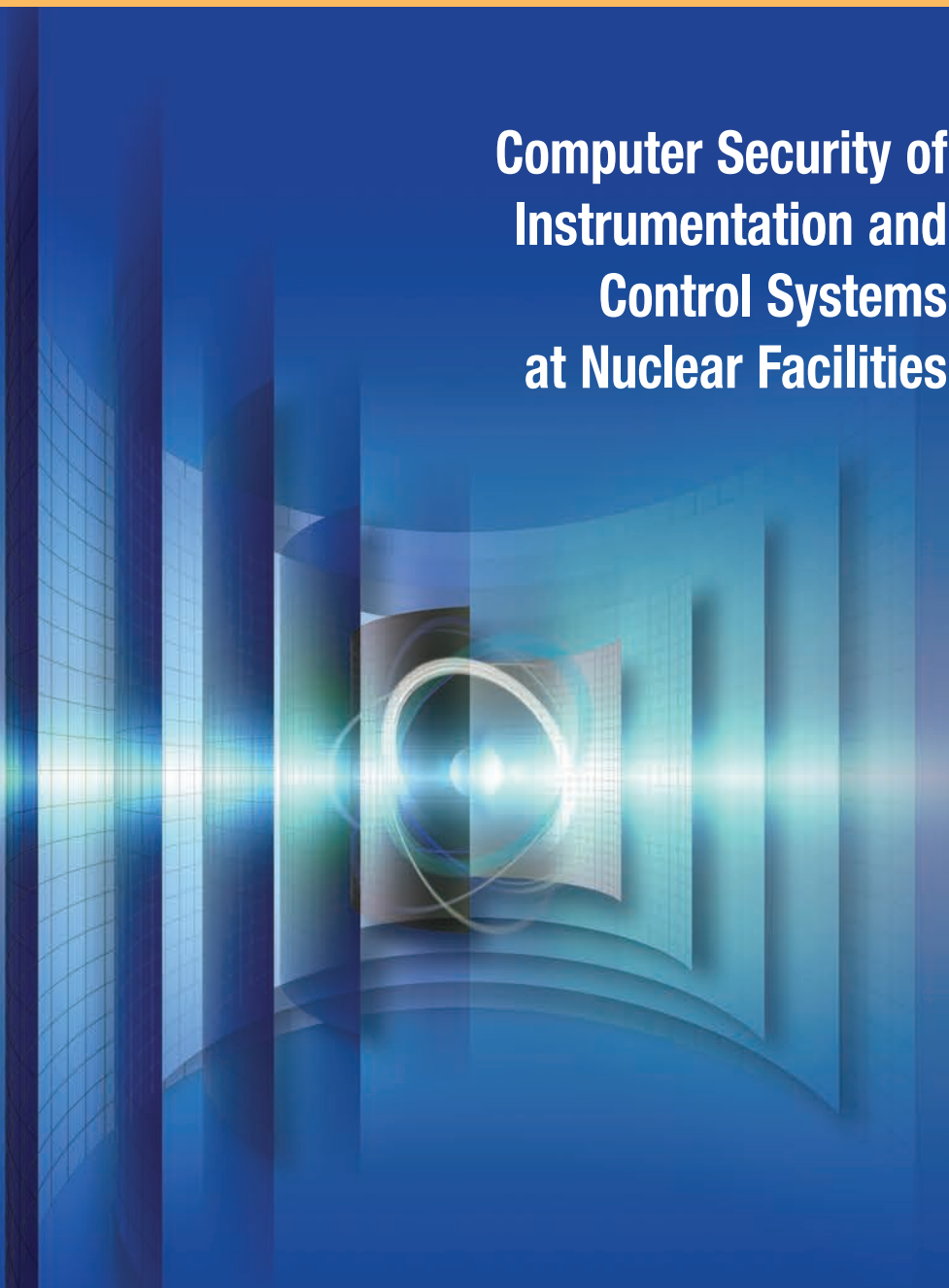
IAEA Nuclear Security Series No. 33-T

Technical Guidance

Computer Security of Instrumentation and Control Systems at 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 OF INSTRUMENTATION AND CONTROL SYSTEMS AT 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
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
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
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
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
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''.

IAEA NUCLEAR SECURITY SERIES No. 33-T

COMPUTER SECURITY OF INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2018

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
May 2018
STI/PUB/1787

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Computer security of instrumentation and control systems at nuclear facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2018. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 33-T | Includes bibliographical references.
Identifiers: IAEAL 18-01151 | ISBN 978–92–0–103117–4 (paperback : alk. paper)
Subjects: LCSH: Nuclear facilities. | Nuclear reactors — Control. | Computer security.
Classification: UDC 621.039.56 | STI/PUB/1787

FOREWORD

by Yukiya Amano
Director General

The IAEA's principal objective under its Statute is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." Our work involves both preventing the spread of nuclear weapons and ensuring that nuclear technology is made available for peaceful purposes in areas such as health and agriculture. It is essential that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. The central role of the IAEA in facilitating such cooperation and providing assistance to States is well recognized. The IAEA's role reflects its broad membership, its mandate, its unique expertise and its long experience of providing technical assistance and specialist, practical guidance to States.

Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, 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.

Guidance is developed with the active involvement of experts from IAEA Member States, which ensures that it reflects a consensus on good practices in nuclear security. The IAEA Nuclear Security Guidance Committee, established in March 2012 and made up of Member States' representatives, reviews and approves draft publications in the Nuclear Security Series as they are developed.

The IAEA will continue to work with its Member States to ensure that the benefits of peaceful nuclear technology are made available to improve the health, well-being and prosperity of people worldwide.

EDITORIAL NOTE

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. Instrumentation and control (I&C) systems play a critical role in ensuring the safe operation of nuclear facilities. As digital technologies continue to evolve and become more capable, they are increasingly being incorporated into and integrated with I&C systems[1]. New nuclear facilities and modern nuclear facility designs use highly integrated digital I&C systems to efficiently and simultaneously handle vast quantities of process data while requiring less human interaction and intervention than previous I&C systems. Digital technologies are also often introduced into I&C systems during the modernization of existing facilities. However, the application of digital technologies within I&C systems has made these systems vulnerable to cyber attacks.

1.2. A cyber attack is a malicious act carried out by individuals or organizations that targets sensitive information or sensitive information assets with the intent of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible system. Sensitive information assets include control systems, networks, information systems and any other electronic or physical media. Adversaries have launched successful cyber attacks directed at I&C systems, such as the Stuxnet cyber attack, which led to the destruction of equipment at a nuclear facility [1].

1.3. Cyber attacks on I&C systems may jeopardize the safety and security of nuclear facilities. They may contribute to sabotage or aid in the unauthorized removal of nuclear material. The effects of cyber attacks on I&C systems related to safety may result in a wide range of consequences, such as a temporary loss of process control or unacceptable radiological consequences. Public awareness of cyber attacks that affect I&C systems may also undermine confidence in the safety and security of nuclear facilities.

1.4. The need for the protection of computer based systems (including I&C systems) is established in the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2], para. 4.10, which states that:

---

[1] The term I&C system is used throughout the remainder of this publication to refer to those instrumentation and control systems that make use of, depend upon or are supported by digital technologies.

> "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.*"

1.5. IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [3], provides guidance specific to nuclear facilities on implementing a computer security programme to support the guidance stated in Ref. [2]. Reference [3] also provides details of key terminology such as 'computer security', 'IT security' and 'cyber security'. The terms 'IT security' and 'cyber security' are, for the purpose of this publication, considered synonyms of computer security and will not be used.

1.6. Computer security needs to be explicitly considered in every phase of the I&C system life cycle. The term 'life cycle' (as opposed to lifetime) implies that the system's life is genuinely cyclical (as in the case of recycling or reprocessing), and notably that elements of the old system are used in the new system. Reference [4] contains a list of typical I&C life cycle activities.

1.7. Historically, computer security was not given significant consideration in the design of I&C systems at nuclear facilities because hardwired or analogue systems were assumed to be invulnerable to cyber attack owing to their rigid implementation, isolation and system segregation and to a near absence of interactive communications, particularly with external networks or systems. The transition to digital technology has changed the nature of I&C systems at nuclear facilities by enabling the interconnection of reprogrammable (remotely or locally) and functionally distinct I&C systems.

1.8. The greater use of versatile programmable digital components and devices has resulted in a reduction in the diversity of I&C systems. This includes the use of common elements and approaches across a variety of industrial applications (e.g. communication protocols). Malicious acts[2] directed at these common technologies in other industries could also affect a nuclear facility.

1.9. Authorized individuals, whether on-site or at a remote location, who have logical or physical access to I&C systems may, as insiders, pose a threat to the safety and security of a nuclear facility. These insiders may be facility employees

[2] Malicious acts do not include events caused by human error or random equipment or component failures.

or personnel employed by vendors, contractors or suppliers who may be able to use their authorized access to perform malicious acts. The need for the protection of computer systems from insider threats is recognized in Ref. [5].

OBJECTIVE

1.10. The objective of this publication is to provide guidance for the protection of I&C systems at nuclear facilities on computer security against malicious acts that could prevent such systems from performing their safety and security related functions. While the focus of this publication is on the secure operation of these systems, application of this guidance may also contribute to improving the safety and operational performance of nuclear facilities.

1.11. This publication is intended for competent authorities, including regulatory bodies, as well as nuclear facility management, operations, maintenance and engineering personnel, I&C vendors, contractors and suppliers, I&C designers, research laboratories and other organizations concerned with the safety and security of nuclear facilities.

SCOPE

1.12. The scope of this publication is the application of computer security measures to I&C systems that provide safety, security[3] or auxiliary functions at nuclear facilities. These measures are intended to protect I&C systems against malicious acts perpetrated by individuals or organizations. This publication also addresses the application of such measures to the development, simulation and maintenance environments of these systems.

1.13. The guidance given in this publication is applicable to I&C systems at new[4] nuclear facilities and to new I&C systems at existing facilities. The guidance is expected to be implemented to the greatest extent possible for legacy I&C systems at existing facilities, including those that do not use digital technology.

1.14. While not explicitly addressed in this publication, other interfacing systems and information and communications technology (ICT) systems such as work

[3] Systems providing security functions include those used for physical protection and nuclear material accountancy and control.

[4] A new facility is a facility that has yet to complete the commissioning stage.

control and communications systems may introduce risks to the I&C system(s). These risks needs to be accounted for when designing and implementing computer security measures for I&C systems in a facility. Computer security measures for these systems may be different from those applied to I&C systems and are to be evaluated and tailored appropriately.

1.15. This publication does not provide comprehensive guidance on safety considerations for I&C systems. Such guidance can be found in Refs [4, 6]. Additionally, this publication does not define or alter the technical terms used in IAEA safety standards and other safety related IAEA publications. These terms are highlighted in this publication, when used, and their definitions can be found in the IAEA Safety Glossary [7].

