, the DCSA and any externally imposed requirements.

6.30. The operator should ensure that operational requirements are consistent with the computer security level of systems and digital assets. For example, the following might need to be considered:

(a) Access restrictions, access control and monitoring may be different for equipment assigned to different computer security levels.
(b) Different levels of trustworthiness check may be required for personnel working on different systems, depending on their assigned computer security level.
(c) Duties may be segregated.

6.31. Actions applied to systems as part of a vulnerability assessment might lead to plant or process instability and should therefore only be considered using test beds or spare systems, during factory acceptance tests or during long planned outages.

Maintenance

6.32. This section applies to short duration maintenance activities that are routinely performed during the operations stage. Extended maintenance (e.g. refurbishment, replacement of systems, repair) is addressed in the design, construction and cessation of operations stages.

6.33. The operator should ensure that maintenance activities are performed in a manner consistent with the computer security level of the system or digital asset

being maintained. For example, in addition to the general considerations during operation listed in para. 6.30, the following steps should be taken:

(a) The permitted maintenance activities should be specified.
(b) The necessary access for maintenance should be identified and controlled.
(c) Maintenance equipment may be restricted for use only within a specific computer security zone (or for a specific system or digital asset) or only for systems at a specific computer security level.
(d) Secure maintenance environments may be required for some systems or digital assets.

6.34. Systems might be at greater risk during maintenance, when computer security measures might be removed or disabled. Furthermore, there may be additional access routes during maintenance, for example arising from the need to enable remote maintenance interfaces or the use of removable media to configure or upgrade software.

6.35. The operator should put adequate compensatory measures in place when the normal computer security measures are removed or disabled. Examples include the following:

(a) Compensatory measures should provide physical protection when equipment is unlocked.
(b) The need for remote interfaces for maintenance should be identified (and justified) in advance and appropriate computer security measures should be applied to such interfaces in accordance with the CSP.
(c) The use of computer based tools (e.g. measurement, testing and calibration equipment) should be controlled and monitored to ensure that the tools are not compromised by cyber-attack or provide a route to compromise the systems on which they are used. Computer equipment that may be temporarily connected to the system — such as testing or configuring equipment — should be protected against malicious software and unauthorized data transfer. The use of external equipment for such purposes should be minimized. Any such equipment should be inspected before it is brought into the facility.
(d) Software should be checked to confirm that it is free from malicious software before it is loaded on to the system. This may include verifying that the software has not been tampered with and is authentic, for example through software signing with cryptographic hashes.
(e) Safety measures (e.g. concurrent verification by a second party) can also be used for security purposes.

CESSATION OF OPERATIONS

6.36. During the cessation of operations stage, large scale modifications may be conducted in parallel, affecting multiple systems.

6.37. The operator should consider applying compensatory measures to address any risk arising from modifications to or degradation of security systems resulting from environmental or structural changes. This may include placing a greater reliance on administrative control measures and on vendors, contractors and suppliers to implement such measures.

6.38. Examples of changes for which compensatory measures may be applied include the following:

(a) Computer security architectures and measures being modified or disabled to allow modification work to take place.
(b) Fluctuations in staffing levels, possibly including new personnel being brought on-site to perform activities involving digital assets, including SDAs. This may require that additional trustworthiness checks or other measures be put in place to address the insider threat.
(c) Significant replacement of components, which need the creation of a secure installation environment, secure storage, and additional measures for handling and secure sanitization of replaced SDAs.

DECOMMISSIONING

6.39. When digital assets are decommissioned, the effect of this decommissioning (including any loss of integration with other digital assets outside the facility) on computer security should be evaluated and documented. If decommissioning of a system or digital asset reduces the effectiveness of computer security measures, the operator should put compensatory measures in place.

6.40. As the set of facility functions changes, the digital assets supporting these functions may be reassigned to a different computer security level or be unassigned. This might lead to a need to modify computer security measures for those digital assets.

6.41. The operator should ensure the secure destruction of any digital assets containing sensitive information that cannot be securely declassified when they are decommissioned.

7. ELEMENTS OF THE COMPUTER SECURITY PROGRAMME

COMPUTER SECURITY REQUIREMENTS

7.1. The computer security policy and programme should provide the basis for computer security requirements defined by the results of facility and system CSRM (Sections 4 and 5, respectively) and in consideration of the specific stages in the lifetime of the facility (Section 6).

7.2. Computer security at nuclear facilities should be recognized by senior management and managers as a cross-cutting discipline that needs specialized knowledge, expertise and skills.

7.3. Senior management has overall responsibility for computer security at a nuclear facility and needs awareness and understanding of the cyber threat and the potential adverse effect of a cyber-attack on nuclear security.

7.4. Senior management should ensure that all the operator's interactions with others and all internal processes are consistent with legal and regulatory requirements related to information and computer security.

7.5. Managers should promulgate the beliefs and values of nuclear security culture as they pertain to computer security. This includes promoting recognition that a credible threat exists from adversaries with cyber skills, and that these adversaries (including insider threats) might target nuclear facilities via a cyber-attack or a blended attack.

Computer security policy

7.6. A computer security policy sets the high level computer security goals of an organization. The computer security policy should begin with a clear statement of why it is being established and should define the issue being addressed, as well as the goals and the consequences if the policy is not followed. The policy should be consistent with the State's computer security policy and appropriate regulatory requirements. The policy should be enforceable and achievable and should include indicators that can be measured and audited.

7.7. The operator's computer security policy should take into account the results of facility CSRM (see Section 4). The computer security policy should

require the protection of digital assets, including SDAs, against compromise from cyber-attacks. Individual policy clauses should be clear and concise in identifying these requirements. Implementation of the requirements is addressed in detail in the CSP.

7.8. The computer security policy should be endorsed and enforced by senior management. It should identify the organization or individual that owns the policy and the CSP.

7.9. The computer security policy should be part of the overall facility security policy and should be coordinated with other relevant security responsibilities. When establishing a computer security policy, its effect on legal aspects and human resources also needs to be considered.

7.10. The computer security policy may identify potential penalties and disciplinary actions against personnel not complying with the policy requirements.

7.11. The computer security policy should be reflected in the CSP and through other lower level CSP elements that support implementation of computer security.

7.12. The policy needs to set out clear indicators that will be used to demonstrate that policies are being met in all aspects and that each aspect is being performed satisfactorily.

Computer security programme

7.13. The CSP contains details of how the goals set out in the computer security policy are achieved. The CSP establishes the organizational roles, responsibilities, processes and procedures for implementing the computer security policy. A CSP may be specific to a facility (including its associated buildings and equipment) or an organization (including all its sites and organizational units).

7.14. The CSP should be developed, exercised and maintained within the framework of the facility's overall security plan.

7.15. The CSP should take account of the results of facility CSRM (Section 4). Development of the CSP may include personnel involved in computer security, physical protection, safety, operations and information technology (IT). The CSP is illustrated schematically in Fig. 8.

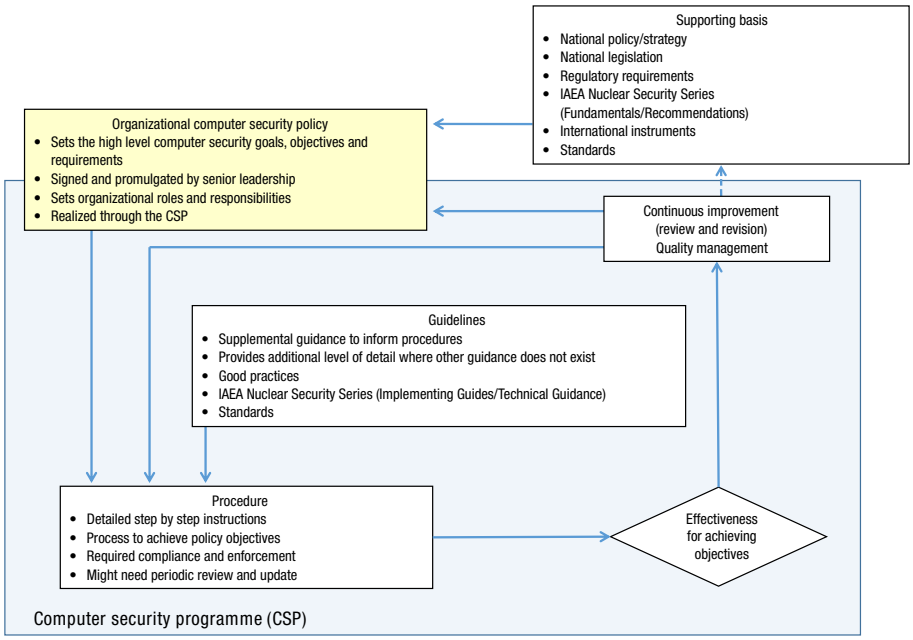


FIG. 8. Overview of a typical computer security programme.

7.16. The CSP should be reviewed and updated (a) periodically to reflect developments in technology and threats and (b) in the event of computer security incidents or other nuclear security events.

Elements of the computer security programme

7.17. Reference [7] describes the elements of a CSP generally applicable for organizations within the nuclear security regime. Paragraphs 7.18–7.20 provide more specific details on elements of a CSP for nuclear facilities.

7.18. The elements of the CSP should include addressing system vulnerabilities, applying computer security measures, performing risk analysis and conducting assurance activities to achieve an acceptable level of computer security risk.

7.19. The elements of the CSP should be adapted and applied to the different stages in the lifetime of a facility and to different phases of the individual systems' life cycles. Specific details of implementation in these different cases should be provided in the CSP.

7.20. The operator should tailor the CSP to its facility, but it is suggested that as a minimum the following areas be included:

(a) Organization and responsibilities:
  (i) Organizational charts;
  (ii) Responsible persons and reporting responsibilities (see paras A.3–A.13 of the Appendix);
  (iii) Periodic review and approval process;
  (iv) Interfaces with other programmes, such as human resources, personnel related security, physical protection and training (see paras A.15–A.38 of the Appendix).

(b) Risk, vulnerability and compliance management:
  (i) Facility CSRM process and outputs (see Section 4);
  (ii) System CSRM process and outputs (see Section 5), including the process for the classification and identification of digital assets[40], including SDAs;
  (iii) Frequency of security plan review and reassessment;
  (iv) Self-assessment practices;
  (v) Audit procedures and deficiency tracking and correction;
  (vi) Method for and occasions to start or repeat risk and vulnerability assessment;
  (vii) Regulatory and legislative compliance.

(c) Security design and management:
  (i) Fundamental security architecture (i.e. DCSA);
  (ii) Fundamental security design approaches (i.e. computer security levels and zones);
  (iii) Assignment of baseline computer security measures to each computer security level;
  (iv) Formalization of computer security requirements for contractors, vendors and suppliers, including maintenance contracts;
  (v) Security considerations for the applicable stages in the facility lifetime (see Section 6).

(d) Digital asset management:
  (i) Attributes of digital assets (identification, computer security level, zone, location, associated consequences);
  (ii) Configuration management (hardware, operating systems, firmware, software applications, equipment status, associated configurations);
  (iii) Data flow and network diagrams identifying all external connections to other systems;

[40] Digital assets include technical control measures that use digital technologies.

(iv) Supplier information for assets.

(e) Security procedures:
  (i) Security incident handling;
  (ii) Business continuity;
  (iii) System backup, restoration and recovery;
  (iv) Supply chain;
  (v) Access control;
  (vi) Information and communications management;
  (vii) Platform and application security (e.g. system hardening);
  (viii) System monitoring, including logging.

(f) Personnel management:
  (i) Trustworthiness checks;
  (ii) Awareness and training;
  (iii) Qualification of personnel;
  (iv) Reporting of security issues, including protection of staff reporting these issues;
  (v) Termination or transfer.

