NUCLEAR SECURITY SERIES NO. XX

NST036

DRAFT, November 2014

STEP 8: Submission to MS for comment

COMPUTER SECURITY OF INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR FACILITIES

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

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 in 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 country, 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 Agency'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 world-wide.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Digital instrumentation and control (I&C) systems and equipment play an increasing role at nuclear facilities. New nuclear facilities and modern designs proposed for construction rely upon highly integrated digital I&C systems. Modernization of many existing facilities has also introduced digital I&C systems. Cyber-attacks on these systems could have serious effects on the safety and security of nuclear facilities.

1.2. Cyber-attacks[1] on digital I&C systems at nuclear facilities have the potential to contribute to physical damage of equipment (i.e. sabotage) or aid in the theft or diversion of nuclear material. The consequences resulting from a cyber-attack can range from negligible impact to limited impact, such as a temporary loss of process control, to 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.

1.3. Malicious compromise of digital I&C systems has occurred. The need for protection of computer systems is recognized in the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [1], with specific focus on computer based systems used for physical protection, nuclear safety and nuclear material accounting and control (NMAC).

1.4. Historically, computer security was not given significant consideration in the design of I&C systems at nuclear facilities because these systems were considered invulnerable to cyber-attack due to rigid implementation (i.e. hardwired or analogue systems), segregation (i.e. isolated systems) and a general absence of interactive communications, especially with external networks or systems. However, the transition to digital technology has changed the nature of I&C systems at nuclear facilities by enabling interconnection of reprogrammable and functionally distinct I&C systems. Consequently, computer security considerations should be explicitly included in every part of the I&C system life cycle.

1.5. The ubiquity of versatile programmable digital components and devices has resulted in a reduction in the diversity of digital I&C systems. This extends to common elements and approaches (e.g. communication protocols) used across a variety of industrial applications including nuclear. Malicious acts directed against these common I&C technologies in other industries could also affect a nuclear facility.

[1] Cyber-attack is a malicious act by individuals or organizations that targets sensitive information or sensitive information assets with the intent of stealing, altering or destroying a specified target through unauthorized access to a susceptible system.

1.6. Authorized individuals, on-site or at a remote location, who have logical or physical access to digital I&C systems may, as insiders, pose a threat to safety and security of the nuclear facility. These insiders may be facility employees or contractor's or vendor's personnel who can use their authorized access to perform malicious activities on the system for an immediate or delayed effect. The need for protection of computer systems from insider threats is recognized in Ref. [2].

OBJECTIVE

1.7. This publication provides guidance on computer security for digital I&C systems which provide safety or auxiliary functions at nuclear facilities. This guidance includes safety and security considerations which have to be addressed in an integrated manner in order to provide security throughout the life cycle of the I&C system. While the focus of this document is on the secure operation of these systems, application of this guidance may benefit facility safety and operational performance.

SCOPE

1.8. The scope of this publication is the application of computer security measures to I&C systems which provide safety or auxiliary functions at nuclear facilities. These measures are intended to provide protection to I&C systems from malicious acts[2] of individuals and organizations. This publication also considers the application of such measures to the development, simulation and maintenance environments of such systems.

1.9. Computer based systems associated with nuclear material accounting and control (NMAC), physical protection and security monitoring are outside the explicit scope of this document, but much of the guidance provided here may be applied to such systems.

1.10. The guidance given in this publication should be applied to digital I&C systems of new[3] nuclear facilities, new I&C systems at existing facilities, and implemented to the greatest extent possible for legacy I&C systems of existing facilities.

1.11. This publication does not provide comprehensive guidance on the safety considerations for I&C systems. This guidance can be found in Ref. [3].

1.12. This publication is intended for competent authorities including regulatory bodies, as well as nuclear facility engineering and operating organizations, digital I&C vendors, digital I&C designers, research laboratories and other organizations concerned with the safety and security of nuclear facilities.

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

[3] A new facility is a facility which has yet to complete the commissioning stage.

STRUCTURE

1.13. This publication following the Introduction is separated into four sections:

— Section 2 presents an overview of digital 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 nuclear safety with regards to digital I&C systems.

— Section 4 presents computer security guidance to be applied at the various life cycle phases of digital I&C systems, including during the decommissioning of the facility.

— Section 5 presents further considerations regarding auxiliary and environmental systems and protection of non-digital I&C systems.

2. ROLE OF COMPUTER SECURITY IN PROTECTING DIGITAL I&C SYSTEMS

2.1. The I&C systems in nuclear facilities may make use of digital technologies; for example:

— Supervisory control and data acquisition (SCADA) systems;

— Distributed control systems (DCS);

— Centralized digital control systems;

— Control systems composed of programmable logic controllers (PLC);

— Micro-controllers, 'smart' devices; and

— Systems using programmed logic devices (e.g., field programmable gate arrays, complex programmable logic devices and application specific integrated circuits).

2.2. Within the nuclear industry systems using such technologies are commonly referred to as digital I&C systems. Similar systems that control industrial plants are often called industrial control systems (ICS). Unless otherwise specified, in this publication the term I&C will refer to digital I&C systems.

2.3. The objective of I&C system design should be to provide for safe, secure, reliable and deterministic behaviour in both normal operating and abnormal operating conditions[4] of the nuclear facility. Designs meant to enhance safety also provide certain benefits for security. For example, design measures such as deterministic performance, fault avoidance, fault detection and fault tolerance

[4] Abnormal operation is referred to in the IAEA Safety Glossary [4] as a synonym for anticipated operational occurrence. For this publication, the former term is considered more readily understood.

approaches, and extensive independent verification & validation, may provide a certain degree of defence against malicious attempts to alter behaviour of I&C systems and components.

2.4. Nuclear facilities also employ architectural concepts (such as independence, redundancy, safety defence in depth[5] and diversity) that may contribute to computer security by mitigating the effects of intentionally caused or accidental mal-operation. For example, diversity of design or technology may reduce common vulnerabilities among key safety or control systems. Such design measures and architectural features should be assessed to determine the contribution of these features to computer security, since they may reduce or eliminate some of the vulnerabilities and weaknesses in the system.

COMPUTER SECURITY OF DIGITAL I&C SYSTEMS

2.5. Paragraph 2.2 of Ref. [1] states that the State's nuclear security regime should seek to achieve its objective through the following three elements:

— 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.

2.6. An example of a mapping of the nuclear security elements to the computer security domain is as follows:

— Prevention: proactive methods and tools that reduce the likelihood that a harmful activity will occur. For example, legacy I&C Systems relied upon isolation and administrative controls to restrict access and thereby meet security objectives.