STRUCTURE

1.16. Following this introduction, this publication is separated into four sections. Section 2 presents an overview of I&C systems in use at nuclear facilities and the role of computer security in protecting these systems from cyber attacks. Section 3 presents the relationship between computer security and safety for I&C systems. Section 4 presents computer security guidance to be applied in the various life cycle phases of I&C systems, including during the decommissioning of a facility.

2. KEY CONCEPTS FOR COMPUTER SECURITY OF I&C SYSTEMS

2.1. The I&C systems in nuclear facilities are used to monitor and control processes and equipment. These systems include:

(a) SCADA (supervisory control and data acquisition) systems;
(b) Distributed control systems;
(c) Centralized digital control systems;
(d) Control systems composed of programmable logic controllers;
(e) Micro-controllers and ‘smart’ devices;
(f) Systems using programmed logic devices (e.g. field programmable gate arrays, complex programmable logic devices and application-specific integrated circuits).

Similar systems that control industrial plants are often called ‘industrial control systems’.

2.2. I&C systems are designed to provide for the safe, secure, reliable and deterministic behaviour of the nuclear facility in both normal and abnormal operation[5]. Design considerations and measures intended to improve safety may also provide benefits for security. For example, design measures such as deterministic performance, fault avoidance, fault detection, fault tolerance approaches, configuration management, independent verification and validation, and other advanced testing methods may provide some defence against malicious attempts to alter the behaviour of I&C systems.

2.3. The design of the overall I&C architecture in nuclear facilities incorporates concepts that may contribute to computer security by mitigating the effects of intentional or accidental mal-operation[6], such as independence, redundancy, safety defence in depth and diversity[7]. The term ‘safety defence in depth’ is used in this publication to refer to defence in depth as defined in the IAEA Safety Glossary [7], to distinguish it from the application of the similar, but security-focused concept of ‘defence in depth’ (as defined in the Nuclear Security Fundamentals [8]) in implementing computer security measures, described in Section 4.

2.4. The implementation of these concepts in a facility’s overall I&C architecture and other design measures should be assessed to determine their contribution to computer security. For example, diversity of design or technology is likely to reduce common vulnerabilities among key safety or control systems; however, it may add vulnerabilities that are unique to each individual system.

2.5. Guidance contained in this publication applies to all I&C systems associated with a nuclear facility unless otherwise noted.

---

[5] Abnormal operation is referred to in the IAEA Safety Glossary [7] as a synonym for ‘anticipated operational occurrence’. For this publication, the former term is considered more readily understood.

[6] The term ‘mal-operation’ is used in this text to refer to situations that have not been previously considered (i.e. are not anticipated operation occurrences), but for which the I&C system does not operate as expected.

[7] Independence, redundancy, safety defence in depth and diversity refer here to specific concepts that are used in the IAEA Safety Glossary [7].

COMPUTER SECURITY OF I&C SYSTEMS

2.6. Paragraph 2.2 of Ref. [2] states that:

"The State's *physical protection regime*[8] should seek to achieve these objectives through:

— Prevention of a *malicious act* by means of deterrence and by protection of sensitive information;
— Management of an attempted *malicious act* or a malicious act by an integrated system of *detection*, delay and response;
— Mitigation of the consequences of a *malicious act*."

2.7. Examples of how prevention, management and mitigation can be applied to computer security of I&C systems include:

— Prevention: Installing fail-secure devices that block unauthorized data communications to reduce the potential for a network based cyber attack that would adversely affect the I&C system.
— Management, including detection, delay and response: Through the inspection of system event log files, the operator may be able to detect precursors and initiate protective actions prior to the commencement of a malicious act that could adversely affect the safety or security of a facility.
— Mitigation and recovery: If an I&C system is discovered to be infected with malware, once the malware's propagation has been stopped, the operator would determine whether compensatory control measures (e.g. updated antivirus signatures, installation or enhancement of intrusion prevention or detection systems or both) are needed to prevent re-infection, conduct a system rebuild, verify the effectiveness of the compensatory control measures, restore the system and place it back into to service, after performing detailed safety analysis and system integrity verification activities, if necessary.

2.8. Protection of I&C systems against compromise is sometimes based upon the presumption that a single preventive measure is sufficient, such as the isolation of the systems from other networks. However, such a presumption is likely to result in insufficient application of management and mitigation measures so that

[8] Historically, the term 'physical protection' has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities.

failure of this single computer security measure might result in the compromise of the protected system.

2.9. Many different approaches, methods, techniques, standards and guidelines for computer security have been developed for general ICT systems. Some of these are not directly applicable to I&C systems at nuclear facilities, which have specific computer security needs that are not shared with ICT systems.

2.10. Nevertheless, since computer security for I&C systems cannot be fully separated from computer security for ICT systems, operators and regulators should develop computer security policies, requirements, measures and practices that consider I&C systems and ICT systems in an integrated way.

2.11. Many I&C systems have a life cycle of decades, including periods during which vendor support may be unavailable or inadequate to meet the computer security requirements[9] for the systems. This includes support given by the original vendor and by associated third parties. For example, over time, antivirus programs may not provide sufficient protection against the exploitation of vulnerabilities in I&C systems, owing to loss of hardware or software compatibility or failure to continue providing signature updates.

2.12. In most applications, I&C systems operate in real time, and I&C system actions are performed within strict time intervals. Examples of such I&C system actions at nuclear facilities include control of normal operations, protective actions, limitation actions and alarm signalling to operators. Computer security measures should not impede, prevent or delay the performance of necessary operational or safety actions. Computer security measures for modern I&C systems can be used to prevent, detect, delay and respond to malicious acts and mitigate their consequences, but care needs to be taken to ensure that the response measures do not impede accredited safety functions or place the system outside of its design basis[10].

---

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

[10] The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear facility. The design basis is further defined in the IAEA Safety Glossary [7]. The design basis for I&C systems is described in more detail in Section 3 of Ref. [4].

2.13. Computer security measures that are retrospectively applied or poorly implemented may introduce additional complexity into the I&C system design, which may result in an increased likelihood of I&C system failure or mal-operation.

2.14. Essential Element 9 of the Nuclear Security Fundamentals [8] identifies the use of risk informed approaches to allocate resources and in the conduct of nuclear security related activities. A design developed using a risk-informed approach to account for security considerations from the beginning of the design process may be simpler and more robust owing to the integration of the security features, the elimination of unnecessary functionality (e.g. remote access) or to system hardening.

COMPUTER SECURITY MEASURES

2.15. Computer security measures are used to prevent, detect, delay and respond to malicious acts as well as to mitigate the consequences of such acts. Computer security measures are also used to ensure that non-malicious acts do not degrade security and increase the vulnerability of computer based systems to malicious acts.

2.16. Computer security measures that address vulnerabilities in the system or provide protective layers of defence can be assigned to one of three categories: technical control measures, physical control measures or administrative control measures. All three categories should be considered and an appropriate combination selected when developing integrated computer security for I&C systems.

2.17. Technical control measures are hardware and/or software used to prevent, detect, mitigate the consequences of and recover from an intrusion or other malicious act. The ability of technical control measures to provide continuous and automatic protective actions should be considered when evaluating their effectiveness compared with physical or administrative control measures.

2.18. Physical control measures are physical barriers that protect instruments, computer based systems and supporting assets from physical damage and unauthorized physical access. Physical control measures include locks, physical encasements, tamper indicating devices, isolation rooms, gates and guards.

2.19. Administrative control measures are policies, procedures and practices designed to protect computer based systems by providing instructions for actions of employees and third party personnel. Administrative control measures specify permitted, necessary and forbidden actions by employees and third party personnel. Administrative control measures for nuclear facilities include operational and management control measures.

APPLICATION OF A GRADED APPROACH

2.20. The operator should impose computer security requirements based on a risk informed graded approach that takes into account the following:

- The importance of I&C system functions for both safety (i.e. safety classification) and security;
- The identified and assessed threats to the facility;
- The attractiveness of the I&C system to potential adversaries;
- The vulnerabilities of the I&C system;
- The operating environment;
- The potential consequences that could either directly or indirectly result from a compromise of the system.

Such an approach could be based on the results of a computer security risk assessment.

2.21. In a graded approach, computer security requirements are defined proportionately to the potential consequences of an attack. The potential consequences of a compromise on I&C system function are, arranged in the order of worst to best cases:

- The function is indeterminate. The effects of the compromise result in an unobserved alteration to system design or function.
- The function has unexpected behaviours or actions that are observable to the operator.
- The function fails.
- The function performs as expected, meaning the compromise does not adversely affect system function (i.e. it is fault tolerant).

2.22. Computer security levels should be applied as described in this publication to I&C systems to allow for the implementation of a graded approach to computer security.

2.23. An example of an implementation of a graded approach using security levels[11] is provided in Ref. [3]. Conversely, an example of an implementation of a graded approach for safety is provided in Ref. [9].

COMPUTER SECURITY LEVELS

2.24. Computer security levels and safety classes are distinct but related concepts. The safety classification of an item important to safety is based upon the relevance to safety of its function as well as the potential consequences of its failure.

2.25. Each I&C system function associated with a facility is generally assigned a computer security level to indicate the degree of computer security protection it needs. Each level will need different sets of computer security measures to satisfy relevant computer security requirements. The security levels are often defined based on an organization's security objectives. Reference [10] provides further information on the implementation of security levels and zones.

2.26. The subsystems and components of I&C systems whose mal-operation could affect nuclear safety (including accident mitigation), nuclear security and nuclear material accounting and control are identified and assigned to security levels according to their contribution to I&C system function.

2.27. The operator assigns a security level to an I&C system, subsystem or component based on the potential consequences of its failure or mal-operation, including mal-operation in a way that differs from its design or conceivable failure modes that would be identified in a facility safety analysis. The computer security level assigned to an I&C system, subsystem or component is specific to that system, subsystem or component, and is independent of its environment.

COMPUTER SECURITY ZONES

2.28. The security zone concept involves the logical and/or physical grouping of computer based systems that share common computer security requirements, due to inherent properties of the systems or their connections to other systems. All systems located within a single zone are protected at the same security level,

[11] References to 'security levels' and 'security zones' throughout this publication indicate computer security levels and computer security zones.

namely that assigned to the I&C system function with the most stringent security level within the zone. Grouping of I&C systems into security zones may simplify the application and management of computer security measures.

2.29. Considerations for implementation of security zones should fulfil the following criteria:

- Systems belonging to the same zone have similar needs for computer security measures.
- Systems belonging to the same zone form a trusted area for internal communications between those systems (i.e. internal trusted zone area).
- Each zone comprises systems that have the same or comparable importance for the security and safety of the facility, or belong to an internal trusted zone area.
- System safety architecture requirements (e.g. redundancy, diversity, geographic and electrical separation, single failure criterion) are maintained.
- Technical control measures are implemented at zone boundaries to restrict data flow and communication between systems located within different zones (e.g. remote location) or assigned to different security levels.
- Removable media, mobile devices and other temporary equipment that needs logical or physical access to a system are used only within a single zone or a specified set of zones.
- Zones may be partitioned into sub-zones to improve the configuration.