7.21. Further information on CSP elements can be found in international standards [19–21].

ORGANIZATIONAL ROLES AND RESPONSIBILITIES

7.22. The operator should define computer security related roles and responsibilities within the organization.

7.23. Managers should ensure that all staff understand who within the organization is responsible for leading the CSP in the functional areas relevant to their work. Staff with computer security responsibilities need to be trained in the elements of and requirements specified in the CSP.

7.24. The management of computer security should be integrated into the existing management system for the facility (see paras 7.30–7.34) to the extent possible and practicable. For existing facilities, the management system will already include well defined roles and responsibilities, and these should be adjusted to incorporate computer security.

7.25. Personnel with significant computer security responsibilities should not have conflicts of interest with other functions of the organization or with other

duties. Managers should put in place policies and processes to avoid or mitigate any potential conflicts.

7.26. The operator should ensure that individuals or organizations performing key assessment and verification activities are appropriately qualified and independent.

7.27. Computer security needs cooperation between staff in different roles and organizational units. The operator should put in place a formalized framework with the aim of ensuring interdisciplinary cooperation.

7.28. The operator needs to identify the external and internal interfaces involved in the CSP. This includes the following:

(a) Routine interfaces between the facility operator and relevant competent authorities (e.g. regulatory bodies, law enforcement, intelligence agencies, security services);
(b) Reporting to competent authorities and interface with external response forces in the event of a security incident;
(c) Internal interface with on-site response team;
(d) Public relations;
(e) Relations with vendors, contractors and suppliers, including the supply chain.

7.29. The operator should manage risk through a formalized process (i.e. facility and system CSRM) that assesses and manages risk and vulnerabilities at the facility. The operator should use the results of these processes within its management system.

Management system

7.30. The management system should be integrated to include computer security, physical protection, safety, health, environmental, quality and financial elements.

7.31. The management system should have formal and established interfaces with the facility and system CSRM.

7.32. The computer and information security goals should be defined and managed within the management system in a manner similar to other business objectives.

7.33. The management system should be reviewed to ensure its completeness and compliance with facility security policies. It should be periodically reviewed and

adapted to changing conditions in the facility and in the environment. Figure 3 of Ref. [22] illustrates the continual improvement process for management systems.

7.34. The elements of the CSP (including facility and system CSRM) should be reviewed and the necessary provisions for computer security should be integrated into the management system.

Computer security indicators

7.35. Computer security indicators can be an effective tool for security managers to measure the maturity of the management system; the risk associated with potential cyber-attacks affecting SDAs; the effectiveness of different components of their security programmes; the security of a specific system, product or process; and the ability of staff within the organization to address security issues for which they are responsible.

7.36. Indicators should support decisions concerning acceptable risk and provide an input to a risk registry.

7.37. An analysis should be performed to identify parameters and establish indicators that support effective management of the CSP. Indicators that may be useful include mean time to recover (from cyber-attack), number of computer security incidents, number of restorations of SDAs (potential reoccurrences), security backlogs and vulnerability tracking information (e.g. common scoring system, mitigation effectiveness, control deployment time, patch deployment).

7.38. The use of the indicators should be integrated into the organization's management system.

SECURITY DESIGN AND MANAGEMENT

7.39. Facility and system security design is specified in facility and system CSRM (see Sections 4 and 5, respectively). One practical implementation of these outputs, namely the DCSA and measures assigned to computer security levels, is described in Section 8.

Computer security requirements

7.40. Modifications to the facility or system should be analysed to determine potential effects on security before changes are made to allow for risks to be managed.

7.41. Computer security should be considered as a factor when determining the design inputs, which include the following:

(a) Functional requirements;
(b) Interface requirements;
(c) Operational requirements;
(d) Location of equipment;
(e) Environmental considerations;
(f) Codes and standards to be used;
(g) Contractual considerations;
(h) Supply chain considerations;
(i) Logistics (e.g. coordination of complex operations involving many people, facilities or supplies);
(j) Past operating experience;
(k) Introduction of new technologies;
(l) Human factor considerations;
(m) Design requirements for each engineering discipline (including computer security);
(n) Fabrication considerations;
(o) Installation;
(p) Commissioning;
(q) Decommissioning;
(r) Financial considerations.

DIGITAL ASSET MANAGEMENT

7.42. The operator should, for each digital asset, document attributes that have significance for computer security. These attributes may include the following:

(a) Asset identifier and location;
(b) Asset configuration;
(c) Functions and operational modes;
(d) Interconnections, including power supplies;
(e) Data flow, including internal and external connections;

(f) Procedures that initiate communication, frequency of communication and protocols for such communication;
(g) Analysis of user groups;
(h) Ownership (for data and computerized systems);
(i) Computer security level and zone, and assessed consequences of failure.

7.43. Digital asset management should take into account the equipment status of technical control measures that use digital technology. Computer security operations and physical protection operations may have joint responsibility for integrated security measures, systems and procedures. Joint operational control may include control over physical devices used to protect computer equipment (e.g. rooms, doors, keys, locks, cameras, motion sensors, tamper indicators).

Configuration management

7.44. The goal of configuration management is to have detailed, up to date records of the installed software and hardware components and how they are configured. Configuration management should include information needed for the following:

(a) Identifying the need for computer security measures;
(b) Verifying that the computer security measures are implemented and configured correctly;
(c) Managing changes throughout the life cycle of the systems;
(d) Supporting computer security assessments;
(e) Understanding the reasons for changes to the computer security measures.

7.45. Configuration management includes the change management process. Computer security should be included in this process such that all changes are evaluated from a computer security perspective before implementation. For example, appropriate reviews are performed and documented before carrying out procedures that could bypass, change or reduce the effectiveness of the computer security measures in place. Personnel changes may also necessitate changes relating to computer security (e.g. credential cancellation and management).

SECURITY PROCEDURES

7.46. The operator should develop security procedures to support facility and system computer security design and management. During development of these procedures, the operator should consider the two person rule or segregation of

work duties, taking into account the appropriate trust model and the security level assigned to the zone(s) applicable to the procedure.

7.47. Procedures that provide detailed instructions on how to disable or bypass computer security measures should ensure that such activities are recorded and logged. The procedure may also provide instructions for the application of alternate or compensatory computer security measures when the baseline computer security measure is disabled.

7.48. These procedures may be new stand-alone procedures or may be integrated within existing procedures that meet one or more safety, security or organizational objectives.

PERSONNEL MANAGEMENT

7.49. Personnel management includes the necessary provisions for establishing an appropriate level of trustworthiness, enforcing confidentiality undertakings, defining required competencies and, where necessary, applying penalties or terminating employment.

7.50. Computer security activities and personnel related security activities should be coordinated to provide protection against insider threats. In particular, personnel with key security responsibilities (e.g. system administrators, security team) may require a higher level of trustworthiness. Further guidance on the protection from insider threats is given in Ref. [6].

7.51. The CSP should include provision of training and awareness raising to develop and maintain personnel and organizational competencies and qualifications that are necessary for computer security.

8. EXAMPLE DEFENSIVE COMPUTER SECURITY ARCHITECTURE AND COMPUTER SECURITY MEASURES

8.1. An example of the implementation of DCSA with five different computer security levels in a nuclear power plant is presented below. This is one possible

implementation of the graded approach; the exact choice of levels, DCSA and computer security measures should be tailored according to the facility and its environment through specific analysis.

EXAMPLE IMPLEMENTATION OF DEFENSIVE COMPUTER SECURITY ARCHITECTURE

8.2. When implementing the DCSA, the operator should consider limiting the dynamic elements of networks and individual systems to make their behaviour more predictable. This increased predictability might help in the implementation of effective computer security measures.

8.3. Zones assigned the most stringent computer security level should only be connected to zones assigned lower levels of security by fail-secure, deterministic, unidirectional data communication pathways. The direction of these data pathways should be from the zone with the more stringent computer security level to the zone with the less stringent computer security level.[41] Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.[42]

8.4. Digital devices or communications used for monitoring, maintenance and recovery should not bypass computer security measures used to protect communication pathways between devices that have different computer security levels.

8.5. Systems assigned to the most stringent computer security level should be placed within the most secure zone's boundaries.[43]

8.6. Data communications between systems within the facility and the emergency centre (either on the site or off the site) should be protected by computer security measures.

---

[41] This excludes zones containing functions performing only sensitive information management, for which the direction is reversed. Sensitive information can be transmitted to restricted data networks, but not vice versa.

[42] Some Member States do not permit exceptions for high or very high consequence facilities. In other types of facility, the competent authority might allow for operator discretion in the application of bidirectional pathways.

[43] Wireless communications functions are problematic when implemented in systems that are assigned to the most stringent security level as it is difficult to provide a secure boundary for such communications.

DECOUPLING COMPUTER SECURITY ZONES

8.7. Computer security measures that ensure the logical and physical decoupling of zones are based on the requirements of the zones' computer security levels. To maintain defence in depth, a direct path connecting through several zones should not be allowed.

8.8. Technical control measures that provide security at the boundaries of zones should be designed to be resilient to cyber-attack and to provide alerts in the event of potential compromise or malicious activity.

EXTERNAL CONNECTIVITY

8.9. Where external connectivity is provided, security should be applied using the graded approach. The provision of external connectivity should meet the requirements for protecting the confidentiality, integrity and availability of sensitive information consistent with the computer security level assigned to the zone.

8.10. Appropriate access restrictions (including monitoring of access) should be applied to provide protection based on the graded approach because these external connections can serve as a route for compromise of systems at the facility.

8.11. Examples of externally accessible systems include the following:

(a) Environmental monitoring systems;
(b) Building automation systems;
(c) Fire protection systems;
(d) Communications with emergency centres;
(e) Remote vendor access (where permitted);
(f) Field devices located outside the physical security perimeter;
(g) Visitor control.

8.12. Figure 9 gives an example of one implementation of a DCSA, showing levels, zones, systems and digital assets. This is based on the guidance provided in Section 3.

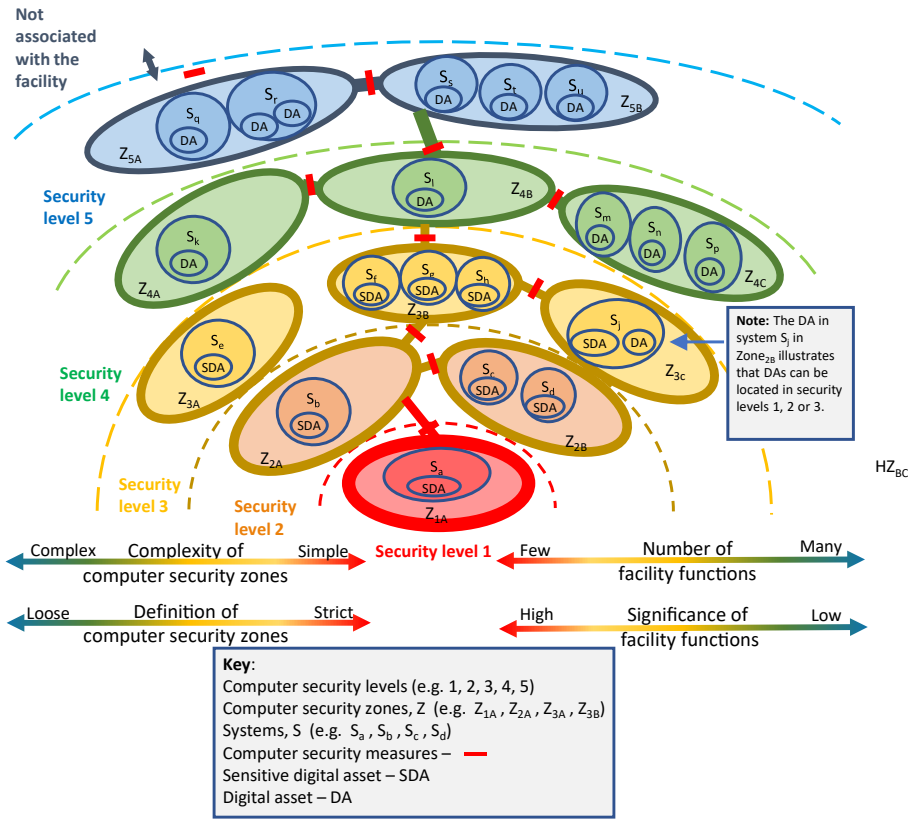


FIG. 9. Example implementation of defensive computer security architecture.