— Management including detection, delay and response: reactive methods and tools that increase the likelihood that a harmful activity will be detected and halted at an early stage. For example, inspection of system event log files may be able to detect precursor events to allow the operator to respond by initiating protective actions prior to the commencement of a harmful activity that adversely affects the safety or security of the facility; and

— Mitigation including recovery: reactive methods and tools that reduce the impact of a harmful activity as much as possible. For example, when an I&C system is discovered to be infected with malware and the response element has neutralized its propagation via any existing or new

[5] The term "safety defence in depth" is used in this publication to refer to defence in depth as defined in the IAEA Safety Glossary [4], to distinguish this from the application of the similar, but security-focused concept of defence in depth (as defined in the Nuclear Security Fundamentals [5]) in implementing computer security measures, described in Section 4.

infection route, then the mitigating actions would be: to determine whether additional compensatory controls (e.g. updated anti-virus signatures) are needed to prevent re-infection; to conduct a system rebuild; and system restoration (after performing detailed event analysis and from known good backups).

2.7. Protection of I&C systems against compromise was often based upon the presumption that a single preventive measure was sufficient, such as the isolation of these systems from other network environments. This presumption was exacerbated by insufficient application of the other elements such that failure of this single security measure could allow for the compromise of the protected system.

2.8. Significant efforts have been devoted to the general issue of computer security, resulting in multiple approaches, methods, techniques, standards and guidelines. These approaches were mainly developed for, and applied to, general information and communications technology (ICT) systems, and are not always directly applicable to I&C systems at nuclear facilities, which have unique computer security requirements.

2.9. Many I&C systems have a lifecycle which lasts for decades with periods during which vendor support may be unavailable or unable to meet the security requirements. This includes support given by the original vendor (e.g. original equipment manufacturer, operating system vendor) and associated third parties. For example, anti-virus programs may not provide sufficient protection against the vulnerabilities and exposures of I&C systems for the entire service lifetime of the system due to loss over time of hardware or software compatibility or signature updates.

2.10. In most applications, I&C systems are real-time systems, the actions of which must be performed within strict time intervals. Examples of such 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 these necessary operational or safety actions. Security of contemporary I&C systems can provide for prevention, detection and response, but care needs to be taken to ensure that the corrective controls implementing a response action do not impede accredited safety functions or place the system outside of its design basis.

2.11. Computer security measures that are retrospectively applied or poorly implemented may introduce additional complexity in the system design which may result in an increased potential for failure. A secure design, developed using a risk-informed approach[6], may be simpler and more robust due to integration of the security features, elimination of unnecessary functionality (e.g. remote access) or by system hardening.

[6] Use of risk-informed approaches is identified as Essential Element 9 in Ref. [5].

COMPUTER SECURITY MEASURES

2.12. Computer security measures are policies, procedures, practices, methods and controls that provide prevention, protection and mitigation against malicious attacks and non-malicious acts that may lead to degraded security or compromise.

2.13. Specific controls that address vulnerabilities in the system or provide protective layers of defence can be assigned to three categories:

— Technical controls: hardware and/or software solutions for the protection, detection and mitigation of and recovery from intrusion or other malicious acts.

— Physical controls: physical barriers for the protection of computer and supporting assets from physical damage and unauthorized physical access. The physical controls include barriers such as locks, physical encasements, tamper seals, isolation rooms, gates and guards.

— Administrative controls: policies, procedures and practices designed to protect computer systems by controlling personnel actions and behaviours. The administrative controls are directive in nature, specifying what employees and third party personnel should and should not do. In the nuclear environment, administrative controls are understood to include operational and management controls.

An integrated security management system consists of elements of all of the above.

2.14. The application of computer security measures should be based on a risk-informed approach that takes into account the threats to the I&C system, the vulnerabilities of the system and the attractiveness of the system to potential adversaries, the operating environment and the potential consequence that could either directly or indirectly result from a compromise of the system.

GRADED APPROACH

2.15. The importance of I&C system functions for both safety and security should be considered when developing a risk-informed graded approach.

2.16. The results of the computer security risk analysis should be used as the basis for the graded approach.

2.17. The use of computer security levels and zones[7] as described in this publication is one approach to implementation of a risk-informed framework for the application of computer security measures that involves the grouping and graded application of protective measures.

[7] An example of a implementation of a graded risk informed approach using security levels and zones is provided in Ref. [6].

SECURITY LEVELS

2.18. Computer security levels[8] are an abstraction that defines the degrees of security protection required by various I&C systems in a facility. Each level will require different sets of protection measures to satisfy the security requirements of that level. The security levels are often predefined based upon an organization's security objectives.

2.19. Security levels and safety classes are distinct but related concepts. The safety classification of an item is based upon the relevance to safety of its function as well as effects of its failure. The security level is assigned to an item based upon the effects of its failure or mal-operation, including operation in a way that differs from the item's design or conceivable failure modes. Furthermore, it may be necessary to assume that multiple components can be compromised by a single cyber-attack (e.g. affecting multiple channels of a reactor protective system) or an attack may affect multiple targets and involve multiple attack modes. The results of the facility safety analysis should be used for the evaluation of the potential safety consequences of successful cyber-attacks.

2.20. The subcomponents of systems whose mal-operation can affect safety or accident monitoring functions need to be identified and assigned to security levels according to their significance.

SECURITY ZONES

2.21. The security zone concept involves the logical and physical grouping of assets that share common security requirements. In computer security this concept can be applied on the basis of logical or physical attributes (or both). Grouping of I&C systems into zones can simplify the application and management of computer security measures. It is often the practice that all systems located within a single zone are assigned to the same security level. Ref. [6] provides an example implementation of security zones and security levels.

2.22. Security zones could be implemented based on the following considerations:

— Each zone comprises systems that have the same or comparable importance for the security and safety of the facility;

— Systems belonging to single zone have similar demands for protective measures;

— Systems belonging to the same zone could form a trusted area for internal communications between those systems;

— Zone boundaries may need implementation of technical controls that restrict data flow and communication between systems located within different zones or assigned to different security levels;

[8] References to security levels throughout the publication indicate computer security levels.

— Zones can be partitioned into sub-zones to improve the configuration.

2.23. An implementation of security zones for I&C systems may result in certain components being assigned to security levels that are higher than their inherent level. For example, a communication device, having no importance for safety or security, but which provides communication between two reactor protective system (RPS) components may be assigned the same level as those RPS components, based upon its location within the RPS security zone. This is a result of the potential for malicious use of that device to compromise the RPS components which are highly important for safety. However, the use of the RPS zone allows for the creation of an internal trusted zone, thereby ensuring that computer security measures do not have to be implemented between the RPS components and the communication device.

3. RELATIONSHIP BETWEEN COMPUTER SECURITY AND SAFETY

3.1. 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 in a way that security measures do not compromise safety and safety measures do not compromise security [5]. This section discusses how an understanding of facility safety can assist in the development of computer security features for the I&C system, the potential conflicts between safety and security, and considerations for resolving such conflicts. Additional guidance on safety considerations can be found in Ref. [3].

3.2. Adversaries can sabotage a facility through cyber-attack on the facility's I&C systems, with potential consequences for safety and security. 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 and analysed failure states. Malicious actions may affect a single I&C system or multiple I&C systems. Malicious acts might, for example, bypass multiple levels of safety defence in depth or could cause simultaneous failure of multiple levels of defence.