2.30. When security zones are used in a facility, some I&C systems or components could be assigned to a zone assigned a more stringent security level than their own inherent security level. For example, a communication device that performs only lower level safety or security functions may be assigned the same security level as the reactor protective system, if it is located within the reactor protective system security zone. This assignment is due to the potential for malicious use of the device to compromise the reactor protective system components, which are highly important for safety. Furthermore, the use of the reactor protective system security zone allows for the creation of an internal trusted zone area, thereby ensuring that additional computer security measures will not need to be implemented between the reactor protective system components and the communication device.

3. RISK INFORMED APPROACH TO COMPUTER SECURITY FOR I&C SYSTEMS

3.1. A risk informed approach to computer security for I&C systems may use risk assessments to identify a facility's vulnerabilities to cyber attack related to these systems and determine the consequences that could result from the successful exploitation of these vulnerabilities. Computer security measures can then be assigned based on the results of the risk assessments.

3.2. Because I&C systems are often essential for facility safety, an understanding of nuclear safety can assist in assessing risk, developing computer security measures for the I&C system, assessing potential conflicts between safety and security, and considering how such conflicts could be resolved. For example, adversaries could sabotage a facility through a cyber attack on a facility's I&C systems, resulting in potential safety and security consequences. Such attacks might cause failures of I&C systems or might cause I&C systems to operate in ways that differ from their intended behaviour or their analysed failure modes. Malicious acts may affect a single I&C system or multiple I&C systems. For example, malicious acts have the potential to bypass or cause simultaneous failure of multiple levels of safety defence in depth[12]. Malicious acts may also combine cyber attacks with physical attack elements.

3.3. Inadequate computer security or a compromised I&C system may cause the safety of a facility to be jeopardized. For example, if an I&C system is compromised, an adversary might obtain data that provide the critical information needed to plan an attack or modify data that facilitate sabotage of facility systems or unauthorized removal of nuclear materials. Alternatively, a cyber attack resulting in sabotage might initiate an accident or degrade the performance of a safety function. Such an attack might also lead to a loss of system availability.

3.4. Cyber attacks on I&C systems might also lead to consequences that enable the unauthorized removal of nuclear material from a facility. I&C systems fulfilling physical protection or nuclear material accounting and control functions may be affected by cyber attacks, which could place a facility in a condition that has not been considered in the site security plan. A malicious act could also combine a cyber attack on these systems with physical attack elements with the objective of the unauthorized removal of nuclear material.

---

[12] The five nuclear safety defence in depth levels are detailed in Ref. [7].

3.5. Therefore, computer security measures for I&C systems need to address both cyber attacks that directly cause sabotage and those that collect information that could facilitate sabotage of the nuclear facility or unauthorized removal of nuclear material.

INTERFACE WITH FACILITY COMPUTER SECURITY RISK MANAGEMENT

3.6. The operator should have a facility computer security risk management (CSRM) process to implement computer security to protect the functions performed by I&C systems. This process is used to identify the facility's vulnerabilities[13] to cyber attack and to determine the consequence of successful compromise of one or more functions performed by I&C systems (which may include exploitation of vulnerabilities).

3.7. The outputs of the facility CSRM processes should include an identification of facility functions performed by I&C systems including supporting and complementary systems that, if compromised, could adversely affect safety, security of nuclear material or accident management. The facility safety analysis may be used as an input for the facility CSRM, but the safety analysis alone is not sufficient as it does not address all mal-operations. Mal-operations caused by cyber attacks might place the facility in conditions that have not been considered by the safety analysis.

3.8. The outputs of the facility CSRM processes should identify the potential consequences related to nuclear safety, nuclear security and nuclear material accounting and control resulting from system compromise due to a cyber attack on the I&C systems. When analysing the consequences of an attack on an I&C system, the possibility should be considered that the attack might be a component of a larger attack affecting multiple I&C systems or a combined cyber and physical attack. This analysis could then be used to assign the appropriate security levels to individual I&C systems and components based upon the potential consequences of their failure or mal-operation.

3.9. The security levels assigned to the I&C systems may be associated with a hierarchical list of potential safety or security consequences. For example, plant

[13] The hierarchy and definitions for plant states are provided in the Safety Glossary [7] unless otherwise noted.

states, sabotage consequences, nuclear material categorization hierarchies or a combination of these might be used, as in the examples in paras 3.10–3.13 and 3.15.

3.10. For reasons of safety, plant states could be used to denote the potential safety consequences of a cyber attack on I&C systems. For example, plant states could be associated with security levels for I&C systems as follows, ordered from the situation with the lowest to the situation with the highest consequence:

(1) Normal operation: A cyber attack on I&C systems cannot cause facility operation outside limits and conditions specified for normal operation.
(2) Anticipated operational occurrence: A cyber attack on I&C systems may cause the plant state to deviate from normal operation in a way that is anticipated to occur, but which in view of appropriate design provisions does not cause any significant damage to items important to safety or lead to accident conditions.
(3) Design basis accident[14]: A cyber attack on I&C systems may cause accident conditions that remain within the facility design basis and for which the damage to the nuclear material (or other radioactive material) and the release of radioactive material are kept within authorized limits.
(4) Design extension conditions: A cyber attack on I&C systems may cause accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

3.11. The consequences of sabotage of functions performed by I&C systems could also be associated with security levels. Such an approach would involve the State defining the threshold for unacceptable radiological consequences (URC), as recommended in para. 3.44 of Ref. [2]. The definition of a threshold for URC may be based on quantitative or qualitative criteria, which may be expressed in terms of releases of radionuclides (e.g. a release exceeding some identified amount), doses (e.g. a release leading to a radiation dose exceeding some identified value to an individual located at some identified point, usually off-site) or facility conditions (e.g. sabotage that may result in significant core damage in a reactor). As stated in Ref. [11], paras 3.94 and 95:

[14] The hierarchy and accompanying text for Design Basis Accident and Design Extension Conditions are taken from Ref. [7].

> "targets for which sabotage could potentially result in a substantial radiological release significantly affecting the population and environment beyond the boundaries of the nuclear facility need the highest level of protection. Such a severe event is referred to…[in Ref. [2]] as having high radiological consequences.
>
> "Therefore, the State should also define the threshold for high radiological consequences."

3.12. An example of a hierarchical list of potential consequences of sabotage is provided in Ref. [11] and summarized for I&C system functions as follows, ranked from the lowest to the highest consequences:

- Radiological consequence below the URC threshold: Targets posing these low consequences need a correspondingly low level of protection.
- URC can be graded into three categories ranked from the lowest to the highest consequences:
  - Consequence Level C: Sabotage that could result in doses to persons on-site that warrant urgent protective action to minimize on-site health effects.
  - Consequence Level B: Sabotage that could result in doses or contamination off-site that warrant urgent protective action to minimize off-site health effects (may also be considered high radiological consequences).
  - Consequence Level A: Sabotage that could give rise to severe deterministic health effects off-site (likely also to be considered high radiological consequences).

3.13. Security levels could also be associated with the possibility of the unauthorized removal of nuclear material. The potential consequences of cyber attacks on I&C systems performing physical protection or nuclear material accounting and control functions could be associated with security levels on the basis of the category of material that could be subject to unauthorized removal. Table I of Ref. [2] provides the criteria for the categorization of nuclear material and further identifies recommendations for physical protection based on this categorization.

3.14. There is currently no international consensus on a model for a completely integrated hierarchy of all safety and security consequences arising from accidents and nuclear security events resulting from cyber attacks. However, the operator or State should develop such a hierarchy at a national level.

3.15. Other consequences, such as loss of reputation, may also be considered when evaluating the combined consequences of a cyber attack on facility I&C systems. A listing of possible consequences can be found in Ref. [12].

3.16. Adversary tactics and techniques are constantly changing and nuclear facilities should foster a nuclear security culture that continually reviews computer security risks and allows for the adaptability of the facility computer security programme. Nuclear security culture is further explained in Ref. [13].

3.17. System configuration and activities associated with I&C systems enhanced with digital equipment should be analysed to identify changes to logical and physical pathways that could provide opportunities that an adversary could exploit. These activities associated with the I&C systems include temporary maintenance activities, procurement processes, vendor support, communication with field devices and manual software updates.

3.18. Facility CSRM is an iterative and cyclical process that could include an initial analysis, threat identification and assessment, definition of security levels, periodic review and updated analysis. There should be a defined acceptance process to review and verify the results of new or updated analyses.

3.19. For new facilities, the facility CSRM should be performed as part of the design process and accepted before completion of the initial commissioning phase.

3.20. For existing facilities, inputs to the new or updated facility CSRM may include safety analysis, details of safety and process architecture and previously accepted facility CSRM outputs.

INTERFACE WITH SYSTEM CSRM

3.21. The system CSRM should use the facility CSRM outputs (if available) and the design basis documents of the I&C systems as inputs to determine the security risk posed by cyber attacks on individual or multiple I&C systems, subsystems or components. The assessed computer security risk to the I&C systems should be analysed and documented.

3.22. The operator should assign roles and responsibilities throughout the I&C system life cycle for the assessment and management of the I&C system computer security risks. Computer security needs focused efforts by multidisciplinary organizations and teams. For example, the operator may establish working groups

responsible for managing the computer security processes and activities as well as for obtaining authorizations.

3.23. The operator should keep an inventory of the I&C system, including software, subsystems and components, which is updated and maintained throughout the life cycle of the system. The operator should use this inventory when performing the system CSRM.

3.24. I&C system components should be assessed and assigned the appropriate security level based on the system CSRM. For these components, the safety and security consequences that could result from mal-operation or compromise should be identified. If security zones are implemented within the facility, the security zone should be assigned and identified.

3.25. When performing the system CSRM, the operator should consider the possibility of cyber attack at each phase of the I&C system life cycle. The operator should also consider in the assessment that cyber attacks may affect an individual system or multiple systems and could be used in combination with other forms of malicious acts causing physical damage. Malicious actions that could change process signals, equipment configuration data or software should also be considered in the system CSRM.

3.26. In addition, all attack vectors that could be used to inject malicious code or data into the I&C system should be considered in the system CSRM. For example, malicious code could be introduced into the I&C system via communication connections, supplied products and services or portable devices that are temporarily connected to target equipment.

3.27. The system CSRM should determine the likelihood of each potential consequence associated with the I&C system occuring, using as inputs the following: the availability of specific attack vectors that could be used to inject malicious code or data into the I&C system; application and effectiveness of computer security measures; threat capabilities; and other associated information.

3.28. The system CSRM is an iterative and cyclical process that, similarly to the facility CSRM, involves an initial analysis, implementation of computer security measures, periodic review and updated analysis. The system CSRM should be considered for review when one of the following occurs:

— The facility CSRM or facility safety analysis is revised.
— System modifications are made.