EXAMPLE REQUIREMENTS

8.13. Example security requirements applied within each computer security level are presented in paras 8.16–8.21. The exact choice of levels and their security requirements should be tailored according to the facility and its environment through specific analysis.

UNASSIGNED DIGITAL ASSETS

8.14. Two types of unassigned digital asset may be encountered:

(a) Restricted or proscribed equipment, where restrictions placed on the operator mean that the security of the digital assets cannot be assessed. This

could be due to licence conditions, or to contractual, regulatory or legal requirements that prohibit the operator from inspecting and modifying the equipment (e.g. safeguards related equipment).

(b) Unannounced equipment, which might be brought to the facility without being requested by or without the prior agreement of the operator. Such equipment is considered to be 'contraband' until a computer security risk assessment can be completed.

8.15. The operator may place restrictions on unassigned assets until they can be assessed and assigned to the appropriate computer security level and the required computer security measures can be put in place. Devices that are unassigned, for example, should not be brought into the proximity of systems that have medium to very high computer security levels.

GENERIC REQUIREMENTS

8.16. For applicable systems and levels, the following generic requirements are applied:

(a) All technical, physical, personnel and organizational security measures for systems and networks are designed and implemented in a systematic manner and according to approved processes and procedures.
(b) Policies and practices are defined for each computer security level.
(c) Users are obliged to comply with security policies and security operating procedures.
(d) Staff permitted access to the system are suitably qualified and experienced and determined to be trustworthy where necessary.
(e) Users and administrators have access only to those functions on those systems that they need for performing their jobs. Accumulation of access rights by an individual person is avoided.
(f) The system's functionality and interfaces are limited to the extent possible, with the objective of reducing overall system vulnerability.
(g) Appropriate access control and user authentication are in place.
(h) Protection against infection and spreading of malware is in place.
(i) Security logging and monitoring, including procedures for adequate response, are in place.
(j) Application and system vulnerabilities are monitored, and appropriate measures are taken.
(k) The adequacy and effectiveness of measures is reviewed periodically.
(l) System vulnerability assessments are undertaken periodically.

(m) Removable media are controlled in accordance with security operating procedures. Privately owned devices are not allowed to be connected to systems and networks.
(n) Digital assets and associated computer security measures are strictly maintained using the applicable change management procedures.
(o) Appropriate backup and recovery procedures are in place.
(p) A service device is assigned to exactly one computer security level.
(q) Physical access to components and systems, including service devices, is restricted according to their functions.
(r) Measures to prevent the unauthorized introduction of systems into computer security zones are in place.
(s) Only approved and qualified users are allowed to make modifications to the systems.

SECURITY LEVEL 1 REQUIREMENTS

8.17. In addition to the generic requirements, requirements for preventive and protective measures are used for systems that are vital to the facility and require the highest level of security (e.g. reactor protection systems). These requirements can include the following:

(a) Systems are designed and implemented to be verifiable and testable against a potential attack by an adversary.
(b) No networked data flow of any kind from systems assigned less stringent computer security levels can enter level 1 systems when integrity and availability are priorities. Only outward communication is possible. Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.[44]
(c) No remote maintenance access is allowed.
(d) Physical and logical access to systems is strictly controlled, monitored and recorded.
(e) The number of staff given access to the systems is limited to an absolute minimum.
(f) The two person rule is applied to prevent unauthorized actions by an insider threat.
(g) All activities and potential security events are logged and monitored.

[44] Some Member States do not permit exceptions.

(h) Connection of external storage devices is approved and verified on a case by case basis.
(i) Strict organizational and administrative procedures apply to any modifications, including hardware maintenance, software updates and software modifications.

SECURITY LEVEL 2 REQUIREMENTS

8.18. In addition to the generic requirements, requirements for preventive and protective measures should be used for systems, such as operational control systems, that require a high level of security. These requirements can include the following:

(a) Only an outward, unidirectional networked flow of data is allowed from level 2 to level 3 systems. Only necessary acknowledgement messages or controlled signal messages can be accepted in the opposite (inward) direction (e.g. for TCP/IP (Transmission Control Protocol/Internet Protocol)).
(b) Remote maintenance is not allowed.
(c) The number of staff given access to the systems is kept to a minimum, with a clear distinction between users and administrative staff.
(d) Physical and logical access to systems is strictly controlled and documented.
(e) Administrative access from other computer security levels is avoided. If this is not possible, such access is strictly controlled (e.g. by adopting the two person rule and two factor authentication).
(f) All reasonable measures are taken to ensure the integrity and availability of the systems.

SECURITY LEVEL 3 REQUIREMENTS

8.19. In addition to the generic requirements, requirements for preventive and protective measures should be used for real time systems that are not required for operations (e.g. process supervision systems in a control room), if all such systems have a medium severity level for various cyber threats. These requirements can include the following:

(a) Access to the Internet from level 3 systems is not allowed.
(b) Logging and audit trails for key resources are monitored.

(c) Security gateways are applied to protect this level from uncontrolled data connections from level 4 systems and to allow only specific and limited activity.
(d) Physical connections to systems are controlled.
(e) Physical and logical access to systems is controlled and documented.
(f) Remote maintenance access is allowed on a case by case basis provided that it is robustly controlled; the remote computer and user follow a defined security policy, specified in the contract.
(g) System functions available to users are controlled by access control mechanisms and based on the 'need to know' rule. Any exception to this rule is carefully considered and protection is ensured by other means (e.g. physical access).
(h) Administrative access from other computer security levels is avoided wherever possible. If this is not possible, such access is strictly controlled (e.g. through two factor authentication).

SECURITY LEVEL 4 REQUIREMENTS

8.20. In addition to the generic requirements, requirements for computer security measures should be applied to technical data management systems that are used for maintenance or operation activity management related to components or systems required by the technical specification for operation (e.g. work permit, work order, tag out, documentation management), if such systems need medium levels of computer security. These requirements can include the following:

(a) Access to the Internet from level 4 systems is not allowed.
(b) Security gateways are implemented to protect this level from unauthorized data communications through trusted and approved external company or facility networks and to allow specific activities that are authorized.
(c) Physical connections to systems are controlled.
(d) Remote maintenance access is allowed but controlled; the remote computer and user follow a defined security policy, specified in the contract.
(e) System functions available to users are controlled by access control mechanisms. Any exception to this rule is carefully considered and protection is ensured by other means.
(f) Remote external access is allowed to selected services and for approved users, provided that appropriate access control mechanisms are in place.

SECURITY LEVEL 5 REQUIREMENTS

8.21. Requirements specifying computer security measures should be used for systems not directly important to technical control or operational purposes (e.g. office automation systems), if such systems need low levels of computer security. These requirements can include the following:

(a) The computer security level does not fall below a baseline protection level, defined according to the latest state of the art.
(b) Only approved and qualified users are allowed to make modifications to the systems.
(c) Access to the Internet from level 5 systems is allowed, provided that adequate preventive and protective measures are applied.
(d) Remote external access is allowed for authorized users, provided that appropriate measures are in place.
(e) Physical connection of third party devices to systems and networks is technically controlled. Those interfaces to higher level systems are characterized and evaluated independently to ensure compliance with the computer security architecture.

Appendix

SELECTED ELEMENTS OF A COMPUTER SECURITY PROGRAMME

A.1. This appendix provides examples of selected CSP elements for use with the performance based approach to computer security. An operator may need to modify these elements to reflect particular organizational or facility specific circumstances, but the examples cover all the types of information that the operator needs to develop and implement an effective CSP.

A.2. The operator should require these or similar elements to facilitate understanding between organizational units, vendors, contractors and suppliers, and competent authorities. The elements may need to be tailored to the specific characteristics of the operating organization and facility to improve understanding.

FACILITY ORGANIZATION AND RESPONSIBILITIES

Management

A.3. Senior management at a facility establishes a computer security policy as well as processes and support mechanisms to ensure that the policy is implemented. To achieve this, senior management should take the following steps:

(a) Assume overall responsibility for all aspects of computer security.
(b) Define security objectives for the facility.
(c) Ensure compliance with relevant laws and regulations.
(d) Maintain awareness of the current nuclear security threat and associated trends.
(e) Set the risk acceptance level for the facility.
(f) Assign organizational responsibilities for computer security.
(g) Ensure adequate communication between personnel responsible for different aspects of nuclear security.
(h) Ensure compliance with the computer security policy.
(i) Provide adequate resources to implement a sustainable CSP.
(j) Ensure periodic reviews and updates of the computer security policy and procedures.
(k) Ensure support for training and awareness programmes.

Computer security specialist

A.4. The operator should assign overall responsibility for computer security at the facility to one individual or group. In this publication, the title 'computer security specialist' is used to define that role.[45]

A.5. The computer security specialist should coordinate closely with activities throughout the facility, but in an independent manner. The computer security specialist should have clear and accessible reporting lines directly to senior management, as computer security can affect almost all facility activities.

A.6. Computer security responsibilities within different organizational departments should be clearly defined and coordinated to avoid gaps or conflicts and to ensure that computer security is implemented in a coherent manner. This is especially necessary if the computer security specialist role is assigned to a group rather than to one individual: the computer security specialist should constitute one single authority within the operating organization, responsible for addressing organization-wide issues and resolving any conflicts that might arise.

A.7. The computer security specialist should have in-depth knowledge of computer security and good knowledge of other aspects of security in nuclear facilities, as well as knowledge of nuclear safety and project management and the ability to integrate people from different disciplines into an effective team.

A.8. The computer security specialist should have the authority and responsibility for administering the CSP.

A.9. The typical specific responsibilities of the computer security specialist include the following:

(a) Advising senior management on computer security.
(b) Leading the computer security team.
(c) Advocating computer security within the organization, including improvements when necessary.
(d) Coordinating and controlling the development of computer security activities (e.g. implementing computer security policy, specific directives and guidelines, procedures and, ultimately, computer security measures).

[45] In other instances, this function may be referred to as 'computer security officer', 'chief information security officer', 'IT security officer' or 'information security officer', or may be assigned to multiple roles.

(e) Coordinating with physical protection personnel and other security and safety personnel to plan and specify computer security measures, including those to respond to computer security incidents.
(f) Identifying systems critical to computer security within the facility (i.e. those providing baseline computer security measures). Asset owners should be informed of their equipment's role in computer security.
(g) Conducting periodic computer security risk assessments, independently from operational staff.
(h) Conducting periodic inspections, audits and reviews of the baseline computer security measures and providing status reports to senior management.
(i) Developing and arranging computer security training and qualification of relevant personnel.
(j) Preparing for and leading the response to computer security incidents, including coordination with relevant internal and external personnel involved in the response.
(k) Investigating computer security incidents and developing post-incident corrective actions.
(l) Participating in assessment of overall facility security.
(m) Participating in analysis of requirements for new computer based systems.

Computer security team

A.10. The operator should identify and assign personnel to a computer security team. This team can be a fixed group of individuals or can include individuals with specific expertise as needed. The team supports the computer security specialist in fulfilling their responsibilities: the computer security specialist needs to have access to expertise in all disciplines associated with computer security, including facility safety and plant operations as well as physical protection and personnel related security.

A.11. Members of the computer security team should be responsible for advocating computer security in their respective organizational units.

A.12. The computer security team's activities include actively monitoring digital assets, including SDAs, for any indications of a possible cyber-attack, and coordinating response to computer security incidents. This might include staffing a security operations centre for the monitoring and assessment of potential computer security incidents and for the initiation and support of response activities, which might also need support from other organizations.