3.3. The five nuclear safety defence in depth levels are detailed in Ref. [7]. These levels may be summarized as:

(1) Prevention of abnormal operation and failures.

(2) Control of abnormal operation and detection of failures.

(3) Control of accidents within the design basis.

(4) Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.

(5) Mitigation of radiological consequences of significant releases of radioactive materials.

3.4. Inadequate or compromised I&C system security may allow for the compromising of the facility's safety. Compromise of I&C systems may allow adversaries to obtain data that may provide critical information needed to plan an attack or to modify data that may facilitate sabotage or theft of nuclear materials. A cyber-attack can cause an initiating event or can undermine the performance of a safety function. Such an attack may also lead to loss of system availability.

3.5. Computer security measures for I&C systems therefore need to address both cyber-attacks that directly cause sabotage and those that collect information that can facilitate sabotage of the nuclear facility or theft of nuclear material.

FACILITY LEVEL COMPUTER SECURITY RISK ASSESSMENT

3.6. The guidance in this section applies to all I&C systems.

3.7. Implementation of computer security in I&C systems needs a facility level computer security risk assessment to determine the effects that may result from cyber-attacks that successfully exploit vulnerabilities in the system.

3.8. This facility computer security risk assessment should include an identification of the facility I&C systems (including supporting and complementary systems) that, if compromised, could have an adverse effect on safety, security of nuclear material or accident mitigation. The identification process may use as an input the facility safety analysis used to define security requirements, but the safety analysis is not sufficient as it does not account for all mal-operations, notably those caused by malicious actions. Cyber-attacks may potentially cause systems important to safety to operate in ways that compromise facility safety. Cyber-attacks might place the facility in conditions that are not considered by the safety analysis.

3.9. The computer security risk assessment should identify the I&C systems whose compromise by cyber-attack could lead to potential consequences. When analysing the consequences of an attack on an I&C system, the possibility that it will be involved in an attack affecting multiple I&C systems (e.g. misuse of auxiliary I&C systems to propagate the attack) or a multi-mode attack (e.g. combined cyber and physical attack) should be considered. This analysis can then be used to assign the appropriate security levels to I&C systems and components based upon the potential consequences of their failure or mal-operation. It may also be useful to associate security levels with a hierarchical list of potential safety or security consequences.

3.10. For safety, an example of such a hierarchy, from the lowest to highest consequence is as follows:

— Normal operation not impeded: A cyber-attack on I&C systems will not cause facility operation outside of limits and conditions specified for normal operation.

— Normal operation impeded: A cyber-attack on I&C systems may cause facility operation outside of limits and conditions specified for normal operation, but will not create an anticipated operational occurrence.

— Anticipated operational occurrence (AOO): A cyber-attack on I&C systems may cause an anticipated operational occurrence, but will not disable the design provisions that have been provided to prevent the AOO from leading to accident conditions.

— Design basis accident (DBA): A cyber-attack on I&C systems may cause accident conditions against which a facility is designed according to established design criteria, and for which the damage to the nuclear material and the release of radioactive material are kept within authorized limits.

— Beyond design basis accidents (including severe accident and other design extension conditions for a nuclear power plant): A cyber-attack on I&C systems may cause accident conditions which may incur damage to the nuclear facility or the release of radioactive material exceeding authorized limits.

3.11. For sabotage, an example of such a hierarchy, from the lowest to highest consequence is as follows:

— Radiological consequence below the Unacceptable Radiological Consequence (URC) threshold. Targets posing these low consequences may need a correspondingly low level of protection.

— Unacceptable radiological consequences. The definition of URC may be based on quantitative or qualitative criteria. Types of URC criteria may include release-based (e.g., release exceeding some identified amount), dose-based (e.g., release exceeding some radiation dose to an individual located at some point, generally off-site) and design limits (e.g., sabotage that may result in significant core damage in a reactor). Therefore the State should also define the high radiological consequence (HRC) level; accordingly, URC can be graded into three categories from lowest to highest:

  - 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.

  - High radiological consequences – Consequence Level A: Sabotage that could give rise to severe deterministic health effects off-site.

3.12. For unauthorized removal of nuclear material, Table I of Ref. [1] provides the criteria for the categorization of nuclear material and further identifies requirements for physical protection based on this categorization. While outside the scope of this publication, I&C systems fulfilling physical

protection or NMAC functions may be affected by cyber-attacks on other I&C systems. These attacks may place the facility in a condition that has not been considered in the site security plan and therefore may be an element of a blended attack which has the objective of unauthorized removal of nuclear material. The potential consequences of attacks that may lead to these conditions should be graded on the basis of the category of material that would be subject to unauthorized removal.

3.13. A complete hierarchy for all safety and security consequences has yet to be determined: however, it is recommended that the facility operator or State develop such a hierarchy.

3.14. Other consequences, such as a loss of reputation, may be considered when evaluating the combined impact of a cyber-attack on facility I&C systems. A listing of possible such impacts can be found in ISO 27005:2011.

3.15. Adversary tactics, techniques and procedures are constantly changing and all nuclear facilities should foster a nuclear security culture[9] that continually reviews computer security risk and allows for dynamic changes to the facility I&C computer security programme.

3.16. As existing I&C systems are enhanced with digital equipment, system configuration and activities should be analysed to identify changes to logical and physical pathways that may provide opportunities that an adversary can exploit. Activities that may be analysed include temporary maintenance activities, procurement processes, vendor support, communication with field devices and manual software updates.

3.17. The computer security risk assessment is an iterative process that involves, for example: an initial analysis; implementation of controls; periodic review; and updated analysis. There should be a defined acceptance process to review and verify the results of new or updated analyses.

3.18. For new facilities, the computer security risk assessment needs to be performed as part of the design process and accepted before completion of the initial commissioning phase.

3.19. For existing facilities, inputs to the new or updated computer security risk assessment may include the following:

— Safety analysis;

— Details of safety and process architecture; and

— Previously accepted facility computer security risk assessments.

I&C SYSTEM SECURITY RISK ASSESSMENT

3.20. The guidance in this section applies to all I&C systems.

[9] Nuclear security culture is further explained in Ref. [8].

3.21. The I&C system security risk assessment should use as an input the safety hazard analysis to determine the security risk posed by cyber-attacks on individual or multiple I&C systems, subsystems or components. The security risk should be analysed and documented.

3.22. There should be assigned roles and responsibilities throughout the I&C system life cycle for the assessment and management of the I&C system security risks.

3.23. An inventory of I&C system components should be kept updated and maintained during the life cycle of the system. This inventory should be used in the I&C system security risk assessment.

3.24. I&C system components should be assessed and assigned to the appropriate security level based upon the security risk assessment. For these components, the safety and security consequences that could result from mal-operation or compromise should be identified.