— Relevant security events or incidents occur.
— New or changed threats or vulnerabilities are identified.

3.29. The system CSRM should identify human actions or omissions that might affect security.

ASSIGNMENT OF COMPUTER SECURITY MEASURES

3.30. The guidance in paras 3.31–3.34 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

3.31. Each I&C system, subsystem or component should be assigned a security level in accordance with the potential consequences of its failure or mal-operation for both safety and security.

3.32. The application of computer security measures to each I&C system should be determined by its assigned security level or the security level of the security zone in which it resides, whichever is more stringent.

3.33. Computer security requirements should be identified and defined for each security level. The effectiveness of measures implementing these requirements should be evaluated to ensure that sufficient protection is provided for the I&C systems assigned to each security level.

3.34. If computer security measures are not able to provide sufficient protection for I&C systems at each security level, additional or alternative measures should be considered, e.g. facility level physical protection features, independent electronic functions, system redesign or administrative measures that eliminate specific vulnerabilities or reduce the consequences of mal-operation.

SAFETY–SECURITY INTERFACES

3.35. As stated in Ref. [8], para. 1.2,

> "Nuclear security and nuclear safety have in common the aim of protecting persons, property, society and the environment. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way that

security measures do not compromise safety and safety measures do not compromise security."

Additional guidance on safety considerations for I&C systems can be found in Refs [4, 6].

3.36. The appropriateness of a given computer security measure will depend on safety, security and operational considerations. Input from safety, security and operations personnel is needed to assign computer security measures for I&C systems. Computer security measures cannot exist in isolation from safety concerns, and safety features cannot exist in isolation from security concerns. For example, for safety reasons, certain security functions (e.g. collection of audit records or generation of security alarms) might need to be implemented in separate systems that can monitor the I&C system but do not adversely affect the system's ability to perform its essential functions. Alternatively, performance of active security scans only when I&C systems are not in service could meet security goals while limiting the impact on the operational systems.

3.37. Inappropriately designed computer security measures could introduce potential failure modes into the system, increase the likelihood of spurious operation and challenge the system's ability to reliably perform its safety function. For example, an inappropriately designed implementation of a malware or virus detection system within the I&C system could increase I&C system complexity, increase I&C system latency and result in the I&C system being vulnerable to exploitation. However, an appropriately designed technical control measure that ensures that only verified and validated software is allowed to run on an I&C system could improve this system's ability to reliably perform its safety function while providing significant security benefits.

3.38. Many functions that are designed into I&C systems for safety reasons may also have security benefits. One example is the checking of received data for validity, authenticity and integrity before it is used in an I&C system function.

3.39. There may be situations where a computer security measure cannot be implemented in accordance with an I&C system's assigned security level, for example, owing to conflicts with essential safety functions, but these exceptions should be thoroughly analysed and justified.

3.40. The full set of I&C system computer security measures should work together and prevent (or not introduce) single points of failure.

3.41. Safety strategy may have the potential to adversely affect security. For example, design for safety often involves the allocation of functions to different subsystems (or processors) in order to isolate the effects of failure, and the provision of redundant and diverse systems so that single failures will not compromise important functions. These strategies result in an increase in the number of subsystems in the I&C systems, which in turn increases the number of targets for cyber attack. Therefore, measures should be taken to reduce the risk that a cyber attack would result in a loss of system diversity or redundancy. Computer security measures should not introduce new vulnerabilities that could result in common cause failures between these redundant and diverse systems.

SAFETY CONSIDERATIONS FOR COMPUTER SECURITY MEASURES

3.42. The guidance contained in paras 3.43–3.52 applies to all I&C systems important to safety.

3.43. The implementation of computer security measures should not adversely affect the essential safety functions and performance of the I&C system.

3.44. Neither the normal nor the abnormal operation of any computer security measure should adversely affect the ability of an I&C system to perform its safety function.

3.45. The operator should identify, document and consider in the system hazard analyses the failure modes of the computer security measures and how the failure modes would affect I&C system functions.

3.46. Computer security measures that protect the human–system interface should not adversely affect the operator's ability to maintain the safety of the facility. The operator should also consider adverse effects such as the interception and modification of process data sent to the human–system interface (e.g. spoofing) with the aim of preventing or delaying the operator from actuating a safety function (e.g. manual trip).

3.47. Computer security measures that cannot be practically integrated into the I&C system should be implemented separately from the I&C system. Additional administrative control measures may be necessary to use and maintain these separate devices.

3.48. Computer security measures integrated into I&C systems should be developed according to the management systems guidance in Ref. [14] or an equivalent alternative management system and qualified to the same level as the system in which the computer security measures reside.

3.49. If there is a conflict between safety and security, then design considerations taken to ensure safety should be maintained provided that the operator seeks a compatible solution to meet computer security requirements. Compensatory computer security measures should be implemented to reduce the risk to an acceptable level and be supported by a comprehensive justification and security risk analysis. The implemented measures should not rely solely upon administrative control measures for an extended period. The absence of a security solution should never be accepted.

3.50. The primary responsibility for design, selection and implementation of computer security measures should be clearly assigned by the operator, but should be a collaborative effort between personnel responsible for activities involving I&C system design, maintenance, safety and security.

3.51. I&C system design analysis should demonstrate that computer security measures integrated into the I&C system and those implemented as separate devices will not adversely affect the accredited safety functions of systems and components important to safety.

3.52. The maintenance of computer security measures should not adversely affect the availability of I&C systems.

4. COMPUTER SECURITY IN THE I&C SYSTEM LIFE CYCLE

4.1. The design of I&C systems for nuclear facilities should be managed through the facility's integrated management system[15] to ensure that all computer security requirements are considered and implemented in all phases of the I&C system life cycle and that these computer security requirements are met in the final design. Reference [14] establishes the General Safety Requirements for the management systems of nuclear facilities. In addition, Ref. [8], para. 3.12(a) refers to the importance for nuclear security of integrated management systems. Reference [3] provides further discussion of the overall relationship between management systems and computer security.

4.2. Paragraph 2.13 of Ref. [4] states that:

> "In digital I&C systems, demonstration that the final product is fit for its purpose depends greatly, but not exclusively, on the use of a high quality development process that provides for disciplined specification and implementation of design requirements."

Paragraph 2.14 adds that

> "in the nuclear power domain as well as in other safety-critical domains such as aerospace, development processes have been applied that are commonly represented as life cycle models, which describe the activities for the development of electronic systems and the relationships between these activities. … Normally, activities relating to a given development step are grouped into the same phase of the life cycle."

Computer security should be considered in all phases of the I&C system life cycle.

4.3. As stated in Ref. [4], para. 2.17,

---

[15] According to Ref. [7], the management system is "A set of interrelated or interacting elements (system) for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective manner." In this publication, this includes the organizational structure, the organizational culture, policies and processes, including those to identify and allocate resources (e.g. personnel, equipment, infrastructure and the working environment) for developing I&C systems.

"Three fundamental levels of life cycles are needed to describe the development of I&C systems:

— An overall I&C architecture life cycle; [16]
— One or more individual I&C system life cycles;
— One or more individual component life cycles: Component life cycles are typically managed in the framework of platform development and independent of the overall architecture level and the individual system level life cycles. Component life cycles for digital systems are typically divided into separate life cycles for the development of hardware and software."

4.4. The definition of life cycle models and the activities grouped into each life cycle phase are generally determined by a system's developers and operators, but the definition and implementation should be a multidisciplinary effort involving many other domains, including computer security. Generally the developers have lead responsibility for the I&C systems until the systems are transferred to the operations organization for installation, integration and commissioning.

4.5. Given that the life cycle I&C systems can span several decades, different organizations may play the role of developers or other roles during the life cycle of a system. For example, it is not uncommon for a vendor to carry out the original development and for the purchaser to develop modifications at a later time, especially if the modifications are minor. The fact that these modifications are developed by different organizations does not eliminate the need to implement computer security measures in all phases in the I&C system life cycle.

4.6. At the earliest opportunity, computer security should be coherently planned for all I&C architecture, system and component life cycles. This planning should specify the computer security measures to be applied in each phase to protect the I&C architecture, systems and components from cyber attacks that may jeopardize functions important to safety. The possibility that safety functions or computer security measures may change during later phases should be considered.

4.7. The I&C system development process should seek to minimize potential computer security vulnerabilities and weaknesses and identify the residual

[16] As defined in Ref. [4], para. 3.10, "the overall I&C architecture is the organizational structure of the plant I&C systems."

potential vulnerabilities and weaknesses in each phase of the I&C system life cycle.

4.8. While life cycle models may be organized in many ways, the following notional life cycle phases are used in this publication as a framework for describing computer security considerations during the I&C life cycle:

— Process planning;
— Design basis;
— Overall I&C architecture and functional allocation;
— I&C system requirements specification;
— Selection of predeveloped items;
— Detailed design and implementation;
— System integration;
— System validation;
— Installation, integration and commissioning;
— Operation and maintenance;
— Modification;
— Decommissioning.

4.9. In addition to these phases, the I&C system life cycle also involves many activities that are common to all life cycle phases. The common activities that are important to computer security are:

— Quality assurance;
— Configuration management;
— Verification and validation[17];
— Security assessment;
— Documentation.

4.10. The computer security requirements and activities for each life cycle phase should be commensurate with the consequences resulting from unauthorized or inappropriate access, use, disclosure, manipulation, disruption or destruction of the I&C system. Consideration should also be given to the compromise of

[17] The IAEA Safety Glossary [7] defines both verification and validation. Computer system verification is "The *process* of ensuring that a phase in the *system* life cycle meets the requirements imposed on it by the previous phase." Computer system validation is "The *process* of testing and evaluating the integrated computer *system* (hardware and software) to ensure compliance with the functional, performance and interface requirements."

any system, support system or information that might adversely affect safety or security.

4.11. The remainder of this section is divided into subsections that discuss general computer security guidance that applies to all life cycle phases, and security guidance that is specific to the individual life cycle phases. In this discussion, the phases are discussed only once but the guidance should be applied to any life cycle in which the phase occurs.

GENERAL GUIDANCE FOR COMPUTER SECURITY

4.12. The computer security policy for a nuclear facility specifies the overall computer security objectives for the facility. For facility and system computer security planning, these objectives are specified in the policy in clear, specific and, when possible, measurable terms. The facility objectives are translated into system objectives. Reference [3] provides further guidance on computer security at nuclear facilities.

4.13. The computer security policy should include elements addressing the security of I&C systems and, consequently, the policy should apply to any organization that is responsible for activities in the I&C system life cycle. These organizations include operators, vendors, contractors and suppliers that design, implement and procure I&C systems, software and components.

4.14. Each organization responsible for I&C life cycle activities should identify and document the standards and procedures that conform with the applicable security policies to ensure the hardware, software and firmware minimize undocumented code (e.g. back door coding), malicious code (e.g. intrusions, viruses, worms, Trojan horses and logic bombs) and other unwanted, unnecessary or undocumented functions or applications, with the aim of minimizing the number of possible pathways through which a cyber attack could take place.