Other management responsibilities

A.13. Managers at different levels within the organization should ensure that appropriate attention is paid to computer security within their areas of responsibility. Typical responsibilities of managers in their respective areas include the following:

(a) Understanding the significance and the role of computer security in nuclear security;
(b) Operating within the requirements and processes defined by the CSP;
(c) Providing operational requirements and feedback to senior management relevant to computer security, and resolving any conflicts between operational, security and safety requirements;
(d) Alerting senior management to any conditions that might lead to changes in the level of computer security, such as changes in personnel, equipment or processes;
(e) Ensuring that staff are sufficiently trained and briefed on computer security issues relevant to their roles;
(f) Ensuring that vendors, contractors and suppliers working for them operate within the requirements and processes defined by the CSP;
(g) Tracking, monitoring, responding to and reporting on computer security incidents;
(h) Enforcing computer security measures.

Individual responsibilities

A.14. Each individual within an organization should be responsible for performing their own tasks consistently with the CSP. Specific responsibilities include the following:

(a) Understanding the significance and the role of computer security in nuclear security;
(b) Understanding the organization's policy for computer security;
(c) Having knowledge of computer security procedures relevant to their job;
(d) Operating within the constraints implied by the computer security policy;
(e) Notifying managers of any changes that might adversely affect computer security;
(f) Notifying relevant points of contact and managers of any incidents or possible incidents involving a compromise of computer security;
(g) Attending initial training on computer security and refresher training on a regular basis.

Cross-department responsibilities

A.15. Computer security is a cross-cutting discipline that affects and is affected by many different organizational units and activities. Computer security needs close coordination and cooperation between different organizational units to be effective. Paragraphs A.16–A.38 describe some of the departmental responsibilities and cross-cutting issues.

Physical protection

A.16. The site security plan and the CSP are both essential in developing a comprehensive security plan for the facility, and they therefore need to complement each other. SDAs are protected by physical access control requirements, and compromise of computer based systems can lead to degradation or loss of physical protection functions. Furthermore, adversaries might seek to attack a facility through coordinated cyber-attack and physical attack (i.e. blended attack).

A.17. If the organizational units responsible for the site security plan and the CSP are different, they should communicate and coordinate their efforts to ensure consistency between the plans during the development and review process.

A.18. The operator should assign relevant roles and responsibilities in the development, implementation and maintenance of the CSP to physical protection personnel. These may include the following:

(a) Ensuring that only authorized access is permitted to SDAs;
(b) Identifying unauthorized removable media and mobile devices entering the facility;
(c) Identifying unauthorized removal of information or information assets from the facility;
(d) Ensuring that policies applicable to any removable media and mobile devices permitted in the facility are applied (e.g. scanning for malicious software before entry into the facility);
(e) Reporting computer security incidents (e.g. detection of malicious software, unauthorized removal of information assets) according to the incident response procedure;
(f) Assessing information security practices (e.g. desk checks, checking of locked rooms and cabinets, provision of standards for devices providing physical protection of information assets, access control and monitoring);

(g) Supporting incident response for computer security incidents related to the physical protection system.

Information technology

A.19. IT personnel perform support, management and administrative tasks within a nuclear facility. These tasks may include activities involving digital assets used to prepare and store operational and maintenance procedures, work instructions, configuration management systems, design documents and operating manuals.

A.20. The CSP should clearly identify the digital assets and associated networks that are the responsibility of the IT personnel. IT personnel should monitor the identified digital assets and associated networks and report any computer security incidents to senior management and the computer security specialist according to the incident response plan.

A.21. IT personnel should take actions to ensure that computer security incidents involving digital assets (but not SDAs) and networks do not propagate to affect SDAs.

Engineering

A.22. Engineering personnel should have formal processes to ensure coordination with other relevant organizational units to ensure that measures for nuclear security and nuclear safety are designed and implemented in an integrated manner consistent with the requirements set out in the CSP. Engineering personnel should recognize that safety, physical protection and computer security are distinct disciplines that need support from appropriately qualified experts in those different disciplines.

A.23. Engineering personnel should provide evidence of the effectiveness of the computer security architecture (i.e. the DCSA) that can be compared with the results expected on the basis of facility and system CSRM.

A.24. Engineering personnel should lead or support the system CSRM process for those facility systems of which they are the owner.

A.25. Engineering personnel should provide direction to vendors, contractors and suppliers regarding requirements for computer security within facility systems. Engineering personnel are responsible for reviewing vendors' designs to ensure that they meet the computer security requirements. Engineering personnel

should seek confirmation from the vendor that products supplied to the facility have been developed in a secure environment. Engineering personnel should establish and follow a procedure for reviewing technical product documentation, accepting on-site product consignments and testing products to ensure that computer security requirements are met.

A.26. Engineering personnel should ensure that performance monitoring activities are in place to confirm that computer security measures continue to be effective.

Operations

A.27. The CSP should identify those facility systems and networks that are the responsibility of operations personnel. Operations personnel are responsible for complying with the requirements for these systems set out in the CSP.

A.28. Operations personnel should ensure that the DCSA and computer security measures under their responsibility are maintained and remain effective.

A.29. Operations personnel should ensure that procedures are in place for identifying computer security incidents and initiating response for systems and networks under their responsibility.

A.30. Operations personnel should promote situational awareness to ensure that only authorized removable media and mobile devices are used within the facility.

Procurement and supply chain organization

A.31. Products should be procured to meet the specifications for the equipment, device or component. The specifications should include appropriate computer security requirements.

A.32. Procurement processes should include checks to ensure that SDAs developed or supplied by vendors and suppliers include computer security measures consistent with each SDA's assigned computer security level.

A.33. Procurement personnel should understand the importance of specific computer security requirements in procurement. These requirements should be enforced through legal agreements with vendors, contractors and suppliers, such as licences or contracts.

A.34. Procurement and engineering personnel might not know that a general purpose device will be classified as an SDA if the operator uses it in a particular application. In such cases, the devices should be procured taking into account the possibility that they might be deployed as SDAs, and appropriate computer security requirements should be applied.

A.35. Procurement personnel should work with engineering personnel to ensure that computer security requirements are specified as contractual requirements for vendors, contractors or suppliers and that designs submitted by vendors, contractors or suppliers meet computer security requirements. Procurement personnel should also inform engineering personnel if support from a vendor, contractor or supplier for an SDA is, or appears likely to be, no longer available.

A.36. Procurement personnel should consider conducting reviews of vendors, contractors and suppliers before entering into contractual agreements. Such reviews may include analysis of the processes used by the vendor, contractor or supplier to design, develop, test, implement or support SDAs or assessment of the vendor, contractor or supplier's training and experience in developing SDAs with the required levels of computer security. The reviews may also help (a) determine whether primary vendors, contractors or suppliers have in place security measures to properly evaluate the trustworthiness of subordinate vendors, contractors and suppliers and (b) ensure the provenance of SDAs, SDA components, and software and updates provided to the operator.

A.37. Procurement personnel should ensure that all vendors, contractors and suppliers of SDAs have procedures in place to notify the operator in case of any supply chain incidents with the potential to affect SDAs (e.g. compromise of SDA components, SDA technology, development processes or sensitive information).

A.38. Procurement personnel should consider ensuring that vendors, contractors and suppliers of SDAs have a trusted distribution route for delivering SDAs, SDA components, and software and updates to the operator.

RISK, VULNERABILITY AND COMPLIANCE MANAGEMENT

External relationships and interfaces for risk management

A.39. Risk management processes should include analysis of external relationships (i.e. vendors, contractors and suppliers). Responsibility and

accountability for meeting requirements derived from system CSRM should be specified in contractual arrangements.

A.40. The operator should audit and inspect relevant activities of vendors, contractors and suppliers to ensure that computer security requirements set out in the CSP are being met. Contracts with vendors, contractors and suppliers should require them to allow the operator to perform these activities.

A.41. The operator's risk management processes should take account of regulatory requirements and other external requirements affecting computer security. The operator should provide for relevant competent authorities to maintain oversight and perform inspections in respect of measures to meet these requirements.

Computer security assurance

A.42. Computer security assurance activities should be conducted throughout the lifetime of the facility, as described in Sections 4 and 5. The specific assurance activities will vary according to the stage in the lifetime. Reference [8] provides details of assurance activities applicable to I&C systems.

A.43. Such activities by an operator might include assessments (including audits), reviews, exercises and testing[46].

A.44. The operator should verify that the CSP is consistent with the operator's computer security policy (e.g. computer security assessment may be used to verify that computer security requirements reflecting the operator's policy are met). This may involve a number of complementary assessments to evaluate different elements of the CSP and their implementation. The outputs of the assessments will include identification of deficiencies and good practices, and suggestions for improvement.

A.45. These activities should form the basis for continual improvement of the CSP. To support this, assurance activities should be repeatable and reliable, and should be conducted on a periodic basis, as well as whenever a computer security incident occurs or the threat changes.

[46] Exercises and testing may also be used for other CSP elements, such as security procedures and personnel management.

A.46. Assurance activities should include the evaluation of organizational effectiveness and the measures in place to ensure correct implementation and effectiveness of computer security.

A.47. Assurance activities may be performed by internal or external groups: for example, computer security assessment can be performed by an internal team as a self-assessment activity. If the assessment is performed by external groups, the results need to be verified internally.

A.48. Internal and external assurance activities should be complemented by independent evaluations performed by external parties. Independent assessors will need access to relevant staff, documentation and equipment. Independent assessors may be members of the operating organization or external to the organization, but they need to be independent of the people who performed, verified and supervised the work being assessed.

A.49. The trustworthiness of independent or external assessors should be determined before they are permitted access to the information or facility, as the assurance activities are likely to involve sensitive computer security information. Further information on trustworthiness assessments is given in Ref. [6].

A.50. The procedures for independent assessment should include appropriate restrictions on the removal, use, storage and distribution of sensitive information and should provide for the destruction of such information when it is no longer needed.

A.51. The capabilities to conduct assurance activities should be developed and maintained to keep pace with changes in technology and the cyber threat. These capabilities are needed by both the staff performing the assurance activities and the competent authority, which might need to review the results of these activities.

Assessment scope

A.52. The operator should identify the scope of the assessment in terms of the functional and security domains.

A.53. The scope should be appropriate to the stage of the lifetime of the facility. For example, a complete assessment of computer security might be needed during some stages, whereas in other stages, assessment of specific functional or security domains might be more appropriate. (Reference [8] identifies assessment activities at various points in the I&C system life cycle.)

Assessment evaluation techniques

A.54. An assessment team should use the following techniques, as appropriate, to acquire the information the team needs to develop its conclusions and recommendations:

(a) Review of documents and records (e.g. legislation, regulations, facility records);
(b) Interviews with personnel from the relevant organizations, such as competent authority personnel, operating personnel of the facility and representatives of other organizations;
(c) Direct observation of the organization, its practices and systems, and the implementation of computer security measures.

Assessment report development

A.55. The data collection component of the assessment consists of recording observations and data of interest from the review of documents and records, interviews with staff, and direct observations. Observations might be individually significant but might also act as a collective indicator of trends at the facility or organization that might need to be addressed. Therefore, the operator should identify observations that support findings indicating trends or recurring issues.

A.56. The observations should be analysed by comparison with requirements such as national regulations, organizational procedures and industry standards, as appropriate. A finding is identified if there is non-compliance with a regulatory requirement or internal procedure. The basis used for identifying findings needs to be well defined and agreed in the planning stage of the assessment.

A.57. Observations do not always result in findings, and not all findings are negative: they may include identification of good practices, organizational practices or procedures that provide an effective, typically novel, method for meeting security objectives. Good practices for potential adoption by other organizations to improve their own computer security may be identified and reported.

A.58. In addition to findings and good practices, the assessment team may also provide recommendations and suggestions in the assessment report associated with the findings.