3.25. Cyber-attack should be considered as a threat that may occur at any point during the I&C system life cycle.

3.26. Attacks may affect an individual system or multiple systems and could be used in combination with other forms of malicious acts causing physical damage.

3.27. Malicious actions that could change process signals, equipment configuration data or software should be considered in the I&C system security risk assessment.

3.28. Any means of injecting malicious code or data into the I&C system should be considered in the I&C system security risk assessment. For example, malicious code could be injected via communication connections, supplied products and services and/or portable devices that are temporarily connected to target equipment.

3.29. The I&C system security risk assessment is an iterative process that involves, for example: an initial analysis, implementation of controls, periodic review and updated analysis. The I&C system security risk assessment should be considered for review when the following occurs:

— The facility-level computer security risk assessment or facility safety analysis is revised;

— System modifications are made;

— Relevant security events or incidents occur; or

— New or changes to threats or new vulnerabilities are identified.

3.30. The analysis should identify human actions or omissions that might affect security.

ASSIGNMENT OF COMPUTER SECURITY MEASURES

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

3.32. The I&C system, subsystem or component should be assigned to a security level commensurate with the importance for both safety and security of the functions it provides.

3.33. Application of computer security measures to I&C systems should be determined by their assigned security level or the security level of the security zone in which it resides, whichever is the most stringent.

3.34. Implemented computer security measures should be evaluated to ensure a sufficient level of protection for I&C systems.

3.35. Where I&C system security controls cannot provide a level of protection commensurate with their security level, additional or alternative measures for protection should be considered, e.g. facility level physical protection features, independent electronic functions, system re-design or administrative measures which eliminate the vulnerability or reduce the consequences of mal-operation.

SAFETY–SECURITY INTER-RELATIONSHIP

3.36. Computer security measures, if designed inappropriately, may introduce potential failure modes into the system, increase the potential for a spurious operation and challenge the system's ability to reliably perform its safety function. The function or failure of computer security measures should not degrade the safety functions of I&C systems. For example:

— An inadequate implementation of a virus detection system within the I&C system may increase complexity, may increase system latency, and may be vulnerable to exploitation.

— Conversely, an adequate technical security control that ensures that only authorized software is allowed to run on an I&C system may improve this system's ability to reliably perform its safety function while providing significant security benefits.

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

3.38. The appropriateness of a given control will depend on safety, security and operational considerations, and therefore assigning controls needs expertise and effort from multiple domains. Security controls cannot exist in isolation from safety concerns, and safety features cannot exist in isolation from security concerns. Such constraints may, for example, necessitate that certain security functions (e.g., collection of audit records, generation of security alarms) 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 off line (i.e. not in service) is another manner by which security goals can be met while limiting impact to the operational system.

3.39. Exceptions to the assignment of computer security measures to a given security level may exist, but they should be analysed and justified. Computer security measures may include technical, physical and administrative controls. The full set of measures should work together and prevent or not introduce single points of failure.

3.40. Safety strategy may also have the potential to adversely affect security. For example, design for safety often involves 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, provisions should be taken to ensure that threats arising from cyber-attack do not result in the loss of system diversity or redundancy. Additionally, computer security measures should not introduce new common cause failures between these redundant and diverse systems.

SAFETY CONSIDERATIONS FOR COMPUTER SECURITY MEASURES

3.41. The guidance contained in this section applies to all I&C systems important to safety.

3.42. Computer security measures should be implemented in such a way as to not to adversely impact the essential safety functions and performance of the I&C system.

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

3.44. The failure modes of computer security measures and their impact on I&C system functions should be known, documented and considered in system hazard analyses.

3.45. Computer security measures that protect the human–system interface should be implemented so that they do not adversely affect the operators' ability to maintain the safety of the facility. Adverse impacts that may prevent the operator from actuating a safety function (e.g. manual trip) should also be considered.

3.46. Computer security measures that cannot practically be integrate into an I&C system, should be implemented in devices that are separate from the I&C system. Additional administrative controls may be necessary to use and maintain these separate devices.

3.47. Computer security measures integrated into I&C systems should be developed according to the management systems guidance in Ref. [3] or an equivalent alternative management system and qualified to the same level of qualification as the system in which the controls reside.

[3.48. If there is a conflict between safety and security, then design considerations taken to assure safety should be maintained provided that a solution addressing the security risks is pursued. The acceptance of the absence of a security solution is 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.]

OR (alternative text)

[3.48. Safety and security have to be achieved. The measures to achieve this aim may be altered, but the absence of a security solution should not be accepted.]

3.49. The prime responsibility for design, selection and implementation of security controls needs to be clearly assigned, but meeting the responsibility should be a collaborative effort between personnel performing activities involving I&C system design, maintenance, safety and security domains.

3.50. Design analysis should demonstrate that security controls 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.

3.51. The maintenance of security controls should not adversely affect the availability requirements for operating I&C systems.

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

4.1. The guidance in this section applies to all I&C systems.

4.2. The design of I&C systems for nuclear facilities needs to be controlled by management systems that provide an acceptable level of assurance that all requirements are considered and implemented in all phases of the system life cycle and that these requirements are met in the final design. These requirements apply to I&C systems and computer security activities that are provided to ensure facility safety. Ref. [9] establishes the requirements for management systems of nuclear facilities. Management systems are required to integrate safety, health, environmental, security, quality and economic elements to ensure the protection of people and the environment as they are governed by the IAEA Nuclear Security Fundamentals [5]. Ref. [6] gives further discussion on the overall relationship between management systems and computer security.

4.3. To assure that I&C systems fulfil their requirements, the nuclear facility community as well as other specialized domains such as aerospace, have applied development processes that are commonly represented as life cycle models. Life cycle models describe the activities for the development of electronic systems and the relationships between these activities. Computer security needs to be considered at all phases in the I&C system life cycle.

4.4. Three fundamental levels of life cycle are needed to describe the development of I&C systems:

— An overall I&C architecture life cycle;

— One or more individual I&C system life cycles; and

— One or more individual component life cycles. Component life cycles are typically managed in the framework of a platform development and independent from the overall architecture level and the individual system level life cycles. Component life cycles for I&C systems are typically divided into separate life cycles for the development of hardware and software.

4.5. The definition of life cycle models and the processes associated in each life cycle phase is generally determined by the system developers and operators, but the definition and implementation needs to be a multidisciplinary effort involving many other domains, including computer security. Generally the developers have lead responsibility until the systems are turned over to the operations organization for installation, integration and commissioning. Given that the service life of I&C systems may span several decades, different organizations may play the role of developers or other roles during the life of a system. For example, it is not uncommon for a vendor to do the original development and for the purchaser to develop modifications, 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 throughout the life cycle processes.