4.15. The computer security policy, programme, associated standards and applicable procedures should address each individual phase of the I&C system life cycle to protect the facility's I&C systems against compromise.

4.16. Computer security policies, programme, standards and procedures as well as all computer security measures should meet regulatory and computer security requirements.

4.17. Computer security policies, standards and procedures may be provided in an organization's I&C security programme or may be incorporated into the I&C system life cycle plans. In practice, a mixed approach is often taken.

ASPECTS OF THE COMPUTER SECURITY POLICY RELATED TO I&C SYSTEMS

4.18. The computer security policy for nuclear facilities should describe the application of a graded approach to the implementation of computer security measures for I&C systems. The graded approach should be applied in accordance with the importance for safety and security of each I&C system function (e.g. in accordance with the assigned security level of each system). Management should set and enforce clear computer security policy objectives consistent with overall facility safety and security objectives, and specifically address the security of I&C systems. More detail on general considerations for a computer security policy and programme are identified in Ref. [3].

4.19. The computer security policy should include considerations important for I&C systems, such as:

— Access control, including both physical and logical access control, and use of least privileges.
— Configuration and asset management, including password management, patch management, system usage, system hardening, configuration control, restrictions on use of mobile devices and removable media, wireless devices and networks and remote access;
— System and component integrity verification activities;
— Procurement processes;
— Risk and threat management, including processes to gather, analyse, document and share with others who have a need to know and to act upon information about vulnerabilities, weaknesses and threats);
— Incident response and recovery;
— Auditing and assessments.

4.20. The computer security policy should assign roles and responsibilities to organizations or individuals that perform I&C system life cycle activities.

COMPUTER SECURITY PROGRAMME

4.21. Each organization that has responsibility for implementing I&C system life cycle activities should develop and implement an integrated or separate computer security programme addressing I&C systems.

4.22. The computer security programme should define the roles and responsibilities for each phase of the I&C system life cycle for every I&C system.

4.23. The computer security programme should specify that responsible organizations apply the concept of defence in depth and identify applicable computer security measures for I&C systems according to their assigned security level.

4.24. The computer security programme should specify the implementation of computer security measures intended to protect against malicious acts committed by insiders and the manipulation of the I&C system (including its integrity) in each phase of the I&C system life cycle.

4.25. The computer security programme should specify that access to I&C systems, components, software, configuration data and tools is controlled during all phases of the I&C system life cycle. Examples of access control practices are the principle of least privilege and need-to-know.

4.26. The computer security programme should address the confidentiality of computer security measures, including the protection of related documentation, consistent with the security level of the I&C systems referred to in the documentation.

4.27. The computer security programme should address potential computer security vulnerabilities and weaknesses for each phase of the I&C system life cycle.

4.28. The computer security programme should identify the process by which I&C system security information, such as details regarding vulnerabilities found in facility I&C systems or the specific defences being used to protect the systems, is classified as sensitive information and compartmentalized[18]. Reference [8]

[18] Compartmentalization means dividing information into separately controlled parts to prevent insiders from collecting all the information necessary to attempt a malicious act.

defines sensitive information as “Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.”

4.29. Nuclear facilities and associated organizations are strongly encouraged to share other non-sensitive vulnerability information so that facilities will be better prepared in the event that vulnerability information on I&C systems is distributed and shared among potential adversaries. Guidance on the security of nuclear information (including classification) is provided in Ref. [15].

4.30. The computer security programme for I&C systems should specify that periodic computer security reviews and assessments be performed and documented in each life cycle phase.

4.31. The computer security programme should specify the computer security measures that provide for a secure environment in which development activities may take place.

4.32. For legacy I&C systems, there may be more reliance on administrative control measures and isolation than for contemporary systems. The computer security programme should identify and sustain additional compensatory computer security measures that are necessary to ensure computer security for legacy I&C systems.

SECURE DEVELOPMENT ENVIRONMENT

4.33. The guidance contained within paras 4.34–4.40 applies to the development of all I&C systems, subsystems and components to which a graded approach to computer security is applied in accordance with their assigned security level.

4.34. I&C system development should be conducted in a secure development environment. This applies to both internal and external sites. The assignment of a security level to this environment should consider the security level of the system in the target environment, the security level of other systems developed or stored within the common development environment and the development tools. The environment’s computer security measures should be evaluated to confirm conformance with requirements of the assigned security level.

4.35. The secure development environment should include administrative control measures, such as configuration control and asset management.

4.36. Physical control measures should be used to control access to secure development environments.

4.37. Test and support equipment used in I&C development environments should be verified to confirm that use of this equipment does not provide pathways for the introduction of malicious code or data into the secure development environment.

4.38. Computer security measures should be in place to control the movement of data and devices for all development phases to ensure that malicious code or data is not introduced into secure development environments and to protect sensitive information associated with I&C systems. These computer security measures should include administrative and technical control measures such as usage restrictions and procedures for the control of removable media and mobile devices. The secure development environment should be recognized as a distinct environment that is both physically and logically separated from the operational and corporate business environments.

4.39. Computer security measures should be implemented to protect the integrity of the secure development environment as well as of design inputs and outputs (e.g. data, configuration files, software updates and software patches) during transfers between the secure development environment and the target environment. These measures could include automated asset configuration systems where the security benefit for the secure development and target environments has been confirmed by analysis.

4.40. Third party or vendor tools used for I&C system development should be tested, validated and protected commensurate with the assigned security level of the development environment.

CONTINGENCY PLANS

4.41. Organizations that implement one or more I&C system life cycle activities should develop contingency plans and procedures to prevent escalation and progression of anomalous behaviour and to recover from computer security incidents. These contingency plans and procedures should be reviewed, periodically exercised and updated when deficiencies are discovered.

4.42. The operator should develop a computer security incident response plan consisting of procedures that define, identify and respond to possible abnormal or suspicious behaviour detected on I&C and associated systems.

4.43. The computer security incident response plan should address information collection and legal requirements for evidence preservation during security events to support investigative analysis.

4.44. The computer security incident response plan should assign personnel to the facility computer security incident response team. This team should be available at the facility to respond to any identified computer security incident. Assigned personnel may include those having I&C system specific or computer security expertise.

4.45. I&C system backup and restoration copies important to contingency plans and procedures should include software, essential data and configuration files. These copies should be stored in a physical location separate from the source location to guard against common cause failure. Computer security measures should be used to protect these copies against theft, tampering, and deletion or destruction.

I&C VENDORS, CONTRACTORS AND SUPPLIERS

4.46. In paras 4.47–4.53, ‘vendors’, ‘contractors’ and ‘suppliers’ are those who supply the nuclear facility with digital equipment, software and services for I&C systems to which a graded approach to computer security is applied in accordance with the assigned security level of the system. The operator should enforce the application of the guidance contained within paras 4.47–4.53 via the execution of a contract with the vendors, contractors or suppliers in question.

4.47. Vendor and sub-vendor organizations should have robust and verifiable computer security processes.

4.48. Vendors, contractors and suppliers should meet all applicable computer security requirements. This includes the application of computer security measures specified by the operator, during support provided on-site or at the vendor, contractor or supplier’s workplace and during any transit or storage of purchased goods.

4.49. The vendor, contractor or supplier should have a computer security management process.

4.50. The applicable computer security requirements at sites where a vendor, contractor or supplier performs activities with I&C systems should be clearly and contractually specified by the operator based on the assigned security level of the system, subsystem or component.

4.51. A process should exist to enable the operator and the vendor, contractor or supplier to report vulnerabilities to one another and to coordinate response and mitigation efforts.

4.52. The vendor, contractor or supplier should demonstrate that it has a credible mechanism for receiving reports of vulnerabilities, assessing them and reporting them to the nuclear facility during the entire period of their contractual service. This consideration may extend beyond any normal warranty period to support the life cycle of the installed equipment. In these cases, the mechanism should be included for the extended period within the contractual obligations agreed upon by the vendors, contractors or suppliers.

4.53. Audits and assessment of vendors, contractors or suppliers responsible for I&C design, development, integration and maintenance should be conducted and the results reported to the operator.

COMPUTER SECURITY TRAINING

4.54. All personnel performing work involving I&C systems, including work involving sensitive information associated with these systems, should receive periodic training on computer security awareness and procedures.

4.55. All personnel who have physical or logical access to I&C systems should be qualified consistent with their computer security responsibilities and should receive specialized security training for I&C systems based upon their roles and responsibilities to maintain their qualification.

4.56. All personnel who have physical or logical access to I&C systems should be trained to a competency level appropriate to their roles to support computer security tasks and recognize potential computer security incidents. These individuals may be informed of the impact of changes made on either the I&C system or its associated computer security measures to which they have access.

4.57. Personnel identified as computer security incident response team members should receive training on computer security incident identification and response. This may involve the use of an I&C test bed as a component of the I&C security training programme.

4.58. Engineering, operations and maintenance staff should be trained to maintain both safety and security functions of I&C systems.

4.59. I&C design personnel should receive training on secure design and programming for I&C systems for nuclear facilities (e.g. how to consider security in software design).

COMMON ELEMENTS OF ALL LIFE CYCLE PHASES

4.60. In most cases, the Safety Requirements for the management system [14] and the general guidance contained in the associated Safety Guides [16, 17] provide sufficient guidance for management system activities related to computer security in all phases of the I&C system life cycle. There are a few areas, however, where more specific guidance is warranted.

Management systems

4.61. The guidance contained within paras 4.62–4.70 applies to all organizations that perform one or more life cycle activities relevant to I&C systems to which a graded approach to computer security is applied in accordance with the security level assigned to the system.

4.62. The Safety Requirements 6–8 for management systems in Ref. [14], paras 4.8–4.20, should be consulted when drafting regulatory and/or computer security requirements related to management systems.

4.63. Each organization that is responsible for developing, deploying, operating, maintaining or retiring I&C systems or components should consider computer security for I&C systems in its integrated management system.

4.64. The integrated management system of the facility should support computer security processes and procedures.

4.65. Life cycle activities should be conducted within the framework of a management system providing for adequate arrangements for security of I&C systems and components.

4.66. Auditable processes and procedures should be in place to confirm that I&C systems, subsystems and components that are important for maintaining computer security continue to perform their security functions throughout their operational lives.

4.67. Provision should be made for security examinations of I&C systems (e.g. inspections for configuration) throughout the entire I&C system life cycle to demonstrate that security procedures have been followed and the required standard of workmanship has been achieved (e.g. no extra components have been added).

4.68. Independent[19] inspections should be conducted to check that computer security processes and procedures are carried out as described by the operator's quality assurance plan.

4.69. Detailed records of life cycle activities should be produced and retained in such a way as to allow review of these records and comparison with computer security requirements at any time. These records should include all computer security incidents and the response or contingency actions taken following the incidents.