A.59. Recommendations provide guidelines for meeting legal and regulatory requirements or international norms (e.g. convention obligations) when appropriate. Recommendations do not normally include how to correct a problem, but rather only identify that a problem needs to be corrected.

A.60. Suggestions provide an additional level of information regarding a finding, including suggested corrective or mitigatory measures. Such information is not necessarily derived from regulatory guidance, but more typically from industry technical standards and good practice.

Example assessment method

A.61. An example assessment method is described in Ref. [23]. The example method provides a cross-domain assessment of a facility's functional operations and its computer security. This assists in ensuring coverage of processes and systems that perform facility functions, including operations, safety, security, and emergency preparedness and response.

DIGITAL ASSET MANAGEMENT

Configuration management plan

A.62. Computer security measures that protect SDAs should be managed under a configuration management plan. Such a plan should be developed and implemented by the operator and should include the following measures:

(a) Assign relevant roles and responsibilities, and define configuration management processes and procedures.
(b) Detail the configuration of the SDAs and their interactions.
(c) Identify when in the system development life cycle the SDAs are placed under configuration management.
(d) Establish the means for identifying SDAs and a process for managing computer security measures to protect them.

Baseline configuration

A.63. A current baseline configuration of SDAs should be maintained under configuration control. The baseline configuration should be updated as necessary on the basis of system performance monitoring and, for example, to reflect system hardening or the effects of modifications on computer security.

System hardening

A.64. The operator should consider putting in place a systematic process for system hardening of SDAs. System hardening is the application of a combination of administrative and technical control measures designed to make computer system components less vulnerable to cyber-attack by removing or disabling hardware and software components that are not needed for the operation or maintenance of the system. Hardware and software typically removed or disabled include the following:

(a) Unused network interfaces or protocols (including disabling of driver software);
(b) Unused peripherals (including disabling of driver software);
(c) Support for removable media;
(d) Unauthorized wired and wireless communications;
(e) Messaging services not related to the facility functions performed by the system;
(f) Social media services and applications;
(g) Servers or clients for unused services;
(h) Software compilers in user workstations and servers, except for those used for system development;
(i) Software compilers for languages that are not used in the control system;
(j) Unused networking and communications protocols;
(k) Unused administrative utilities, diagnostics, network management and system management functions;
(l) Backups of files, databases and programs used during system development;
(m) Unused data and configuration files;
(n) Sample programs and scripts;
(o) Unused document processing utilities;
(p) Unnecessary add-ins for applications (e.g. browsers);
(q) Games.

A.65. System hardening should be mandatory for SDAs that use commercial 'off the shelf' components, the functionality of which should be reduced to that needed to perform the SDAs' facility functions (or system functions).

A.66. System hardening should aim to reduce the amount of data that need to be monitored and analysed to determine the security of the protected digital asset or system. System hardening can also help the operator better understand the normal behaviour and functionality of the system.

A.67. System hardening may include the use of technology to ensure that only the approved versions of authorized computer programs are allowed to run on the SDA. The records of system hardening should include documentation of the libraries that the technology has used.

A.68. System hardening should use only secure, trusted update mechanisms. These update mechanisms should be assessed to ensure that they eliminate or minimize the potential for the update to be used as a route to attack the system being updated by, for example, ensuring that system updates are identified by encrypted signatures of authorized vendors.

Considerations for software updates

A.69. Vendors issue computer security updates, typically in the form of 'patches', to address vulnerabilities identified in their systems. Since modifications to safety systems need to follow resource intensive procedures, the immediate installation of a patch might not be possible, leaving the system at risk for some period of time.

A.70. The operator should obtain from the vendor or develop itself a list of software components used in the systems and the applicable software updates (including security patches).

A.71. The operator should have a formal process in place to ensure that computer security updates to equipment and components are assessed to determine their applicability and effect and, specifically, whether immediate installation is necessary to mitigate the associated vulnerability. The operator should either install the update or provide effective compensatory measures appropriate to protect against exploitation of the vulnerability.

A.72. The operator should identify and implement computer security measures that provide robust security to allow for the assessment of updates and associated vulnerabilities without those vulnerabilities being exploited during the period of assessment and installation. For example, system hardening could reduce the number of security updates that need to be assessed and installed, as updates that affect only functionality that has been removed or disabled need not be installed.

System monitoring

A.73. All systems covered by the CSP should be assigned an owner (e.g. a system engineer) who is responsible for monitoring the system.

A.74. System monitoring should include monitoring the status and effectiveness of computer security measures.

A.75. The system owner should be responsible for ensuring that recovery media and configuration information are up to date and that system recovery plans are maintained and can be executed when necessary (e.g. through regular exercise of the recovery plan).

Configuration change control

A.76. Configuration changes to an SDA should be controlled with explicit consideration for security consequence analyses. The manager or asset owner should approve any configuration changes to an SDA prior to implementation of the changes. This approval should be formally documented.

A.77. Activities associated with change to the configuration of an SDA should be reviewed by the computer security specialist. Records of changes to the configuration of an SDA should be prepared, retained and reviewed.

A.78. The computer security specialist should have overall responsibility for oversight of configuration change control activities involving SDAs but may delegate this responsibility to asset owners. The computer security specialist should put in place requirements to ensure that effective oversight is performed and coordinated.

Computer security exercises (including drills)

A.79. The continual monitoring of the effectiveness of a CSP in practice should include the evaluation of CSP components through exercises.

A.80. Exercises for information and computer security can combine assessment with training. Exercises should also include scenarios involving blended attacks incorporating coordinated cyber-attack and physical attack.

A.81. The information and computer security management system may be exercised in a graded way for personnel with different roles and at different levels within the organization. Exercises test how effectively work processes and communications function in responding to a computer security incident; they also provide training for all levels of personnel involved in the management and response.

A.82. The operator should consider the benefit of the following:

(a) Exercises of security procedures to test the effectiveness of the procedures in meeting the objectives of the CSP;
(b) Drills to train personnel in carrying out the security procedures and thereby improve awareness of the procedures, the rationale for the tasks in the procedure and the response to computer security incidents.

Intrusive testing

A.83. The operator should consider whether to perform intrusive testing (simulating a real cyber-attack on real systems) as part of the evaluation of a system's or a digital asset's computer security, taking account of legal, safety and security considerations and of the operator's capability to avoid or remediate any adverse effects caused to the digital asset and system. Reference [8] identifies specific restrictions on intrusive testing of I&C systems.

A.84. Since the detailed method of a cyber-attack will be strongly dependent on the exact configuration of the systems attacked, a system being tested needs to be as similar to the real system as possible. Full backup and restore procedures should be in place to return the system to a known stable state if an assessment test creates abnormal conditions.

A.85. A test plan should specify the schedule and budget for testing and identify the goals of the testing, the expected deliverables, the hardware and software to be used, the resources needed, the rules of engagement and a recovery procedure.

A.86. Testing techniques may include the following:

(a) 'Fingerprinting', which involves identifying and quantifying all communications within and between components in a system and analysing the effects of these communications on the SDAs to which the tests relate. Fingerprinting a network provides the following:

(i) A network baseline;
(ii) An accurate network diagram;
(iii) Identification of any rogue devices or malicious data communications;
(iv) Verification that boundary protection devices are working as designed;
(v) Identification of opportunities to improve zoning and perimeter protection.

(b) 'Fuzzing', which aims to find bugs or vulnerabilities in a component or system by injecting a wide variety of data in an automated fashion to identify types of data and injection points that might be used for malicious purposes. This can identify weaknesses in software coding and provide an indication of system hardness.

A.87. Computer security indicators can provide a common basis for evaluating vulnerabilities. Well chosen and commonly agreed indicators (e.g. a common scoring system for vulnerabilities) provide a common basis for comparing vulnerabilities across different systems. The operator should assess possible ways in which identified vulnerabilities could be exploited and take measures to prevent such exploitation. The operator should consider reporting all vulnerabilities for inclusion in a national vulnerability database.

Computer security incident response

A.88. Computer security staff should be responsible for reporting any suspected computer security incidents according to the incident response plan. The operator should consider providing specialized awareness training for personnel in key roles not directly related to computer security but that could be affected by failures in computer security.

A.89. The operator should have a contingency plan to detect and respond to computer security incidents that might potentially affect SDAs (and for any other nuclear security events that involve computer security incidents). The plan should provide procedures to identify the location and nature of the threat, prevent or mitigate the consequences of any malicious act, notify relevant competent authorities, and recover from the event.

A.90. Incident response is a collection of activities (see Fig. 10), each of which should be considered.

A.91. Computer security incidents can involve compromise of the confidentiality, integrity and/or availability of the data processed, stored or transmitted by a computer based system. A computer security incident might

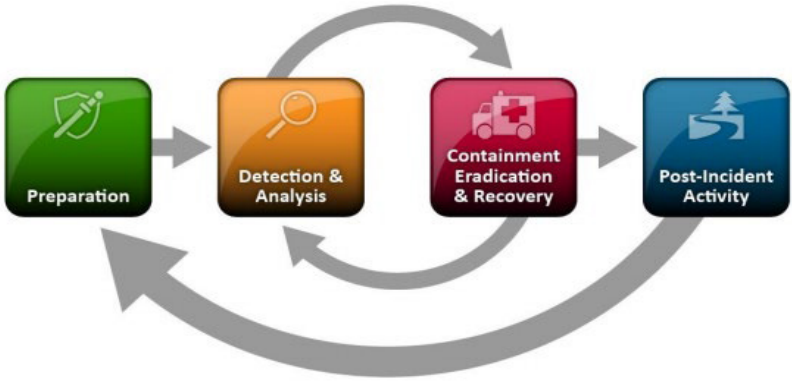


FIG. 10. Computer security incident response (reproduced from Ref. [24] courtesy of NIST).

also involve violation of an explicit or implied computer security policy, an acceptable use policy or a standard computer security practice. Some adverse events (e.g. floods, fires, electrical outages, excessive heat) can cause a system outage but are not the result of malicious acts and therefore are not considered to be computer security incidents.

A.92. A computer security incident might become an information security incident or breach if it involves the actual or suspected compromise of sensitive information. Reference [5] provides examples of potentially sensitive information associated with nuclear facilities.

A.93. The operator should create a local computer security incident response team, which is responsible for responding to computer security incidents within the organization. The size, composition and capabilities of a computer security incident response team will depend on the nature of the organization and its computing infrastructure, but it should include personnel with expertise in nuclear security, nuclear safety, and emergency preparedness and response as well as computer security. The computer security incident response team may have the same membership as, or some members in common with, the computer security team.

A.94. A computer emergency response team is a technical authority that provides assistance and response capabilities when a computer security incident occurs. The computer emergency response team may exist at different levels (e.g. national, local, industrial sector). The computer emergency response team may be available to supplement the internal computer security response

capabilities of an operating organization in responding to any computer security incident. The availability of this team to respond during times of crisis should be considered in planning the operating organization's response activities.

A.95. The operator should ensure the participation in exercises of any computer emergency response team members who would be involved in response as well as the computer security incident response team members. Interfaces between the computer emergency response team and the computer security incident response team, including preparatory activities (e.g. preclearance of computer emergency response team members for access to identified areas of the facility) should be considered. Exercises should be designed to test the key communication items between the competent authorities, the computer emergency response team, the computer security incident response team and site operations, as shown in Fig. 11.

Phases in computer security incident response

Preparation

A.96. Planning actions in the preparation phase include establishing a policy that will guide the operational processes for responding to computer security incidents, defining the roles and responsibilities of all parties involved in the incident response, drafting procedures consistent with the policy, and identifying assets available for response. Requirements and criteria for use in responding to computer security incidents need to be clearly defined. The plan of response actions should be approved by senior management.

FIG. 11. Computer security incident response interfaces.