4.6. At the earliest opportunity, computer security should be coherently planned for the entire I&C life cycle. This planning should specify the computer security measures to be taken to protect the I&C architecture, I&C systems or components from cyber-attacks that may jeopardize functions important to safety during all phases of the I&C lifecycle. The likelihood 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 potential vulnerabilities and weaknesses in each phase of the I&C system life cycle. 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 the computer security considerations during the I&C life cycle[10]:

— Process planning;

— Design basis;

— Overall I&C architecture and functional allocation;

— Requirements specification;

— Selection of pre-developed items;

— Detailed design and implementation;

[10] Ref. [3] contains a listing of typical I&C life cycle activities.

— System integration;

— System validation;

— Installation, integration and commissioning;

— Operation and maintenance;

— Modification;

— Decommissioning/Retirement;

4.8. 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;

— Security assessment;

— Documentation.

4.9. The remainder of this section is divided into subsections that discuss (1) general computer security guidance that apply to all life cycle phases, and (2) security guidelines that are 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.

4.10. The security requirements and activities for each life cycle phase should be commensurate with the risk and magnitude of the adverse impact resulting from unauthorized and inappropriate access, use, disclosure, disruption or destruction of the digital system. Consideration should also be given to the compromise of any system, support system or information that might adversely affect safety or security.

GENERAL GUIDANCE FOR COMPUTER SECURITY

4.11. The guidance in this section applies to all I&C systems.

4.12. A computer security policy for a nuclear facility specifies the overall computer security goals at the facility. In the overall and system level computer security planning, the objectives are specified in clear, specific and, wherever possible, measurable terms. The high level overall objectives are translated into system-level objectives. Ref. [6] provides technical guidance on computer security at nuclear facilities.

4.13. The computer security policy should include elements to address 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 and contractors 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 will conform with the applicable security policies to ensure the system design products (hardware and software) minimize undocumented code (e.g. back door coding), malicious code (e.g. intrusions, viruses, worms, Trojan horses or bomb codes), and other unwanted, unnecessary or undocumented functions or applications.

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

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

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

I&C SYSTEM ASPECTS OF THE COMPUTER SECURITY POLICY

4.18. The guidance in this section applies to all I&C systems.

4.19. The computer security policy for nuclear facilities should describe the application of a risk-informed graded approach to the implementation of computer security measures for I&C systems in accordance with their importance for safety and security (e.g. security level). Management should set and enforce a clear computer security policy direction in line with nuclear safety and security objectives that addresses security of I&C systems as distinct from other computer systems.

4.20. The computer security policy should include considerations specific to I&C systems, such as:

— Access control (both physical and logical access control, use of least privileges).

— Configuration and asset management (includes password management, patch management, system usage, system hardening, configuration control, as well as restrictions on use of mobile devices and removable media (e.g. USB drives, CD-ROM), wireless devices and networks and remote access).

— Procurement processes.

— Risk and threat management (includes process to gather, analyse, document, share with others having a need to know and act upon information about vulnerabilities (and weaknesses) and threats).

— Incident response and recovery.

— Auditing and assessments.

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

COMPUTER SECURITY PLAN

4.22. The guidance contained within this section applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.23. Each organization that has responsibility for implementing I&C system life cycle activities should have an integrated or separate computer security plan.

4.24. For each I&C system, the computer security plan should define the roles and responsibilities for each phase of the life cycle.

4.25. The computer security plan for I&C systems should require application of defence in depth protective strategies and identify applicable security measures according to the security level.

4.26. Security measures should address the potential for malicious insider activity and manipulation of the I&C system throughout the system life cycle. For example, information addressing potential vulnerabilities in I&C systems should be considered as sensitive information [11] and compartmentalized[12].

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

4.28. The computer security plan should address the confidentiality of computer security measures, including protection of related documentation, consistent with the security level.

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

4.30. The computer security plan for I&C systems should require that periodic computer security reviews and assessments be performed and documented in every life cycle phase.

4.31. The computer security plan should specify the computer security measures that allow for the assurance of a secure development environment in which development activities take place.

[11] Sensitive information means information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise nuclear security.

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

4.32. For legacy I&C systems there may be more reliance on administrative controls and isolation than other contemporary computer systems. The computer security plan should identify and sustain these additional controls that are necessary to ensure I&C system security.

SECURE DEVELOPMENT ENVIRONMENT

4.33. The guidance contained within this section applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.34. I&C development should be conducted in a secure environment. This applies to both internal and external development 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 environment, security level of development tools and, if applicable, the computer security measures implemented at the vendor site.

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

4.36. Physical controls should be provided 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. Security measures should be in place to control the movement of data and devices for all development phases to ensure that malicious code is not introduced into the secure development environment; this should include administrative and technical controls such as usage restrictions and procedures for digital devices. Where practical, the secure development environment should be distinct and both physically and logically separated from the operational and corporate business environments.

4.39. Security measures should protect the integrity of the secure development environment, design inputs and design outputs (e.g. data, configuration files, software updates, software patches) during transfers between the secure development environment and the target environment.

CONTINGENCY PLANS

4.40. The guidance provided in this section applies to all organizations that implement one or more I&C system life cycle activities.

4.41. The facility should develop a computer security incident response plan consisting of procedures that define, identify and respond to possible anomalous and suspicious behaviour on I&C and associated systems.

4.42. Contingency plans and procedures to prevent escalation and progression of anomalous behaviour and to recover from computer security incidents should be prepared and periodically exercised.

4.43. The computer security incident response plan should address information collection and evidence preservation requirements 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 (CSIRT). The CSIRT 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. Backup and restoration copies used in contingency plans and procedures should include software, essential data and configuration files. These materials should be stored in a physical location separate from the source location to guard against common cause failure. Security controls should support the protection of these materials against theft, tampering and deletion or destruction.

I&C VENDORS AND THIRD PARTIES

4.46. The guidance contained within this section applies to vendors or third parties who supply digital equipment, software and services for the nuclear facility to which a graded approach may be applied in accordance with their assigned security level.

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

4.48. Computer security requirements and controls should be met and applied respectively by vendors including support provided on site, at the vendor's workplace and during any transit or storage of purchased goods.

4.49. The vendor should have a computer security management process.

4.50. The applicable requirements for computer security at sites where a vendor performs activities with I&C systems should be clearly and contractually specified based on security level by the operator.

4.51. A process should exist between the facility (i.e. operators) and vendor for either organization to report vulnerabilities and to coordinate response and mitigation efforts.

4.52. The vendor should demonstrate that they have 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 may extend beyond any normal warranty period to support the life cycle of the installed equipment.

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

COMPUTER SECURITY TRAINING

4.54. The guidance provided in this section applies to all organizations that implement one or more I&C system life cycle activities.

4.55. All personnel working with or on I&C systems should receive periodic training on computer security awareness and procedures.

4.56. Individuals who have physical and/or logical access to I&C systems should be trained to support computer security tasks and recognize potential computer security events. These individuals may be informed of the impact when changes are made on either the I&C system or its associated security controls for which they have been provided access.

4.57. Personnel should be qualified to an extent consistent with their overall computer security responsibility. Personnel should receive specialized security training for I&C systems based upon their roles and responsibilities in order to maintain their qualification.