4.70. Authorized individuals having privileged logical or physical access to I&C systems should be subject to trustworthiness evaluation, computer security training and behavioural observation consistent with the facility insider mitigation programme or equivalent (see Ref. [5]).

Computer security reviews and audits

4.71. The guidance contained within paras 4.72–4.77 applies to all organizations that perform one or more life cycle activities relevant to I&C systems to which a graded approach to computer security is applied in accordance with its assigned security level.

[19] 'Independent' means the inspection is performed by an individual or organization that is different from the party under review.

4.72. Computer security reviews and audits of I&C systems and associated activities should be performed on a regular basis to verify compliance with regulations, computer security policy and good practices for I&C system security.

4.73. Computer security reviews of I&C systems should be independent and performed by qualified internal and/or external reviewers.

4.74. Policies and procedures including roles and responsibilities for conducting such reviews should be defined and documented.

4.75. Computer security reviews of I&C systems should verify the implementation and effectiveness of their associated computer security measures.

4.76. Intrusive assessment testing should not be conducted against operational I&C systems. Intrusive assessment testing involves attempting to exploit a vulnerability (e.g. as in penetration testing) that may change either the operating conditions or the configuration of the I&C system outside its design basis. The operator should consider using controlled methods to perform payload-free tests while the facility is in a condition in which URC are prevented; for example, if the facility is in a shutdown or defuelled state. Facility policies and procedures should address the conduct and performance of these tests. These tests should be designed specifically for each system. Intrusive assessment tests should involve the computer security incident response team.

4.77. Records of computer security reviews and associated analysis data should be archived, maintained and protected throughout the entire life cycle of the I&C system.

Configuration management for computer security

4.78. The guidance provided in paras 4.79–4.87 applies to all I&C systems, subsystems and components having an assigned security level.

4.79. Software configuration control activities may assist in preventing and detecting computer security incidents, although the primary purpose of these activities is not to address specific nuclear security objectives. The computer security benefit gained by performing these activities should be analysed and confirmed prior to taking credit for such benefits. For example, a computer security incident could be detected through these activities but the timing of the initiation of the response to a detected incident would likely be insufficient to protect the system, compared with the timing of a response in a computer security

system that incorporates layered computer security measures with automatic response elements.

4.80. Unmanaged changes to software configuration are a significant source of new vulnerabilities and unpredictable situations. Typically, the configuration management system used for I&C systems is a generic system that also manages many other types of system. Nevertheless, the configuration management system should be used in a way that incorporates knowledge of both the I&C systems and their computer security measures.

4.81. Configuration management depends upon change management, which is a process that seeks to ensure that approved design processes and appropriate verification and validation are used when a computer system is changed. It also includes control of documents that support these processes. Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1 [16], para. 5.26, states that:

> "The types of document to be controlled should include, but should not be limited to: documents that define the management system; safety requirements; work instructions; assessment reports; drawings; data files; specifications; computer codes; purchase orders and related documents; and supplier documents."

4.82. Computer security measures for I&C systems using the facility's configuration management process should be consistent with the facility configuration control requirements applicable to the associated I&C system.

4.83. Configuration management should be ensured for computer security measures associated with I&C systems throughout the life cycle of I&C systems.

4.84. Configuration management for computer security measures associated with I&C systems should include techniques and procedures for analysing the effects of configuration changes, approving configuration changes, ensuring software versions are combined correctly, releasing design documents and software for use, and establishing and maintaining a chronological record of configuration changes (e.g. of which versions of software tools are used at a particular point in design).

4.85. Identification, storage and issue for use of I&C components and associated technical control measures should be protected from compromise.

4.86. Configuration documents for computer security measures associated with I&C systems should be maintained and protected from unauthorized access or compromise. This information should be classified as sensitive information and access to this information should be limited to a need-to-know basis.

4.87. Technical control measures to limit access and ensure integrity should be applied to software and configuration files during development, transport, installation and operations.

Verification and validation

4.88. The guidance provided in paras 4.89–4.94 applies to all I&C systems, subsystems and components having an assigned security level.

4.89. Each phase of the I&C system development process uses information from earlier phases and provides results to be used as the input for later phases. Verification should be performed after concluding a phase of the development process and before progressing to the next phase of the development process and should include assessment of the computer security measures.

4.90. Prior to the completion of the commissioning phase of the I&C system development process, the validation of the I&C system should be performed with the aim of ensuring that the computer security requirements are met while also continuing to comply with the functional, performance and interface requirements. This is intended to provide a high degree of assurance that the system will perform its function as required. The validation of computer security measures should be carried out by teams, individuals or groups that are independent of the designers and developers. The extent of the independent validation and degree of independence, for example, should be suitable for the security level assigned to the system or component involved whether the validation is performed by vendor, contractor or supplier staff or performed by external experts independent of the vendor, contractor or supplier.

4.91. Verification and validation activities should demonstrate that the I&C system meets the relevant computer security requirements.

4.92. The operator should verify and validate each technical control measure to confirm that it provides the I&C system with the intended protection and does not reduce the reliability of its safety or security functions.

4.93. Computer security measures should be verified and validated using a level of effort commensurate with the security level assigned to the associated I&C system or using a level of effort commensurate with the safety classification of the I&C system, whichever is more stringent.

4.94. Verification and validation activities should identify, record and document detected vulnerabilities, weaknesses or other anomalies and their resolution. Given the size and complexity of most modern computer based systems it may be difficult to ensure that the results of these activities will be comprehensive or successful in uncovering all anomalies. For example, automated tools to perform software code reviews depend on the platform and programming language used, and may only be partially successful. Additionally, it may not be possible to scan certain operating systems, machine code and callable library functions, which may contain vulnerabilities that could be exploited.

Computer security assessments

4.95. The guidance provided in paras 4.96–4.100 applies to all I&C systems, subsystems and components having an assigned security level.

4.96. Computer security assessments should be performed for each phase of the I&C system life cycle to identify potential threats as well as vulnerabilities and weaknesses.

4.97. Public or open source information as well as vendor, contractor or supplier and expert sources should be monitored to promptly identify changes in the threat landscape and new vulnerabilities.

4.98. New or changed threats and vulnerabilities should be assessed to evaluate their potential impact on I&C system computer security. Corrective action (e.g. amended security features) should be taken if these changes could result in potential security violations or unacceptable risks for the facility.

4.99. Each organization that is responsible for developing, deploying, operating, maintaining or decommissioning I&C systems or components should perform periodic computer security assessments and audits.

4.100. The results of the computer security assessments should be used to update the system CSRM.

Documentation

4.101. The guidance provided in paras 4.102–4.106 applies to all I&C systems, subsystems and components having an assigned security level.

4.102. Documentation for I&C system computer security helps in avoiding ambiguities and facilitates correct and error-free operation, surveillance, troubleshooting, maintenance, future modification and modernization of the system and training of facility and technical support staff.

4.103. Documentation should be generated to record sufficient information related to the computer security of I&C systems to demonstrate that computer security measures are designed, implemented and maintained in a way that meets the required level of protection consistent with the assigned security level.

4.104. Computer security input documents and output documents should be defined for the activities of each phase of the I&C system life cycle.

4.105. Documentation should ensure the traceability of the computer security requirements across all activities of the I&C system life cycle. The addition, modification and removal of computer security measures for I&C systems should be recorded.

4.106. Documentation should be protected against unauthorized disclosure, tampering and deletion, and destruction commensurate with the assigned security level of the associated I&C system.

Design basis

4.107. The guidance contained within paras 4.108–4.114 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.108. Reference [4], para. 3.11, states that "The design basis identifies functions, conditions and requirements for the overall I&C and each individual I&C system." This information is then used to assign computer security requirements to each I&C system and to supporting security systems. The design basis is also used to establish design, implementation, construction, testing and performance specifications for computer security measures.

4.109. The design basis for the overall I&C architecture and each I&C system should be used to inform the design of computer security measures to be implemented to meet regulatory computer security requirements (including design basis threat or threat assessment). Further guidance on design basis threat (including threat assessments and alternative threat statements) is provided in Ref. [18].

4.110. Computer security design considerations and assumptions for the I&C systems and the supporting security systems should be identified in the design basis.

4.111. The level of protection to be applied to each I&C system should be defined in the design basis, consistent with the assigned security level identified in the facility and system CSRM.

4.112. The design basis should specify requirements for computer security measures, including technical, physical and administrative control measures.

4.113. The design basis should specify safety requirements that allow for effective validation activities, with the aim of preventing computer security measures from adversely affecting the safety performance of I&C systems.

4.114. The design basis should be maintained and periodically updated to reflect changes to regulatory computer security requirements or risks.

Access control

4.115. The guidance contained within paras 4.116–4.120 applies to all I&C systems, subsystems and components to which a graded approach to computer security is applied in accordance with their assigned security level.

4.116. Physical and logical access to I&C systems should be controlled with the aim of preventing unauthorized access. Privileged access to I&C systems should be strictly controlled such that only authorized personnel have access to or are able to make changes to the existing configuration, software and hardware. This access may be restricted according to the work function of the authorized personnel, both in terms of duration and the numbers of systems that are able to be accessed.

4.117. The number of access points to networks and devices should be reduced to as few as possible to minimize the number of potential attack vectors.

4.118. Digital communication should be restricted to authorized uses and monitored for abnormal activity. Appropriate actions should be taken when abnormal activity is detected.

4.119. For I&C systems assigned the most stringent security level, multifactor authentication methods should be considered where such methods are compatible with time dependent interactions between facility personnel and the I&C system.

4.120. Procedures for managing and assigning roles and access rights for system and user accounts should be developed and updated periodically. The procedures should take into account the principle of least privilege. This process may be referenced or integrated into the facility computer security programme and the facility integrated management system.

Protection of the confidentiality of information

4.121. The guidance contained within paras 4.122–4.125 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.122. When insufficient physical protection and computer security measures for protecting the confidentiality of information are applied, it is possible for an unauthorized disclosure of information to occur that could lead to a compromise of the physical protection or computer security of the system or facility. IAEA Nuclear Security Series 23-G [15] states that:

> "Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film, magnetic or optical media, or held in electronic systems."

4.123. Information related to I&C systems should be identified (e.g. associated databases, files and documentation; change components; simulators), and, where appropriate, classified as sensitive information and secured with appropriate measures. References [12, 15] provide additional information on recommendations for protecting sensitive information.

4.124. Computer security measures should be used to protect the confidentiality of information associated with I&C systems, which may include information about the design, manufacturing, installation and operations of I&C systems and associated equipment.

4.125. The operator should apply technical, physical and administrative control measures for the prevention, detection and response to unauthorized disclosure or exfiltration of sensitive information related to I&C systems.

Security monitoring

4.126. The guidance contained within paras 4.127–4.130 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.127. Computer security requirements for the security monitoring of I&C systems should be specified consistent with the systems' assigned security levels.

4.128. Monitoring of I&C systems requiring the highest or a high level of security should employ independence[20] or diversity in the computer security measures deployed to detect compromise or mal-operations. User interfaces for security monitoring, compromise indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring of computer security in all plant states.

4.129. Requirements for monitoring the status of technical or physical control measures should be established to facilitate the taking of any necessary safety and security actions.

4.130. I&C systems and their associated computer security measures should be continuously monitored and logged. Analysis should identify unauthorized access or changes. The integrity of these records should be protected.

Considerations for the overall defensive computer security architecture

4.131. The guidance provided in paras 4.132–4.140 applies to all I&C systems, subsystems and components having an assigned security level.

4.132. The operator should specify an overall defensive architecture for the computer security of I&C systems in which all I&C systems are assigned a security level and protected according to the applicable requirements.

[20] An example of independence is the segregation of monitoring systems from the I&C system, which would allow for the separation of duties.

4.133. Defensive architecture should be used to facilitate and maintain the capability for I&C systems to prevent, detect, delay, mitigate and recover from cyber attacks. Defensive architecture includes, but is not limited to, formal logical or physical boundaries such as the security zones in which defensive measures are deployed.[21] When implementing such architecture, operators should consider limiting the dynamic elements of both the composite networks and their individual systems to increase the determinacy of their behaviour. This increase in determinacy may assist the implementation of effective computer security measures for the detection of potential computer security incidents.

4.134. Computer security boundaries should be implemented between I&C systems, subsystems and components that have different security levels and are protected using different computer security measures. Computer security boundaries are the logical and physical boundaries of a system or a set of systems at the same security level, and may therefore be secured by the application of common defensive measures (e.g. computer security zones).

4.135. Data flow should be controlled between security zones assigned to different security levels and between individual I&C systems on the same security level based on a risk informed approach to ensure that the defensive architecture remains effective.

4.136. I&C systems requiring the highest level of security (i.e. the most stringent security level) should only be connected to systems requiring lower levels of security (i.e. weaker security levels) via fail-secure, deterministic, unidirectional data communication pathways.[22] The direction of these data pathways should be limited to the transmission of data from devices requiring the most stringent security level to the devices assigned to weaker security levels. 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.[23]

4.137. Digital devices or communications networks used for monitoring, maintenance and recovery activities should not bypass technical control measures used to protect communication pathways between devices having different security levels.

---

[21] An example of such a defensive architecture is one that includes a series of concentric defensive levels of increasing security and considers both hardware and software components.

[22] Remote access to the systems in the most stringent security level is unable to be implemented owing to the unidirectional limitation of outbound traffic from the I&C system.

[23] Some Member States feel strongly that exceptions should not be allowed in any case.

4.138. Systems assigned to the most stringent security level should be placed within the most secure zone boundaries. Wireless communications functions are problematic when implemented in I&C systems that are assigned to the most stringent security level as it is difficult to provide a secure boundary for such communications.

4.139. Data communications between facility I&C systems and the emergency centre (either on-site or off-site) should be protected and controlled by computer security measures.

4.140. Technical control measures implemented within each security zone or at the security zone boundary should employ different technologies from those implemented in adjacent security levels or boundaries. This will ensure the use of diverse technologies to protect the I&C systems.

Defence in depth against compromise

4.141. The guidance contained within paras 4.142–4.151 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.142. Defence in depth against compromise involves providing multiple defensive layers of computer security measures that must fail or be bypassed for a cyber attack to progress and affect an I&C system. Therefore, defence in depth is achieved not only by implementing multiple defensive layers (e.g. security zones within a defensive computer security architecture), but also by instituting and maintaining a robust programme of computer security measures that assess, prevent, detect, protect from, respond to, mitigate and recover from an attack on an I&C system. For example, if a failure in prevention were to occur (e.g. a violation of policy) or if protection mechanisms were to be bypassed (e.g. by a new virus that is not yet identified as a cyber attack), other mechanisms would still be in place to detect and respond to an unauthorized alteration in an affected I&C system.

4.143. No single failure within or across the defensive layers should render the overall computer security of the I&C systems invalid or ineffective. For example, the exploitation of a critical vulnerability within a common network protection device used at two logically linked but physically separated locations would have the potential to facilitate an attack bypassing multiple layers of computer security measures.

4.144. I&C systems and related digital components should be designed and operated in accordance with the concept of defence in depth against compromise.

4.145. Personnel should be assigned to perform security actions that complement technical control measures. The balance between human activity and technical control measures should be analysed and justified.

4.146. A systematic approach should be taken to identify and document human actions that can adversely affect I&C security in each phase of the I&C system life cycle.

4.147. A risk informed approach should be used to determine the appropriate provision of security for I&C systems, including the implementation of technical control measures and defence in depth against compromise. The layers of computer security measures used to implement defence in depth against compromise should be implemented in accordance with the facility and system CSRM.

4.148. Each defensive layer should be protected from cyber attacks originating in adjacent layers.

4.149. Protection mechanisms used for isolation between defensive layers should mitigate common cause failures.

4.150. Defensive layers and associated countermeasures should prevent or delay the advancement of attacks.

4.151. Defensive layers should be effective throughout the I&C system life cycle and should be considered in the design, configuration, modification and parameter assignment of the components of the system.

SPECIFIC LIFE CYCLE ACTIVITIES

Computer security requirements specification

4.152. The computer security requirements for the defensive architecture and for individual I&C systems and components should be established and documented. These requirements for the defensive architecture should be derived from the I&C design basis.

4.153. The computer security requirements for I&C systems, subsystems and components should consider functional and performance requirements, system configuration, qualification, human factors engineering, data definitions and communication, documentation, installation and commissioning, operation, and maintenance.

4.154. The development of computer security requirements for I&C systems should take into account the facility and system CSRM. The computer security requirements should be reviewed and updated based upon changes to the outputs for the facility and system CSRM.

4.155. The combination of the computer security requirements for defensive architecture and individual I&C systems should fulfil the design basis established for the overall I&C architecture.

Selection of predeveloped items

4.156. The guidance contained within paras 4.157–4.164 applies to all I&C systems, subsystems and components to which a graded approach may be applied.

4.157. Predeveloped items might include electronic devices, predeveloped software (PDS), commercial off-the-shelf (COTS) products, digital devices composed of hardware and software (including firmware), hardware devices configured using hardware description language or predeveloped functional blocks.

4.158. Predeveloped items could include predeveloped hardware and software (including firmware) from organizations that do not have an appropriate computer security programme or who are not willing to share the details of their computer security programme. In such cases, it is necessary to analyse the computer security characteristics of the items and to justify their use within either I&C systems or auxiliary systems.

4.159. PDS and COTS products are likely to be proprietary and generally their source code is unavailable for extensive verification activities. Consequently, it is likely that there is no reliable method for the operator to comprehensively determine security vulnerabilities for these products. In such cases, compensatory computer security measures will be needed unless these products are modified by the application developer.

4.160. Computer security measures should be applied to ensure that PDS and COTS product features are not able to cause the I&C systems to fail to meet their computer security requirements. For example, guidance may be available to reduce the amount of code running, to prevent entry points from being available to unauthorized users and to eliminate unnecessary functionality, thereby minimizing the attack surface (i.e. system hardening). However, only limited protection can be obtained by the application of these computer security measures, and the operator should apply additional compensatory computer security measures.

4.161. Predeveloped components or software should be selected and configured using a security qualification process commensurate with the security level of the I&C system.

4.162. The use of PDS and COTS products should be verified to ensure these products meet I&C system computer security requirements.

4.163. The operator should determine the documentation required to qualify PDS products. Technical control measures that cannot be verified as effective should not be relied upon.

4.164. Unneeded functions or services in a configurable PDS or COTS product should be removed.

I&C system design and implementation

4.165. The guidance contained within paras 4.166–4.174 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.166. In the I&C system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures and related machine executable representations. Implementation addresses hardware configuration and set-up, software coding and testing, and communication configuration and set-up (including, where decided, the incorporation of reused software and COTS products).

4.167. In the design and implementation phases of the I&C system life cycle, computer security requirements for the I&C systems should be identified and their implementation verified.

4.168. Requirements identified in the I&C system specification should be translated into specific design items in the system design description. These specific design items should include provisions to be implemented within the I&C system design or by computer security measures implemented externally to the I&C system.

4.169. The I&C system computer security design items should address control over physical and logical access to the system functions, use of I&C system services and data communication with other systems.

4.170. Physical and logical access to an I&C system should be controlled based on the assigned security level of the I&C system. For example, systems assigned to the most stringent security level will need to have computer security requirements for multifactor access control, such as access control requiring a combination of knowledge (e.g. password), property (e.g. key, smart card) and personal features (e.g. fingerprints).

4.171. I&C systems should be designed to include features to provide resistance to or protection against compromise.

4.172. Design measures should provide adequate confidence that the security of a system assigned to a given security level is not reduced by connections to systems assigned to weaker security levels.

4.173. Appropriate combinations of administrative control measures (e.g. a computer security programme) and physical control measures should be designed to reduce the susceptibility of an I&C system to cyber attack.

4.174. I&C system components should be allocated and installed in facility locations that physically secure the equipment and its network communications with other systems, for example, the placing of all data connections for systems and components within secure enclosures.

I&C system integration

4.175. The guidance provided in paras 4.176–4.178 applies to all I&C systems, subsystems and components.

4.176. I&C system integration is the process of combining I&C system hardware and software (including firmware) into a single system. Often, vendors, contractors or suppliers will perform integration testing of each individual system

that they produce as well as a combination of systems within their scope prior to shipping to the facility site. This testing verifies the proper execution of software components and proper interfacing between components within the I&C system.

4.177. During the system integration phase of the I&C system life cycle, the integrated technical control measures should be in place and configured according to specifications prior to testing.

4.178. During integration testing, the vendor, contractor or supplier should confirm that the integrated computer security measures perform as specified and do not adversely affect the I&C systems' ability to perform their essential functions.

System validation

4.179. The guidance provided in paras 4.180–4.185 applies to all I&C systems, subsystems and components having an assigned security level.

4.180. System validation activities normally occur in parallel with other life cycle phases. After system integration has been completed, partial system validation is typically performed, for example, by using simulated inputs. Validation activities usually continue as part of the installation, I&C integration and commissioning phases. Validation is considered complete when a system is turned over for normal facility operations.

4.181. During the validation of each I&C system, subsystem and component, the implementation of computer security requirements and configuration items should be demonstrated. The objective of testing security functions is to ensure that the computer security requirements for the I&C systems are validated by the execution of integration, system and acceptance tests where practical and necessary.

4.182. System validation activities should confirm the effectiveness of the computer security measures and check for potential impacts, direct or indirect, on safety functions.

4.183. Each technical control measure that is implemented in the I&C system should be demonstrated to perform in the intended manner and not to increase the risk of security vulnerabilities or reduce the reliability of safety functions.

4.184. The validation of I&C system computer security measures should include an assessment of system configuration (including all external connectivity), software qualification testing, system qualification testing and system factory acceptance testing. The validation of these computer security measures may be supported by I&C system tests that identify potential vulnerabilities or characterize unexpected behaviours or actions.

4.185. System validation testing should be conducted within a secure environment. For example, testing devices such as simulators or emulators should be secured by computer security measures. The stringency of computer security measures should be commensurate with the security level assigned to the I&C system.

Installation, overall I&C system integration and commissioning

4.186. During installation and commissioning, the operator should perform an acceptance review of the correctness of the physical and technical control measures in the target environment while taking into account the overall I&C system integration[24].

4.187. I&C system installation, overall I&C system integration and commissioning should be conducted in a secure environment. The assignment of a security level to this environment should consider the security level of the system in the target environment and the security level of tools used in installation and commissioning.

4.188. The secure environment should be protected using computer security measures commensurate with the security level assigned to the I&C system and the security processes being undertaken to achieve installation and commissioning. In some cases, compensatory administrative and physical control measures should be provided to control access to the secure environment as well as associated equipment and data sources.

4.189. Equipment used in the secure environment should be verified to confirm that its use does not provide pathways for the introduction of malicious code or data into the environment or I&C system components.

---

[24] In this publication, 'overall I&C system integration' refers to the integration of all I&C systems in a facility, and is distinct from 'I&C system integration', discussed earlier in this publication.

4.190. Computer security measures should be in place to control and monitor the movement of data and digital assets into and out of the secure environment.

Operations and maintenance

4.191. The guidance contained within paras 4.192–4.205 applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.192. Operations and maintenance activities continue throughout the I&C life cycle and have already been discussed in the above sections dealing with process planning and activities common to all life cycle phases. The operating organization should assume full responsibility for computer security for the ongoing performance of operations and maintenance activities when entering the operations and maintenance phase for a system.

4.193. Maintenance activities are activities required by the operator to maintain systems or components in good operating condition. These maintenance activities should be extended to the technical and physical control measures providing computer security to I&C systems and may include:

— Periodic preventive maintenance or testing;
— Actions to detect, preclude or mitigate degradation of components;
— Actions to diagnose, repair, overhaul or replace failed components with identical components.

4.194. Computer security measures should be applied to operations and maintenance activities to ensure components and systems are not compromised.

4.195. The operations phase involves the use of the I&C system by the operator in its intended operational environment. During the operations phase, the operator should:

— Check that the I&C system security is intact through techniques such as periodic testing and monitoring, review of system logs and real time monitoring, where possible;
— Evaluate the impact of I&C system changes in the operating environment on I&C system security;
— Assess the effect on I&C system security of any proposed changes;
— Evaluate operating procedures for compliance with the intended use;
— Analyse security risks affecting the operator and the system;

— Evaluate new security constraints in the system;
— Evaluate operating procedures for correctness and usability;
— Perform periodic computer system security self-assessments and audits, which are key components of a good security programme;
— Assess the available incident reports about new threats and vulnerabilities.

4.196. Operations and maintenance activities should be analysed to ensure that computer security measures are implemented to prevent the introduction of malicious software to the I&C system.

4.197. Maintenance activities should conform to existing I&C system computer security requirements unless those requirements are to be changed as part of the maintenance activity. In some cases, computer security measures may need to be temporarily removed or disabled to permit execution of the required maintenance tasks. During the period for which the computer security measures are unavailable, the system is at greater risk and compensatory measures should be implemented.

4.198. Calibration, testing and maintenance activities might involve the use of removable media and mobile devices that are temporarily connected to digital I&C systems and components. Computer security measures for these activities should consider:

— The implementation of effective administrative and technical control measures in the safe and secure handling of the digital devices;
— The verification of the integrity of all control set points with the aim to prevent and protect them from undesired changes;
— The use of qualified personnel (including third parties) that have received training in the performance of these activities based on computer security requirements.

4.199. Interfaces should be disabled or access restricted when not required or not in use (e.g. connection of maintenance and development computers).

4.200. Computer security measures should be in place to prevent unnecessary or unauthorized access.

4.201. Monitoring processes or applications should be in place to verify the current software configuration against known configurations.

4.202. Remote access should be restricted to the greatest extent possible. When remote access is needed, the risk of such connections should be considered, and additional computer security measures need to be implemented. Such connectivity should be maintained for only as long as needed for its specific purpose.

4.203. Operation and maintenance activities should be carefully controlled through formal work order processes and maintenance procedures. For example, checks and balances, such as the two person rule, should be considered for tasks such as performing configuration changes on operational I&C systems.

4.204. Operation activities should not require changes to the I&C system computer security measures.

4.205. System operational and maintenance tools that may be used to compromise the I&C system should be protected commensurate with the security level of the associated I&C system. For example, tools used on a system assigned to a more stringent security level should not be used on a system assigned to a weaker security level.

Modification of I&C systems

4.206. The application of computer security measures to legacy I&C systems at an existing nuclear facility is not always straightforward. For example, the following difficulties may arise:

— Alteration of the legacy I&C architecture may not be possible without affecting the deterministic behaviour of the legacy I&C systems.
— Existing technologies used for program or data storage, interfaces, or communication may not support modification.
— Existing facility structures and layout may not allow for sufficient physical protection measures.
— Contemporary technical control measures that provide security monitoring functions may not be compatible with the technologies implemented within legacy I&C systems.

4.207. During the modernization of a nuclear facility that involves the replacement of legacy I&C systems with modern I&C systems, the operator should consider the possibility that legacy interfaces with the original facility systems and other systems may need to be maintained and that new vulnerabilities and weaknesses may be introduced owing to the new technology or design.

4.208. Modifications of I&C systems change the system or its documentation. These changes may be categorized as follows:

— Changes or enhancements (corrective or adaptive);
— Migration (i.e. the movement of a system to a new operational environment);
— Replacement (i.e. the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system).

4.209. I&C system modifications may be derived from requirements or specified to correct errors (corrective), to adapt to a changed operating environment (adaptive), or to respond to additional operator requests or enhancements.

4.210. When modifications to an I&C system are made, an assessment of the security of the modified I&C system should be included, for example, by updating the system CSRM.

4.211. Computer security should be considered as part of the change management process. This includes changes to software and hardware for I&C systems.

4.212. To ensure that vulnerabilities have not been introduced into the facility environment by modifications, the operator should assess proposed I&C system changes including their impact on the computer security programme and existing I&C system security, evaluate anomalies that are discovered during operation, assess migration needs and assess modifications made, including validation and verification activities.

4.213. Computer security measures should be assessed as described in paras 4.206–4.212 above, and should be revised to reflect computer security requirements derived from the modification process, as appropriate.

4.214. During modification, existing I&C system computer security requirements should remain in force unless those requirements are to be changed as part of the modification activity.

4.215. Configuration management for computer security measures should be in place to prevent the introduction of unauthorized software to I&C systems.

4.216. When migrating systems, the operator should verify that the migrated systems meet the computer security requirements for the I&C system.

4.217. Artefacts from development, installation and testing should be removed from the system and its configuration files prior to placing in service for operation.

4.218. Modifications to I&C systems should be treated as development processes and should be verified and validated.

4.219. All modifications to the I&C system and its components, including software, hardware and system configurations, should account for potential security vulnerabilities and threats that may occur not only during the execution of these activities but also as a result of the modifications.

4.220. Many digital assets and associated components, including removable storage media, have the ability to retain digital data when removed from a system. This digital data may include preprogrammed logic or residual system data such as sensor readings, control signals, analytical data and network traffic. These data may be extractable from the discarded components.

4.221. Administrative and technical control measures should be in place to ensure that remnant data on discarded components cannot be used to support the development of a computer exploit. The components should be destroyed or the data should be securely removed, unless residual data on components to be discarded have been evaluated to show that the data do not pose a risk of security compromise.

4.222. For modifications involving the replacement of I&C systems, the operator should conduct activities such as data cleansing, disk destruction or complete overwrite to ensure data cannot be recovered from the replaced I&C system upon removal from service.

DECOMMISSIONING

4.223. In the decommissioning phase, before nuclear materials, other radioactive material and sensitive information assets have been removed from the facility, the operator should assess the effect of replacing or removing the existing I&C system security functions from the operating environment.

4.224. The operator should include in the scope of this assessment the effect on safety and non-safety system interfaces of removing the system security functions.

4.225. The operator should document the methods by which a change in the I&C system security functions will be mitigated (e.g. replacement of the security functions, isolation from other safety systems and operator interactions or decommissioning of the I&C system interfacing functions).

4.226. Until decommissioning of a facility has been completed, the security procedures should retain elements that ensure the cleansing of hardware and data.

REFERENCES

[1] ALBRIGHT, D., BRANNAN, P., WALROND, C., Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report (2011), http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8

[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, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

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

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants - Instrumentation and Control Systems - Requirements for Security Programmes for Computer-based Systems, IEC 62645:2014, IEC, Geneva (2014).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series 27-G, IAEA, Vienna (2018).

[12] INTERNATIONAL STANDARDS ORGANIZATION, Information Technology – Security Techniques – Information Security Risk Management, ISO/IEC:27005:2011, ISO, Geneva (2011).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

IAEA
International Atomic Energy Agency

No. 25

ORDERING LOCALLY

In the following countries, 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.

CANADA

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.
Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

FRANCE

Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: www.libreriaaeiou.eu

JAPAN

Maruzen-Yushodo Co., Ltd
10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.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 2600 29302 or +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

18-03271

COMPUTER SECURITY AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 17
STI/PUB/1527 (69 pp.; 2011)
ISBN 978–92–0–120110–2 Price: € 33.00

SECURITY OF NUCLEAR INFORMATION
IAEA Nuclear Security Series No. 23-G
STI/PUB/1677 (54 pp.; 2015)
ISBN 978–92–0–110614–8 Price: € 30.00

INSTRUMENTATION AND CONTROL SYSTEMS AND SOFTWARE IMPORTANT TO SAFETY FOR RESEARCH REACTORS
IAEA Safety Standards Series No. SSG-37
STI/PUB/1692 (75 pp.; 2015)
ISBN 978–92–0–102615–6 Price: € 41.00

DESIGN OF INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. SSG-39
STI/PUB/1694 (161 pp.; 2016)
ISBN 978–92–0–102815–0 Price: € 54.00

Computer security represents a challenging area that faces increased threat vectors within a dynamic technological environment. Computer security at nuclear facilities is further complicated owing to the integration of instrumentation and control (I&C) systems into the computer security management framework. This publication provides guidance addressing the challenge of applying computer security measures to I&C systems at nuclear facilities, including the technical basis and methodologies for the application of computer security measures to I&C systems that provide safety, security or auxiliary functions at nuclear facilities. These measures are intended to protect I&C systems against malicious acts perpetrated by individuals or organizations. This publication also addresses the application of such measures to the development, simulation and maintenance environments of these systems.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–103117–4
ISSN 1816–9317