Detection and analysis

A.97. During the detection and analysis phase, the computer security incident response team should be responsible for the technical characterization of the incident. Detection activities include ensuring that there is adequate data monitoring in place to support detection through the collection and preservation of information related to possible incidents. The computer security incident response team may use a dedicated testing and evaluation environment to analyse incidents without affecting operational systems or disturbing potential forensic evidence.

A.98. Analysis activities may extend beyond the computer security incident response team and the initial technical characterization of the incident, and some aspects of the analysis may require extensive resources. Typical priorities for analysis include the following:

(a) Determining the potential effects of the computer security incident on nuclear security, safety and emergency preparedness and response, and identifying actions to place the facility in a safe condition;
(b) Identifying the extent of the incident to determine an adequate response;
(c) Determining the potential damage from the computer security incident in terms of information loss, physical damage to the facility and public perception;
(d) Determining the nature of the computer security incident with regard to the adversary's immediate intent and possible future threats, including the possibility of a future attack exploiting effects from this incident;
(e) Identifying the root cause of the computer security incident and the measures needed to prevent or mitigate the effects of future incidents of a similar nature;
(f) Identifying the adversary and developing a profile of the adversary, including the techniques and tools used and the vulnerabilities exploited by the adversary.

Mitigation (containment, eradication and recovery)

A.99. Mitigation actions aim to contain a computer security incident; eradicate any malware or correct any mal-operation or altered configuration from the affected systems; and recover system function and data integrity, using compensatory measures where necessary. Even if the compromised components or systems do not perform a critical safety or security function, they need to be checked and cleared to prevent propagation of the attack to a component or

system that does perform such a function. Mitigation activities continue and are adapted as information is collected and analysed during the detection and analysis phase.

A.100. When planning how to contain computer security incidents, the operator should recognize that a number of components or systems may be identified during the incident investigation as having been compromised. If any of the compromised components or systems provide a critical safety or security function — such as contributing to the protection of SDAs, the safe operation of the facility or the protection of nuclear or other radioactive material — it will be necessary to implement compensatory measures to perform that function until the component or system can be brought back into operation.

A.101. Recovery measures may include like-for-like replacement (e.g. a backup firewall); isolation of safety structures, systems and components from the compromised component or system; or temporary measures, such as a guard to control access to the relevant part of the facility to replace a digital access control system. Recovery measures need to replace the function, not necessarily the compromised component or system.

Post-incident activities

A.102. The last phase of response is post-incident activities to implement measures that will prevent the recurrence of similar types of computer security incident in the future, enable their rapid detection and/or minimize their consequences. This phase may include learning lessons within the organization and sharing intelligence on threats and lessons learned, as appropriate, with the wider computer security incident response community to help prevent a similar attack from succeeding elsewhere. Post-incident findings may allow the development of new security measures to prevent re-infection and provide information to update threat and vulnerability profiles. Other post-incident activities may include evaluating the effectiveness of the CSP and identifying training to address any gaps in the response of personnel, as well as assessing the resources that were needed to address the computer security incident as a guide to planning for future incidents.

Reporting

A.103. During the response to a computer security incident there may be situations in which reporting to competent authorities (or other organizations) is required or desirable. Reporting allows everyone who needs to know about

a computer security incident to be informed in a timely manner. Since those responding to the incident are likely to be busy, the operator needs to consider carefully the frequency of reporting and the level of detail provided. The operator may consider assigning a specific individual as the point of contact for computer security incident reporting and for requests for information from outside organizations.

Activity planning

A.104. Activity planning should ensure that the computer security requirements for the performance and verification of the activities are identified and planned.

A.105. Required personnel and contractor qualifications related to computer security should be identified for the activities being performed, and this should be taken into account in the planning. Each responsible organization has the responsibility to report suspected computer security incidents according to the incident response plan.

A.106. When developing work instructions, computer security requirements need to be taken into account. These could include instructions for the following:

(a) Removal of computer security measures (to allow for maintenance);
(b) Provision of alternate or compensatory measures (while normal measures are unavailable);
(c) Reapplication of computer security measures (following maintenance);
(d) Confirming that computer security measures have been correctly re-established.

A.107. Maintenance instructions should include instructions for configuring the security settings on devices.

A.108. If maintenance requires the disposition of equipment that is no longer required, this equipment should be sanitized or securely destroyed.

A.109. Procurement requirements related to computer security should be identified and implemented in the work plan.

AWARENESS AND TRAINING

A.110. Although computers are used in many aspects of work and personal life, there is a general lack of awareness and knowledge regarding the technology, cyber threats, computer security measures and the possible effects of compromise. Awareness raising and training in computer security are needed for all personnel and contractors in organizations that have nuclear security responsibilities.

A.111. Human error causes or adversely contributes to computer security incidents. Staff at all levels need awareness and constant reaffirmation of computer security.

A.112. Awareness of its importance can support computer security as follows:

(a) By promoting understanding that computer security supports not only the nuclear security of the facility but also the safety of the facility;
(b) By ensuring a common understanding of the key aspects of computer security within the organization;
(c) By encouraging observation and coaching of colleagues, reporting of potential computer and information security incidents, and situational awareness;
(d) By promoting understanding that cyber-attacks can affect multiple security and/or safety measures simultaneously, reducing defence in depth;
(e) By providing a means by which conflicts between safety and security objectives can be resolved;
(f) By recognizing and promoting good practices in computer security;
(g) By raising awareness of how humans can inadvertently contribute to computer security incidents.

A.113. The following indicators may be used to evaluate awareness of computer security in an organization:

(a) Computer security requirements are clearly documented and well understood by staff.
(b) Clear and effective protocols and procedures exist for operating computer systems both inside and outside the organization.
(c) Staff members understand and are aware of the importance of the computer security measures set out in the CSP.
(d) Computer systems are kept secure and operated in accordance with the computer security baseline and approved procedures.

(e) Breaches of computer security procedures are regarded by all as serious and undesirable.
(f) Results of observations, evaluations, tests and exercises are positive (e.g. testing indicates that staff do not respond to phishing emails).
(g) Managers are fully committed to and supportive of security initiatives, whether related to cyber or to physical systems.

A.114. The aim of a computer security training programme is to ensure that personnel and contractors have the knowledge and capability to perform their work in accordance with the facility computer security requirements and procedures. Computer security training should be incorporated into an existing training management system.

A.115. The operator should have a training programme with the following elements:

(a) A computer security training programme, successful completion of which is a precondition for access to computer systems. Individuals' training should be commensurate with the computer security levels of systems to which they will have access.
(b) Specialized training and qualification for individuals with key security responsibilities (e.g. computer security specialist, computer security team, other security officers, project managers, IT administrators, system engineers, designers, technicians, document management personnel, project personnel, procurement personnel, contractors, senior management).
(c) Training materials that are updated on a regular basis to include new procedures and measures to address emerging threats.
(d) Training that is repeated on a regular basis to ensure that staff are familiar with the latest procedures and threats.
(e) A requirement for staff to acknowledge that they understand their computer security responsibilities.
(f) Practical evaluations of staff's understanding of their computer security responsibilities.

A.116. A variety of training approaches should be used, such as e-learning, classroom training, practical exercises and discussion forums[47]. External

[47] Discussion forums might result in information leaks that could assist the adversary; therefore, posting of information on publicly available and open discussion forums is discouraged.

organizations, including the IAEA, can provide materials to support such activities.

A.117. The training programme should include (a) indicators for evaluating computer security awareness and the effectiveness of training and (b) processes for continual improvement and periodic refresher and update training for staff, as needed.

EXAMPLE PROCESS FOR PLANNING RESPONSE TO COMPUTER SECURITY INCIDENTS

A.118. An example process for planning response to computer security incidents can be found in Ref. [25].

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Security during the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2018, ISO, Geneva (2018).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2018, ISO, Geneva (2018).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2013).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).
[18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2009, ISO, Geneva (2009).
[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Requirements, ISO/IEC 27001:2013, ISO, Geneva (2013).
[20] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva (2014).
[21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Code of Practice for Information Security Controls, ISO/IEC 27002:2013, ISO, Geneva (2013).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Conducting Computer Security Assessments at Nuclear Facilities, IAEA, Vienna (2016).
[24] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computer Security Incident Handling Guide, NIST SP 800-61, Rev. 2, NIST, Gaithersburg (2012).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, IAEA, Vienna (2016).

Annex I

POTENTIAL ATTACK SCENARIOS AGAINST SYSTEMS IN NUCLEAR FACILITIES

I–1. This annex provides some examples of ways in which adversaries could exploit vulnerabilities in systems performing critical facility functions. However, these are only examples, and operators need to think creatively about computer security to imagine how adversaries might act and how computer security measures might counter their actions.

I–2. The examples are derived from discussions with experts from Member States. They are not intended to provide an exhaustive list of possibilities or a recipe for attacking nuclear facilities, but rather a starting point for facility operators and Member States to develop plans to address the dynamic, rapidly changing cyber threat environment.

I–3. A coordinated cyber-attack might consist of several phases:

(a) Identifying a target or targets;
(b) Performing reconnaissance;
(c) Obtaining access to or otherwise compromising relevant systems;
(d) Carrying out the attack;
(e) Concealing evidence about the attack and the adversary.

I–4. Adversaries will use some or all of these tactics, and they need to be considered when developing cyber threat profiles specific to nuclear facility instrumentation and control (I&C) systems and other sensitive digital assets (SDAs). The example scenarios presented in this annex include the use of these tactics and illustrate common types of attack suggested by computer security experts with experience of the nuclear industry.

I–5. Types of threat are described in Ref. [I–1].

SCENARIO I: COMPROMISE OF A SUPPORT LEADING TO ACCESS TO CRITICAL OPERATIONAL SYSTEMS

I–6. Goal of the attack: To gain access to nuclear information and digital assets by exploiting a trusted path used by vendors to provide support.

I–7. Description: The attack is initially directed at the Internet based remote access portal through which vendors have access to sensitive information and facility SDAs to provide support. The adversary compromises the portal and, via privilege escalation, gains administrative control over the database and changes the email address associated with a specific vendor. This vendor has remote access to critical operational information about the facility and some of the SDAs. The adversary uses the 'forgotten password' function on the portal, which sends a password refresh link to the email address introduced by the adversary. The adversary uses this link to change the vendor's password and logs in to the portal with the identity of the authorized vendor. Once logged in, the adversary has access to all the information on the portal and all the SDAs to which the vendor has access. The adversary then begins to modify the settings and operational parameters of SDAs, leading to operational instability and ultimately to the shutdown of the facility.

SCENARIO II: EXPLOITATION OF THE TRANSITIVE TRUST BETWEEN REPORTING SERVERS ON THE PERIMETER NETWORK AND INTERNAL SDAs

I–8. Goal of the attack: To gain access to internal SDAs and systems.

I–9. Description:

(1) Using open source tools and search engines, the adversary locates the perimeter network[1] server used to report production information related to nuclear isotopes from trusted internal systems to the Internet. This server resides on the perimeter network but is populated by a master database server on the same network as the control system for a facility that produces nuclear isotopes. The master database server collects information from the internal manufacturing production environment and sends this information to the database located on the perimeter network. The perimeter network is separated from the production network by a firewall, which is configured with an access control list to ensure that only the database on the perimeter network server can communicate to the master database.

(2) The adversary exploits a vulnerability to obtain administrative access to the server on the perimeter network and takes control of the communication

[1] Such networks are used as 'buffers' between trusted internal systems and publicly accessible systems that are not trusted, such as the Internet. They are sometimes referred to as 'demilitarized zones'.

channel between that server and the master database server on the control system network. The firewall is configured to allow communications between the perimeter network and the master database (i.e. it establishes 'transitive trust' between the networks), so the adversary, who has control of the server on the perimeter network, can connect directly to the master database on the control system network.