4.58. All personnel working with or on I&C systems should receive periodic training on computer security awareness and procedures.

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

4.60. Engineering, operations and maintenance staff should be trained to maintain both safety and security functions.

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

ACTIVITIES COMMON TO ALL LIFE CYCLE PHASES

4.62. In most cases the Safety Requirements on the management system for safety [9] and the general guidance contained in the associated Safety Guides sufficiently describe the management system activities as they apply 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 to ensure that computer security requirements for I&C systems are properly considered by management systems. This section discusses these cases.

Management systems

4.63. The guidance contained within this section applies to all organizations that implement one or more I&C system lifecycle activities to which a graded approach may be applied in accordance with their assigned security level.

4.64. There are specific requirements for management processes in Ref. [9] paragraphs 5.11–5.29 and these requirements should be consulted when defining the computer security requirements for management systems.

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

4.66. 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.

4.67. Procedures should be in place to confirm that structures, systems and components that are important to computer security will perform their required security functions throughout their operational lives.

4.68. Provision should be made for security examination (e.g. inspections for configuration) throughout the entire life cycle to demonstrate that security procedures have been followed and the required standard of workmanship has been achieved (e.g. no extra components).

4.69. Independent[13] inspections should be conducted to check that computer security processes and procedures are carried out as required within the framework of the nuclear quality assurance plan.

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

4.71. Authorized individuals (i.e. insiders) having privileged logical or physical access to I&C systems should be subject to security screening (i.e. trustworthiness evaluation), cyber security training and behavioural observation consistent with the facility insider mitigation programme or equivalent (see Ref. [2]).

[13] Independence means the activity is performed by an individual or organization that is independent from the party under review.

Computer security reviews and audits

4.72. The guidance contained within this section applies to all organizations that implement one or more I&C system lifecycle activities in which a graded approach is used for implementation of the I&C system.

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

4.74. Security reviews should be independent and performed by qualified internal and external reviewers.

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

4.76. Security reviews of I&C systems should verify the implementation and effectiveness of their associated security controls.

4.77. Intrusive assessment testing should not be conducted against operational I&C systems. Intrusive assessment testing involves attempting to exploit a vulnerability (i.e. penetration testing) that may change either the operating conditions or configuration of the I&C system outside of its design basis.

4.78. Records of security reviews and associated analysis data should be archived, maintained and protected.

Configuration management for computer security

4.79. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.80. Software configuration control activities while not implemented to address a specific nuclear security objective, may provide some coverage of the prevention and detection elements, however the response element to a detected event would be insufficient when compared to a computer security system which incorporates layered security controls which provide all three elements.

4.81. Unmanaged changes are a significant source of new vulnerabilities and unpredictable situations. The configuration management system for I&C systems will generally be a generic system managing many nuclear facility systems. Nevertheless, the configuration management system should reflect a strong understanding of the digital system and computer security items that need to be controlled.

4.82. Configuration management includes change management, which is a process that ensures approved design processes and appropriate verification and validation are used when a computer system is changed. It also includes control of documents14 that support these processes.

4.83. Computer security measures should be managed within the facility's configuration management process consistent with the configuration control requirements of the associated I&C system.

4.84. Configuration management for associated computer security measures should be developed throughout the life cycle of I&C systems.

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

4.86. Identification, storage and issue for use of digital I&C components and associated security controls should be protected from compromise.

4.87. Configuration documents for associated computer security measures should be protected from unauthorized access or compromise and maintained. For example, access to this information could be limited based on a need-to-know basis.

4.88. Access and integrity controls should be applied to software and configuration files during development, transport, installation and operations.

Verification[15] and validation[16]

4.89. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.90. Each phase of an 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 when

[14] GS-R-3 [7] states documents may include: policies; procedures; instructions; specifications and drawings (or representations in other media); training materials; and any other texts that describe processes, specify requirements or establish product specifications.

[15] The IAEA Safety Glossary [6] states that computer system verification is "The process of ensuring that a phase in the system lifecycle meets the requirements imposed on it by the previous phase".

[16] The IAEA Safety Glossary [6] states that 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."

concluding a phase, before progressing to the next phase, and should include assessment of the computer security measures.

4.91. Prior to the completion of commissioning phase of the I&C system development process, validation should be undertaken to ensure that the system security requirements are met without degradation of functional, performance and interface requirements. This provides a high degree of assurance that the system will achieve its intended requirements. Validation of computer security aspects 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 (e.g., performed by vendor staff or performed by external experts independent of the vendor) should be suitable for the security level assigned to the system or component involved.

4.92. Verification and validation should demonstrate that the I&C system meets the specified system security requirements.

4.93. Each system security feature should be verified and validated to confirm that the implemented feature provides the system with its intended protection and does not reduce the reliability of its safety functions.

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

4.95. Verification and validation activities should identify, record and document detected vulnerabilities, weaknesses or other anomalies and their disposition. This may be a difficult task with little assurance that the results will be comprehensive and successful in uncovering all anomalies given the size and complexity of most modern computer systems. For example, automated tools to perform software code reviews are dependent on the platform and programming language, and may only be partially successful. Additionally, it may not be possible to scan operating systems, machine code and callable library functions and these may contain vulnerabilities for exploitation.

Security assessment

4.96. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.97. Security assessments should be performed to identify potential threats as well as vulnerabilities and weaknesses in each phase of the I&C system life cycle.

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

4.99. New or changed threats or vulnerabilities should be assessed to evaluate their potential impact on I&C system security. Corrective action (e.g. amended security features) should be taken, if

changes in the threat landscape or new vulnerabilities create potential security violations or unacceptable risks for the facility.

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

4.101. The results of the security assessments should be used to update the computer security risk assessment.

Documentation

4.102. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.103. Adequate documentation helps in avoiding ambiguities, facilitates correct and error-free operation, surveillance, troubleshooting, maintenance, future modification or modernization of the system, as well as training of facility and technical support staff.

4.104. Documentation should be generated to retain sufficient information of computer security of I&C systems to demonstrate that security controls are designed, implemented and maintained to meet the required level of protection consistent with the assigned security level.

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

4.106. Documentation should ensure traceability of the security control requirements across all activities of each phase of the I&C system life cycle.

4.107. Addition, modification and removal of computer security measures of I&C systems should be recorded.

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

Design basis

4.109. The guidance contained within this section applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.110. The design basis identifies functions, conditions and requirements for the overall I&C architecture and each individual I&C system. This information will then be used to assign security requirements to each I&C system and supporting security systems. Also, the design basis will be used to establish design, implementation, construction, testing and performance requirements.

4.111. The design basis[17] for the overall I&C architecture and each I&C system should identify the security controls to be implemented and meet regulatory requirements.

4.112 The design basis should identify the security design considerations and assumptions for the I&C systems and the supporting security systems.

4.113. The design basis should define the level of protection consistent with the assigned security level of the I&C system as identified in the computer security risk assessment.