(3) The adversary uses the connection to the master database to perform reconnaissance and enumeration of the control system assets that are on the same network. Since there are no security measures on the control system network, the adversary is able to take control of SDAs and compromise the technology controlling isotope development, management, transport, storage and inventory.

SCENARIO III: MALWARE INFECTION OF NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL SYSTEMS

I–10. Goal of the attack: To force the shutdown of a nuclear power plant.

I–11. Description:

(1) An engineer at a nuclear power plant works at home on a laptop computer that is used to support plant engineering and optimization, update performance programmes and 'tune' software for safety monitoring.

(2) While at home, the engineer uses the computer to access a vendor's web site and obtain a software update for the plant I&C systems that are instrumental in supporting plant operations. While the update is downloading, the engineer uses an on-line bank, visits the corporate web site and uses social media, during which malicious software is downloaded to the computer. This malware is new and is not detected by the antivirus software on the computer.

(3) Since corporate policy prohibits taking the computer into the plant, the engineer copies the downloaded control system update to a USB storage device, intending to use this to apply the software updates to the I&C assets. However, the malware has also copied itself to the USB device, and when the engineer uses it to install the update through an engineering workstation in the plant, the malware copies itself onto the plant system. The plant operator has assumed that the physical protection measures in place will prevent an unauthorized computer from connecting to the plant control system network, and the possibility of infection via removable media has not been considered.

(4) After the malware infects the engineering workstation, it replicates and moves to other networked components within the plant. Since the operator has not deployed computer security measures at the plant level and there is no antivirus software on critical plant systems, the malware infects critical digital assets on the network, causing failures and forcing the plant to shut down.

SCENARIO IV: OBTAINING OF SENSITIVE INFORMATION ABOUT NUCLEAR PLANT OPERATIONS DIRECTLY FROM INAPPROPRIATELY DECOMMISSIONED EQUIPMENT

I–12. Goal of the attack: To obtain enough information to plan an accurate attack on plant operations.

I–13. Description:

(1) An adversary collects information from social media and observation indicating that a nuclear facility will be procuring a control system in the form of a system upgrade. In addition, the facility operator intends to sell old operational equipment to help pay for the new control system.
(2) Since the facility has no formal decommissioning procedure related to information security, a system that was used to run critical I&C operations is sold without reviewing or removing information stored in it. The adversary buys the system and discovers up to date project files, network diagrams, username and password information, and other data that provide a comprehensive understanding of the nuclear facility operations.
(3) The adversary uses this information to develop a plan to attack specific SDAs used at the facility and to create convincing emails for use in a phishing campaign. Ultimately, the adversary uses both the information obtained from the purchased system and that unwittingly provided by victims of the phishing campaign to launch a blended attack on the facility.

SCENARIO V: STRATEGIC SOCIAL ENGINEERING ON THE FACILITY SECURITY OFFICER

I–14. Goal of the attack: To obtain, through social engineering, information from a facility security officer that can be used to further an attack.

I–15. Description:

(1) An adversary conducts a focused social engineering campaign against a facility security officer using phishing, physical reconnaissance and publicly available information, including that from the officer's social media presence.
(2) The adversary, with a false identity, uses this information to begin communicating directly with the security officer, who gradually comes to trust the adversary, believing that it is someone else. As the correspondence continues, the adversary starts to add credible email attachments that are actually malicious software that, when activated, covertly opens a communication path back to the adversary's computer and sends specific files from the security officer's computer to the adversary. With this information, the adversary is able to create accurate and detailed plans to attack the plant's physical protection systems and intercept nuclear material in transit.

REFERENCE TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

Annex II

EXAMPLE OF COMPUTER SECURITY LEVEL ASSIGNMENT FOR A NUCLEAR POWER PLANT

II–1. The assignment of computer security levels to systems (or zones containing systems) is based on the potential consequences of an attack on each system for the safety, security and operation of the facility: the less tolerable the consequences, the more stringent the computer security level.

II–2. To avoid case by case analyses of every system and potential consequence, criteria can be established to facilitate the assignment of the computer security levels.

II–3. One fundamental consideration is the safety classification of the system. However, there is not an automatic connection between computer security levels and safety classes. A stringent computer security level is needed for a system important to safety, but a stringent level may also be needed for systems with no safety classification if they have a critical role in preventing severe potential consequences for security.

II–4. An example graded approach to computer security levels uses the following high level criteria:

(1) Computer security level 1 is assigned to plant digital systems for which compromise of their integrity or availability could lead to radiological consequences to the population off the site. This corresponds to the criterion for 1E/F1A safety classified systems (corresponding to systems supporting category A functions in the International Electrotechnical Commission safety scheme [II–1]).
(2) Computer security level 2 is assigned to plant digital systems for which compromise of their integrity or availability could degrade one or more of the following:
    (i) The management of an emergency;
    (ii) Plant safety in normal operation;
    (iii) The main nuclear process operation;
    (iv) The physical protection of the plant.
(3) Computer security level 3 is assigned to plant digital systems for which compromise of their integrity or availability has no radiological consequences, nor an adverse effect on safety or physical protection, but

could have other major effects. Such systems might include, in particular, digital assets assisting plant operation or maintenance, or systems that could have an effect on power generation.

(4) Computer security level 4 is assigned to plant digital systems for which compromise of their integrity or availability has no short term effect on plant performance but can have such an effect in the longer term.

(5) Computer security level 5 is assigned to plant digital systems for which compromise of their integrity or availability has no effect on safety, on plant availability or on the performance of the facility.

II–5. In addition to these high level criteria, the definition of the computer security levels can include a list of typical facility functions or types of system that are specific to each level. This list could simplify the assignment of computer security levels to systems.

II–6. The computer security level classification focuses on potential consequences related to compromise of computer based systems (see Ref. [II–2]). In many cases, information acquired or calculated by a digital system can also be obtained with analogue tools or by a person, in which case the computer security level can be less stringent (and therefore less restrictive for normal operations).

II–7. When several diverse digital assets are used for the same function, a primary system supporting the function needs to be chosen and assigned to a computer security level according to the consequences of its compromise.

REFERENCES TO ANNEX II

[II–1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems, IEC 61513:2011, IEC, Geneva (2011).

[II–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems — Requirements for Security Programmes for Computer-Based Systems, IEC 62645:2014, IEC, Geneva (2014).

Annex III

EXAMPLE OF APPLICATION OF COMPUTER SECURITY LEVELS AND ZONES

BACKGROUND

III–1. This annex provides an example of the application of computer security levels and zones. Table III–1 provides a list of systems used in this example and shows the mapping of computer security levels to the physical and logical zones used in this example.

III–2. For simple systems, consisting of a small number of assets in well defined physical locations, application of the computer security levels and physical and logical zones is straightforward. It is more complicated for complex systems that extend throughout the facility or for physical areas that contain systems that need to be assigned to multiple security levels, such as the main control room.

MAIN CONTROL ROOM

III–3. Typically, the main control room contains controls for many different categories of systems that have differing security requirements (e.g. safety systems, steam supply (boiler), electrical systems, auxiliary systems, IT systems). The human–machine interfaces for all facility systems are entirely or partly in the main control room. These systems and human–machine interfaces typically use digital assets to perform their functions.

III–4. In old facilities, this creates difficulties in the application of computer security for several reasons:

(a) Older human–machine interface consoles typically include controls for multiple systems, especially for balance of plant and auxiliary systems. This aggregation can increase the difficulty in providing for isolation and separation of these systems. In some cases, facility functions performed by systems assigned to different computer security levels may be combined into one human–machine interface console, to which the most stringent security level needs to be applied.
(b) The digital assets located within the physical area of the main control room and its equipment rooms would, using the approach of computer security

levels and zones, be assigned different computer security levels. For example, a reactor protection system may be assigned the most stringent level (e.g. security level 1), while a personal computer providing the operator with access to email may be assigned the least stringent level (e.g. security level 5).

(c) Personnel performing authorized activities on a system within the main control room may have access to other equipment within the main control room.

III–5. The following illustrative example is provided to explain potential computer security solutions for the issues described above, in terms of the concepts detailed in Fig. 1 of the main text.

III–6. Application of computer security zones to the main control room (along with the physical protection and fire protection systems) is difficult because of the need for centralized monitoring and management of facility functions. The computer security zone concept allows for physical and/or logical boundaries, which can help to address these limitations. The relationship is illustrated in Fig. III–1.

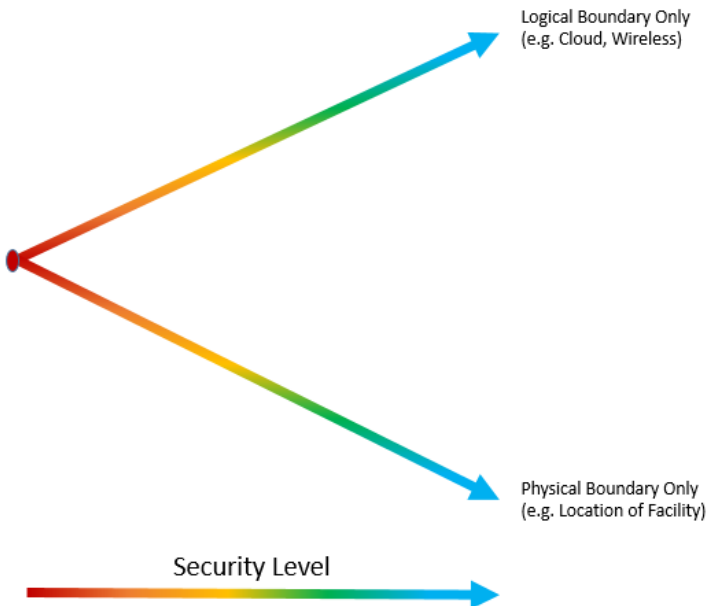


FIG. III–1. Physical and logical boundary zone requirements based on computer security level.

III–7. The main control room (and the rooms within the protected area containing electronic equipment) is assumed to be classified and protected as a vital area. This implies that sabotage of equipment within the main control room could ultimately result in unacceptable radiological consequences.

III–8. Table III–1 provides an example of a subset of systems that need monitoring, communications or operation from within the main control room.

TABLE III–1. LIST OF SYSTEMS: EXAMPLE OF APPLICATION OF COMPUTER SECURITY LEVELS AND ZONES

System	Most significant function	CSL	Logical boundary	Physical boundary
I&C reactor protection system	Prevent accident conditions	1	Dedicated internal network decoupled using data diode No external network connectivity	Equipment located in a single VA only Computer security measure (data diode) located in VA
I&C reactor limitation system	Control reactivity	2	Dedicated networks, decoupled using data diode, firewall or other security devices	Equipment located in one or more VAs Network cables, equipment, or routing outside of VAs are physically hardened (e.g. secured conduit, panels)
I&C process information system	Provide alarms and notifications to operator on facility environment and status	3	Interconnected networks with HMI Note: This may be a separate or additional MCR HMI console	Equipment and networks located in PA and/or VAs

TABLE III–1. LIST OF SYSTEMS: EXAMPLE OF APPLICATION OF COMPUTER SECURITY LEVELS AND ZONES (cont.)

System	Most significant function	CSL	Logical boundary	Physical boundary
I&C operational automation systems	Control BOP systems	3	Interconnected networks with HMI Note: This may be a separate or additional MCR HMI console or combined with an I&C process information system	Equipment and networks located in PA and/or VAs
Office IT	Perform personnel functions	4	No logical connection (wired, wireless or portable interface) allowed with any level 1, 2 or 3 zone (system)	Allowed in LAA, PA and VAs
Telecommunication systems	Call to response forces or other external agencies as required	4	No logical connection (wired, wireless or portable interface) allowed with any zone assigned to level 1, 2 or 3	Allowed in all locations necessary for operator objectives
Personal mobile IT devices	None required — exemption only	5	Only allowed on level 5 networks No proximity with any zone assigned to level 1, 2 or 3	Not allowed in VAs

Note: BOP — balance of plant; CSL — computer security level; HMI — human–machine interface; I&C — instrumentation and control; IT — information technology; LAA — limited access area; MCR — main control room; PA — protected area; VA — vital area.