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

4.115. The design basis should specify safety requirements that allow for effective validation activities to ensure that computer security measures do not adversely affect the safety performance of I&C systems.

Access control

4.116. The guidance contained within this section applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

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

4.118. The number of access points to networks and devices should be reduced as far as possible to minimize vulnerability.

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

4.120. For I&C systems in the highest security level, multi-factor authentication methods should be considered where such methods are compatible with time-dependent interactions between facility personnel and the I&C system.

[17] Design basis is defined in IAEA Safety Glossary [6] as the range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

Protection of the confidentiality of information

4.121. The guidance contained within this section 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. Insufficient physical and computer protection can result in an unauthorized disclosure of information that may lead to a compromise of physical and computer protection of the system and facility.

4.123. Information related to I&C systems should be identified and classified (e.g. databases, documentation, change components, simulator, etc.) and secured with appropriate measures. Sensitive information is information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise I&C system security. Ref. [10] provides additional information on recommendations for protecting sensitive information.

4.124. Computer security measures should 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. Security controls should be provided to allow for prevention, detection and response to unauthorized disclosure or exfiltration of sensitive information.

Security monitoring

4.126. The guidance contained within this section 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. Requirements for security monitoring of I&C systems should be specified consistent with their assigned security level.

4.128. Monitoring of I&C Systems with a high security level should employ independence or diversity in the detection of suspect compromise or mal-operations[18]. User interfaces for security monitoring, comprise indications, recording instrumentation and alarms should be provided at appropriate locations and should be suitable and sufficient to support effective monitoring of computer security during all facility states.

4.129. Requirements for monitoring of the status of the security controls should be established to facilitate the taking of any necessary safety and security actions.

[18] An example of independence could be the segregation of monitoring systems from the I&C system which would allow for the separation of duties.

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 I&C security architecture

4.131. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

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

4.133. Effective defensive architectures should be used to facilitate and maintain the capability for I&C systems to detect, prevent, delay, mitigate and recover from cyber-attacks. Defensive architectures include, but are not limited to, formal logical or physical boundaries (e.g. zones) or security levels in which defensive measures are deployed.[19]

4.134. Computer security boundaries[20] should be implemented between I&C items that have different security levels and have different computer security measures.

4.135. Data flow should be controlled between systems of 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 in the highest security level (i.e. requiring the greatest degree of security) should only be connected to systems in lower protection categories via fail-secure, deterministic, unidirectional data communication pathways[21]. The direction of these data pathways should be limited to transmission of data from the highest security level to the devices in the lower security levels (i.e. lower levels are not allowed to transmit data to the higher level). 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.

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

[19] 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.

[20] Computer security boundaries are usually defined as the logical and physical boundaries of a system or a set of systems that require a common level of protection and can therefore be secured by the application of common security controls.

[21] For example, remote access to the systems in the highest security level should not be implemented.

4.138. Systems requiring the greatest degree of security should be placed within the most secure boundaries[22].

4.139. Data communications between facility I&C systems and the emergency control centre (either onsite or offsite) should be protected and controlled.

4.140. Technical controls implemented within each security level should employ different technologies from those of the adjacent levels.

Defence in depth against cyber compromise

4.141. The guidance contained within this section 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 cyber compromise involves providing multiple defensive layers 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 security boundaries, but also by instituting and maintaining a robust programme of security controls that assess, prevent, detect, protect, respond, 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), 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 entire security solution invalid or ineffective

4.144. I&C systems and related digital components should be designed and operated such that defence in depth against cyber compromise is achieved by the provision of multiple layers of protection.

4.145. Personnel should be assigned to perform security actions that complement technical security controls. The balance between human activity and technical security controls 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 throughout the life cycle.

4.147. A risk informed approach should be used to determine appropriate provision of security for the I&C system, including security functions and defence-in-depth protection.

[22] For example, I&C systems that are assigned to the highest security level should not use wireless communications as it is difficult to provide a secure boundary for such communications.

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

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

4.150. Defensive layers and associated countermeasures should prevent or delay 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/or parameter assignment of the components of the system.

LIFE CYCLE ACTIVITIES

Computer security requirements specification

4.152. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.153. The security requirements of the overall I&C architecture, individual I&C systems and I&C components should be established and documented.

4.154. Computer security requirements for the overall I&C architecture and each individual I&C system should be derived from the I&C design basis.

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

4.156. Security requirements for I&C systems should be defined by considering the computer security risk assessment.

4.157. The combination of the security requirements of the full set of individual I&C systems should fulfil the security design basis established for the overall I&C.

Selection of pre-developed items

4.158. The guidance contained within this section applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.159. Pre-developed items might be hardware devices, pre-developed software (PDS), commercial off-the-shelf (COTS) devices, digital devices composed of both hardware and software, hardware devices configured with hardware description language (HDL) or pre-developed functional blocks usable in a HDL description.

4.160. In some cases the selected pre-developed items may include pre-developed hardware and software from organizations that do not have an appropriate computer security programme, or who are not willing to share the details of their cyber security programme. In such cases, it is necessary to analyse the cyber security characteristics of this hardware and software and to justify their use within I&C system.

4.161. PDS and COTS systems 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 to comprehensively determine security vulnerabilities for these types of systems. In such cases, compensatory measures will be required unless these systems are modified by the application developer. For PDS and COTS systems, computer security measures should ensure that the system features do not compromise the security requirements of the system. For example, guidance may be available to reduce the amount of code running, reduce entry points available to unauthorized users and to eliminate unnecessary functionality to minimize the attack surface by technical hardening. Only limited protection can be credited from the application of these basic security provisions, and the application of compensatory security measures is recommended.

4.162. Pre-developed components or software should be selected and configured using a security qualification process commensurate with the security level of the I&C system.

4.163. Use of PDS (e.g., reuse software and COTS systems) should meet the security requirements of the I&C system that it is to be installed.

4.164. The facility should determine the documentation required to qualify PDS. Security features that cannot be qualified should not be relied upon.

4.165. If configurable unneeded functions or services in PDS or COTS should be removed.

I&C system design and implementation

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

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

4.168. In the design and implementation phase of the I&C system life cycle, security requirements should be identified and their implementation verified.

4.169. The I&C system security requirements identified in the system requirements specification should be translated into specific design items in the system design description.

4.170. The I&C system security design items should address control over (1) physical and logical access to the system functions, (2) use of I&C system services, and (3) data communication with other systems.

4.171. Physical and logical access control should be based on the assigned security level. For example, systems assigned to the highest security level may have requirements for more stringent access control, such as a combination of knowledge (e.g., password), property (e.g., key, smart-card) or personal features (e.g., fingerprints), rather than just a password.

4.172. Design of I&C systems should contain features that provide resistance to or protection against malware.

4.173. Design measures should be defined to provide adequate confidence that a system assigned to a given security level is not degraded by systems assigned to lower levels.

4.174. Appropriate combinations of programmatic controls and physical security measures should be designed to reduce the susceptibility of an I&C system to cyber-attack.

4.175. I&C system components should be allocated and installed in facility locations that physically secure the equipment and its network communication to other systems[23].

System integration

4.176. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.177. System integration is the process of combining the software and hardware into one system. Often vendors will do integration testing of each individual system that they produce and 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.

4.178. During the system integration phase, the integrated security features should be in place and configured as per specification prior to testing.

4.179. Integration testing should confirm that the integrated security controls perform as required and do not adversely affect the systems' ability to perform their required functions.

[23] For example, placing all data connections for systems and components within enclosures.

System validation

4.180. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

4.181. System validation activities normally occur in parallel with other life cycle phases. Validation activities usually continue as part of the installation, overall I&C integration and commissioning phases. Validation is considered complete when a system is turned-over for normal facility operations.

4.182. The security requirements and configuration items are part of validation of each I&C component. The objective of testing security functions is to ensure that the system security requirements are validated by execution of integration, system and acceptance tests where practical and necessary.

4.183. System validation should confirm the effectiveness of the security controls and check for potential impacts, direct or indirect, on safety functions.

4.184. Each system security control should be validated to confirm that the implemented system does not increase the risk of security vulnerabilities and does not reduce the reliability of safety functions.

4.185. Validation of I&C system computer security measures should include system hardware configuration (including all external connectivity), software qualification testing, system qualification testing and system factory acceptance testing.

4.186. System validation testing should be conducted within a secure environment. For example, testing devices such as simulators or emulators should be secured or under security controls.

Installation, overall I&C integration and commissioning

4.187. The guidance provided in this section applies to all I&C systems, subsystems and components independent of their assigned security level.

4.188. During installation and commissioning, the operator should perform an acceptance review of the correctness of the physical and logical system security features in the target environment.

4.189. I&C system installation 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.

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

4.191. 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.

4.192. Security measures should be in place to control and monitor the movement of data and digital assets into and from the secure environment.

Operations and maintenance

4.193. The guidance contained within this section applies to all I&C systems, subsystems and components to which a graded approach may be applied in accordance with their assigned security level.

4.194. These activities are continuations of similar activities that occur 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 main point is that the operating organization needs to assume full responsibility for the ongoing performance of these activities when entering the operations and maintenance phase for a system.

4.195. Maintenance activities are activities undertaken by the operating organization to keep systems or components in good operating condition: Maintenance includes:

— Periodic preventive maintenance or testing to confirm operability;

— Actions to detect, preclude or mitigate degradation of components; and

— Actions to diagnose, repair, overhaul or replace failed components with identical items.

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

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

— Ensure that the I&C system security is intact by 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; and

— Perform periodic computer system security self-assessments and audits, which are key components of a good security programme.

4.198. The maintenance process should continue to conform to existing I&C system security requirements unless those requirements are to be changed as part of the maintenance activity. In some cases, security controls may need to be temporarily removed or disabled to permit execution of the required maintenance tasks. During the period for which the control is unavailable, the system is at greater risk and compensatory measures should be put in place.

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. Unnecessary or unauthorized access should be prevented to protect against system compromise.

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

4.202. Remote access should be restricted to the greatest extent possible. When remote access is required, the risk of such connections should be considered and additional security measures put in place. Such connectivity should be maintained for only as long as required 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 two-person rule, should be considered for tasks performing configuration changes on operational I&C systems.

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

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

Modification of I&C systems

4.206. The guidance provided in this section applies to all I&C systems, subsystems and components having an assigned security level.

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

— Alteration of the legacy I&C architecture may not be possible without affecting its required deterministic behaviour.

— Existing technologies used for program/data storage, interfaces, communication, etc. may not support modification.

— Existing facility structures and layout may not allow for sufficient physical protection measures.

— Contemporary technical controls that provide security monitoring functions may not be compatible with the technologies implemented within legacy I&C systems.

4.208. During modernization of a nuclear facility that involves replacement of legacy I&C systems with digital I&C systems, the following issues should be considered:

— Legacy interfaces with the original facility and other systems may need to be maintained.

— New vulnerabilities and weaknesses may be introduced because of the new technology/design.

4.209. Modification changes the system or associated documentation. These changes may be categorized as follows:

— Modifications (i.e., corrective or adaptive, changes or enhancements).

— Migration (i.e., the movement of 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).

4.210. System modifications may be derived from requirements specified to correct errors (corrective), to adapt to a changed operating environment (adaptive), or to respond to additional operator requests or enhancements.

4.211. Modifications of an I&C system should include an assessment of the security of the modified system or computer security risk assessment.

4.212. Computer security should be considered within the change management process. This includes changes to software and hardware for I&C systems.

4.213. 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 requirements; and assess modifications made including validation and verification tasks to ensure that vulnerabilities have not been introduced into the facility environment from modifications.

4.214. Security functions should be assessed as described in the above paragraphs, and should be revised (as appropriate) to reflect requirements derived from the modification process.

4.215. The modification process should continue to conform to existing I&C system security requirements unless those requirements are to be changed as part of the modification activity.

4.216. Configuration management processes should be in place to prevent the introduction of unauthorized software to I&C systems.

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

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

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

4.220. All modifications to the I&C system and its components, including software, hardware and system configurations should take into account potential security vulnerabilities and threats during the execution of these activities, but also as a result of the modifications.

4.221. Many digital assets and associated components (including removable storage media) have the ability to retain digital data when removed from the systems. This digital data may include pre-programmed logic and / or remnants of system data such as sensor readings, control signals, analytical data and network traffic. Such data may be extractable from the discarded components

4.222. Controls should be in place to ensure remnant data on discarded components cannot be used to support the development of a computer exploit.

4.223. Unless remnant data on components to be discarded have been evaluated to show that the data does not pose a risk of security compromise, the components should be destroyed or the data should be securely removed.

DECOMMISSIONING

4.224. In the decommissioning phase, until nuclear materials and other radioactive material 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.

4.225. 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.

4.226. 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).

4.227. Until decommissioning is completed, the security procedures should include cleansing the hardware and data. Upon removal from service, the operator should conduct activities such as data cleansing, disk destruction or complete overwrite to ensure data cannot be recovered.

5. OTHER CONSIDERATIONS

5.1. This publication discusses digital I&C systems associated with a nuclear facility. Other digital I&C systems such as environmental monitoring and communications systems which are important to the facility but typically are not accredited with the performance of a safety function, should be considered for computer security. These systems may introduce risks to the I&C system(s) and this risk needs to be taken into account. Security controls for these systems may be different from those discussed for digital I&C systems and should be evaluated and tailored appropriately.

5.2. I&C systems that do not use digital technology are also important and should be adequately secured. These can be covered by existing security controls prevalent for conventional systems.

REFERENCES

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

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, Draft Safety Guide DS-431 (to be published)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, 2007 Edition.

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design Specific Safety Requirements, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, Safety Requirements No. GS-R-3, IAEA, Vienna (2006).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, Draft Implementing Guide NST022 (to be published).