ZONES OUTSIDE THE MAIN CONTROL ROOM MONITORED FROM INSIDE THE MAIN CONTROL ROOM

Reactor protection system (computer security level 1)

III–9. In Table III–1, the most stringent computer security level (level 1) has a requirement that both the logical and physical computer security zone boundaries be specified strictly and that these boundaries do not extend past each other. For example, the dedicated network can be constrained to locations within the vital area (or equivalent).

III–10. Physical and logical access to zones assigned computer security level 1 needs to be strictly controlled. Physical access can be controlled using a robust barrier with access control and intrusion detection to meet the requirements recommended in Ref. [III–1], and logical access can be controlled through a fail-secure, unidirectional data communication pathway (e.g. a data diode) in accordance with the guidance in this publication and Ref. [III–2].

III–11. Typically, systems that perform the facility function of preventing accident conditions (e.g. those on a reactor protection system) will be assigned to the most stringent computer security level. The equipment providing the function will be located in a vital area close to the reactor, but the equipment will be monitored through a human–machine interface in the main control room. This creates a potential problem with applying computer security zones, since the interconnection between the reactor protection system and the human–machine interface might be routed outside the vital areas (e.g. in the protected area), which would violate the physical security requirement.

III–12. One solution would be to separate the monitoring function from the function of preventing accident conditions. This would allow for logical separation by means of a data diode between the digital assets in the vital area preventing accident conditions and those outside the vital area used for monitoring in the main control room. This solution would only be effective if the function of preventing accident conditions was independent and did not need any action or information from outside the systems assigned to perform the function.

III–13. The digital assets credited with preventing accident conditions will be assigned to the most stringent computer security level (level 1) on the basis of facility function. These digital assets will be located in a vital area outside the main control room. The digital assets credited with monitoring the reactor

protection system (e.g. the reactor protection system human–machine interface console in the main control room) will be assigned security level 2 (or higher).

ZONES OUTSIDE THE MAIN CONTROL ROOM OPERATED FROM INSIDE THE MAIN CONTROL ROOM

Instrumentation and control reactor limitation system (computer security level 2)

III–14. According to Table III–1, digital assets performing functions assigned to security level 2 are required to be in a vital area and to have strictly controlled physical and logical access. However, for operational reasons, the control of reactivity function needs command input from the main control room (e.g. instructions to increase or decrease power).

III–15. The equipment is located within vital areas, and the network infrastructure (cabling, switches and panels) is hardened when it is in less secure areas (e.g. if network cables are routed through the protected area). Since command input is needed (i.e. communications initiated from the main control room to the equipment), installation of a data diode to control logical access is not possible.

III–16. A solution would be to physically and logically isolate the zone containing network and digital assets supporting these command communications from other zones assigned to lower security levels (levels 3 to 5). This would allow for logical separation between other systems at lower levels. This solution will only be effective if the function of preventing accident conditions is independent and does not need any action or information from outside the systems assigned to perform the function.

III–17. The same rationale and solution can also be applied for the instrumentation and control (I&C) process information system and I&C operational automation systems assigned to computer security level 3.

ZONES OR DEVICES WITH EXTERNAL CONNECTIVITY

Office information technology and telecommunications systems (computer security level 4 or 5)

III–18. According to Table III–1, office information technology (IT) and telecommunications systems provide necessary functions that need external connectivity. This allows the operator to access information and resources that might be needed during certain events and conditions.

III–19. These external connections, to the Internet and other services, networks and devices, can increase risk unless measures are put in place to ensure that information cannot be exchanged between these external sources and systems performing facility functions assigned to higher security levels. Robust measures are needed to remove or restrict access to portable interfaces, wired and wireless connections, and other means by which information can be exchanged with digital assets that have external connectivity, as well as to enforce tightly bounded computer security zones for such digital assets with strong decoupling mechanisms. Separation of security zones within the main control room is discussed further in paras III–21 to III–27.

Personal mobile information technology devices (unassigned)

III–20. Personal mobile IT devices and software are assumed not to have been hardened to remove capabilities for exchanging information through proximity to assigned digital assets. Personal mobile IT devices are therefore not allowed in the main control room (or its associated equipment rooms).

SEPARATION OF SECURITY ZONES WITHIN THE MAIN CONTROL ROOM

III–21. As noted in para. III–13, digital assets often perform multiple facility functions that would call for different computer security levels, and such digital assets are likely to be located within the main control room. This proximity increases the risk of compromise of these assets from cyber-attacks.

III–22. This is especially true if there are no physical controls in place to protect the access to and interfaces between the digital assets. In such a case, an insider who has logical or physical access to the main control room zone would have unrestricted opportunity to compromise digital assets in that zone.

III–23. Digital assets (and systems) located in the main control room perform functions that often need information from other digital assets or need actions to be undertaken by operating personnel. If the reactor protection system has been logically and physically separated from the main control room as in the example above (e.g. through a data diode for monitoring), the other fundamental safety functions to consider are control of reactivity and removal of heat from the core.

III–24. Systems performing these safety functions are usually assigned to computer security level 2. According to Table III–1, computer security level 2 requires strict zone boundaries, but these can be a combination of physical and logical boundaries.

III–25. The assignment of digital assets in the main control room to zones is further complicated by the need for corporate IT functions (e.g. email, Internet, operations management) to assist operators in the main control room. The installation of digital assets to support these functions can create a situation in which systems assigned to security levels 2 and 5 are provided to the same personnel in the main control room, yet the requirement to separate digital assets performing facility functions that are assigned to different security levels needs to be enforced.

III–26. In this example, the following solutions may be adopted:

(a) Logical networks are never connected directly and always employ strong decoupling mechanisms. Networks at security level 2 do not extend outside the main control room (and the associated equipment rooms within the protected area) without such decoupling mechanisms in place.
(b) Logical networks are clearly separated and identified, and responsibility for them can be assigned to different organizational units (e.g. IT, engineering).
(c) Physical control measures can be put in place to create subzones within the main control room. These might be locked panels, portable interface locks (e.g. port blockers), secure network conduits and/or limited access areas within the main control room.

III–27. Given the suggested solutions above, the use of logical and physical controls would allow multiple computer security levels to exist within a single physical zone (e.g. the main control room). However, with the installation of additional computer security measures, the main control room can be divided into several subzones that have each been assigned their own security level.

REFERENCES TO ANNEX III

[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

GLOSSARY

administrative control measures. Policies, procedures and practices specifying permitted, necessary and forbidden actions to protect computer based systems by providing instructions for the actions of employees and of vendors, contractors and suppliers.

blended attack. A malicious act involving the coordinated use of both cyber-attack and physical attack.

computer based systems. Technologies that create, provide access to, process, compute, communicate or store digital information or that perform, provide or control services involving such information. These technologies may be physical or virtual. They may include desktop, laptop, tablet and other personal computers; smartphones; mainframe computers; servers; virtual computers; software applications; databases; removable media; digital instrumentation and control devices; programmable logic controllers; printers; network devices; and embedded components and devices.

computer security. A particular aspect of information security that is concerned with the protection of computer based systems.

computer security incident. An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of a computer based system (including information) or that constitutes a violation or imminent risk of violation of security policies.

computer security level. The strength of protection required to meet computer security requirements for a function related to nuclear security, safety, nuclear material accounting and control, and/or sensitive information management.

computer security measures. Measures intended to prevent, detect or delay, respond to, and mitigate the consequences of malicious acts or other acts that could compromise computer security.

computer security programme. A plan for the implementation of the computer security strategy specifying organizational roles, responsibilities and procedures. The programme specifies and details the means for achieving

the computer security goals and is a part of (or linked to) the overall security plan.

computer security risk management. Assessment and management of the risks associated with possible cyber-attacks that have the potential to degrade nuclear safety or nuclear security. Computer security risk management is conducted at a facility level and at a system level.

computer security zone. A group of systems having common physical and/or logical boundaries — and, if necessary, arranged using additional criteria — that is assigned a common computer security level to simplify the administration, communication and application of computer security measures.

cyber-attack. A malicious act with the intent of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible computer based system.

defensive computer security architecture. Arrangement of computer based systems according to the design requirements, constraints and measures that are to be imposed during the life cycle of a system, such that systems that perform identified facility functions of significance to the safety and security of the facility and that are assigned to computer security levels at the facility level have the required level of protection.

design basis threat. The attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated.

detection. A process in a physical protection system that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with an assessment of the cause of the alarm.

facility function. A coordinated set of actions, processes and operations associated with a nuclear facility. Their purpose might include performing functions important or related to nuclear safety, nuclear security, nuclear material accounting and control, or sensitive information management. Facility functions also include operational and administrative (or organizational) functions.

information security. The preservation of the confidentiality, integrity and availability of information.

insider. An individual with authorized access to associated facilities or associated activities or to sensitive information or sensitive information assets who could commit, or facilitate the commission of, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities, or other acts determined by the State to have an adverse impact on nuclear security.

nuclear security event. An event that has potential or actual implications for nuclear security that must be addressed.

nuclear security measures. Measures intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities or to detect or respond to nuclear security events.

nuclear security regime. A regime comprising:

— The legislative and regulatory framework and administrative systems and measures governing the nuclear security of nuclear material, other radioactive material, associated facilities and associated activities;
— The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security;
— Nuclear security systems and nuclear security measures for the prevention of, detection of and response to nuclear security events.

nuclear security system. An integrated set of nuclear security measures.

physical control measures. Physical barriers that protect instruments, computer based systems and supporting assets from physical damage and prevent unauthorized physical access.

sensitive digital assets. Sensitive information assets that are (or are parts of) computer based systems.

sensitive information. Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.

sensitive information assets. Any equipment or components that are used to store, process, control or transmit sensitive information. For example, sensitive information assets include control systems, networks, information systems, and any other electronic or physical media.

technical control measures. Hardware or software used to prevent, detect, mitigate the consequences of and recover from an intrusion or other malicious act.

threat assessment. An evaluation of the threats — based on available intelligence, law enforcement and open source information — that describes the motivation, intentions and capabilities of these threats.

threat statement. A description of credible adversaries (including attributes and characteristics) in the form of design basis threat or representative threat statement, developed on the basis of the national nuclear security threat assessment.

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (57 pp.; 2011)
ISBN 978–92–0–111110–4 Price: €28.00

PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (IMPLEMENTATION OF INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 27-G
STI/PUB/1760 (120 pp.; 2018)
ISBN 978–92–0–111516–4 Price: €46.00

COMPUTER SECURITY FOR NUCLEAR SECURITY
IAEA Nuclear Security Series No. 42-G
STI/PUB/1918 (86 pp.; 2021)
ISBN 978–92–0–121120–0 Price: €40.00

COMPUTER SECURITY OF INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 33-T
STI/PUB/1787 (58 pp.; 2018)
ISBN 978–92–0–103117–4 Price: €42.00

NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS
IAEA Nuclear Security Series No. 10-G (Rev. 1)
STI/PUB/1926 (39 pp.; 2021)
ISBN 978–92–0–131020–0 Price: €31.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8-G (Rev. 1)
STI/PUB/1858 (37 pp.; 2020)
ISBN 978–92–0–103419–9 Price: €24.00

This publication provides guidance on establishing, improving, developing, implementing, maintaining and sustaining computer security within nuclear facilities. It addresses the use of risk informed approaches to establishing and enhancing computer security policies and programmes; describes the integration of computer security into the management system of a facility; and establishes a systematic approach to identifying facility functions and appropriate computer security measures that protect the facility from cyber-attacks consistent with the threat assessment or design basis threat. This publication addresses all digital assets associated with a nuclear facility and is applicable to all stages in the lifetime of a nuclear facility.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA