SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

July 2014, Vol. 57 072204:1–072204:12
doi: 10.1007/s11432-013-4792-y

System lifecycle processes for cyber security in a research reactor facility

PARK JaeKwan*, PARK JeYun & KIM YoungKi

Korea Atomic Energy Research Institute, Daedeok-daero 989-111, Dukjin-dong, Yuseong-gu, Daejeon, Korea

Received July 19, 2013; accepted October 24, 2013; published online March 6, 2014

Abstract The digitalization of nuclear facilities has brought many benefits, including high performance and convenient maintainability, in terms of facility operation. However, cyber accidents accompanied by the use of digital technologies have increased, and cyber security has been one of the most important issues in the nuclear industry area. Several guidelines have been published for nuclear power plants, but it is difficult to apply all requirements within the guidelines to research reactor facilities because the characteristics in terms of facility scale, purpose, and system design, are different from those of power plants. To address this emerging topic, this paper introduces system lifecycle processes for cyber security in a research reactor facility. It addresses the integration of activities for securing systems and guarding a facility safely using the practices at a research reactor facility.

Keywords software project management, computer-based safety systems, cyber security, security program

Citation Park J K, Park J Y, Kim Y K. System lifecycle processes for cyber security in a research reactor facility. Sci China Inf Sci, 2014, 57: 072204(12), doi: 10.1007/s11432-013-4792-y

1 Introduction

Instrumentation and control (I&C) systems collect sensor signals installed in plant fields, monitor plant's performance and status, and generate signals to control instruments for plant operation and protection. For a long time, analog technology has been utilized to sure high reliability of systems as a proven technology. Recently, such analog systems have been replaced with digital systems providing efficient performance, high reliability, and convenient maintainability. However, use of the digital I&C system can introduce the cyber security problem that may compromise important functions such as reactor shutdown or the mitigation of release of radioactive materials. Therefore, protection from cyber attacks has been one of key issues in nuclear facilities.

Recently, it has been reported that several plants have been attacked and malfunctioned by outside intruders [1]. On January, 2003, the Slammer worm attacked the I&C system vulnerability at the Davis-Besse nuclear power plant, and computer systems and safety parameter display systems were infected. Because of network traffic generated by the worm, plant personnel could not access the safety parameter display system, which would indicate meltdown conditions of the plant. On August, 2006, a shutdown

*Corresponding author (email: jkpark183@kaeri.re.kr)

of Unit 3 at the Browns Ferry nuclear power plant shows that even critical reactor components can be disrupted and disabled by a cyber attack. Unit 3 was manually shutdown after a failure of controllers with embedded microprocessors and Ethernet communication capabilities. On July, 2010, the Stuxnet worm virus was detected in the Bushehr nuclear power plant. The virus caused by a vulnerability of Microsoft Windows tried to infect systems adopting Siemens control software. A lesson learned from these incidents is that protection should be employed in I&C systems.

To cope with those cyber attacks, various studies have been proposed in information technology (IT) and plant industries. Ref. [2] suggested a security risk assessment framework in the IT industry. The framework includes processes for a security risk and vulnerability assessment. As efforts in the plant industry, Ref. [3] presented outcomes of information and communication technologies (ICT) for a security assessment, by targeting an operational power plant. The results show that the vulnerability of a plant from malicious attacks is severe. Ref. [4] introduced a practice for cyber security risk assessment in power plants. The assessment consists of a target system analysis, asset analysis, threat analysis, vulnerability analysis, risk analysis, and intrusion tests to identify the risks. In addition to research fields, national laboratories, utilities, and regulatory governments have tried to find the best way to cope with not only attacks by intruders from outside but sabotage from inside. From 2006, regulatory guides (RG) 1.152 [5] and 5.71 [6] for cyber security have been published. RG 1.152 specifies regulatory requirements for the safety systems during the development phase, and RG 5.71 describes the guides for the operation and maintenance phases in power plant sites. These guides should be mainly considered in the development process of digital systems in nuclear power plants.

Even though guides of RG 5.71 are required during the operation and maintenance phases, it is acceptable that its cyber security elements be designed and implemented during the development phase before a site application of the systems, as any later treatment of systems for cyber security may cause unpredicted defects in the systems, or may be implemented with less effective security measures. This means that the security controls in RG 5.71 should also be planned, designed, and implemented in the system development phase. This design consideration is incorporated into a cyber security lifecycle process suggested by this paper. As a specific guide, the RG 5.71 includes main elements such as establishing a defensive strategy, applying security controls, and maintaining a cyber security program and continuous monitoring. For a defensive strategy, a layered I&C architecture and the policies for each layer are required to protect the safety systems. To prevent cyber attacks, implementation of about 150 security controls are enforced. Also, a cyber security program including the above is required for a continuous monitoring and assessment. All of these elements are essential for the development and operation of nuclear power plants to comply with the regulatory guidelines.

The focus of this paper is the digital I&C systems of a research reactor that has different characteristics from a nuclear power plant. Table 1 shows the characteristics of research reactors in terms of cyber security. A research reactor has a lower probability to be an attack objective from cyber terrorists than a nuclear power plant in terms of facility importance and purpose. A direct impact caused by a cyber attack is relatively low because it has a far lower power rating and less radioactive materials in the reactor core that can be dispersed in a worst-case accident. The economic feasibility of a facility is one of the important considerations in the process of a system design, mainly in the use of a research reactor for radioisotope production. As learned from previous design practices, many control and monitoring systems are classified as relatively lower quality class than those of a power plant. This leads digital systems to have a weakened design. Generally, a research reactor is located near a town for convenience. Thus, severe accidents (e.g., release of radioactive materials) caused by cyberattacks can highly impact a public safety directly and quickly. Therefore, applying cyber security protection design to research reactor is one of the key issues.

The problem is a lack of studies, practices, and guidelines associated with the cyber security of a research reactor. Actually, this makes system designers hesitate with cyber security in their facilities. Intuitively, all requirements prepared for a nuclear power plant can be used for a research reactor. However, this requires a very high cost to a research reactor, which is small scale facility, and may also result in a blind excessive design of the research reactor. Generally, many design requirements for a power

Table 1 Comparison of characteristics between research reactor and power plant

	Power plant	Research reactor	Accident probability and impact by cyber security
Purpose	Electricity generation	Radioisotope production, R&D using neutron	Low probability
Power	$\sim$ 3000 MW (thermal)	0 $\sim$ 30 MW (thermal)	Low impact
Operation condition	High pressure and high temperature	Low pressure and low temperature	Low impact
System design	Complicated and conservative design	Relatively simple and design efficiency for cost-down	High probability
Site	Far from a town	Near to a town	High probability, high impact

plant have been considered for the system design of a research reactor in a graded approach by both system designers and regulatory bodies. Therefore, it is important to propose and discuss various graded approaches for the cyber security of research reactors.

Based on a graded approach for the common digital I&C systems of research reactors designed in Korea, this paper proposes a cyber securitydevelopment framework which is an overall proactive plan for implementing protective means to prevent and mitigate cyber attacks. The proposed method contains the overall design lifecycle, security considerations within the system, and cyber security activities for the facility. First, a cyber security lifecycle process is established to define additional cyber security activities to the development and operation phases. Next, security activities for securing digital systems in terms of system features are defined, and security activities for protecting digital systems in terms of facility safeguards are proposed. Finally, the security controls for digital I&C systems are analyzed and assessed qualitatively. The application of selected security controls is recommended based on the analysis results.

To describe the research aim and results, this paper consists of the following sections. Section 2 briefly reviews the current status and history of cyber security requirements for nuclear power plants. Section 3 suggests a cyber security lifecycle process for the integration of the system development activities and the overall security activities. Section 4 proposes an integrated development framework of digital systems. Finally, the last section concludes this paper and discusses some avenues for future work.

2 Cyber security requirements in nuclear power plant

10 CFR (Title 10, Code of Federal Regulations) and regulatory guidelines published by the United States nuclear regulatory commission (US NRC) are internationally referenced for the design and construction of nuclear plant facilities. For cyber security, the NRC has published several important codes, such as 10 CFR 50.55a(h) [7], 10 CFR 73.1 [8], and 10 CFR 73.54 [9]. In addition, the NRC has provided two specific guides, RG 1.152 and RG 5.71, in compliance with the regulations. Figure 1 shows history and current state of cyber security requirements in terms of regulation codes, guidelines, and industrial standards.

The 10 CFR 50.55a(h) requires that equipment including software and hardware of digital safety systems shall be protected. The RG 1.152 [10] published in 2006 describes a method that the staff of the NRC deems acceptable for complying with the regulations for promoting high functional reliability, design quality, and cyber security for the use of digital computers in the safety systems of nuclear power plants. The regulatory body provides specific guidance concerning safety system security. It uses the waterfall lifecycle phases as a framework for describing the specific guidance. The framework waterfall lifecycle consists of nine phases, (1) concepts, (2) requirements, (3) design, (4) implementation, (5) test, (6) installation, checkout, acceptance testing, (7) operation, (8) maintenance, and (9) retirement. It requires that system features and development activities for cyber security be implemented and performed through these phases.

In 2007, the NRC updated the design basis threat (DBT) of 10 CFR 73.1 as the DBT includes cyber security threats. Thus, the 10 CFR 73.1 requires ensuring that digital computers, communication systems, and networks be protected from cyber attacks. In 2009, the NRC revised 10 CFR 73.54 to require plant

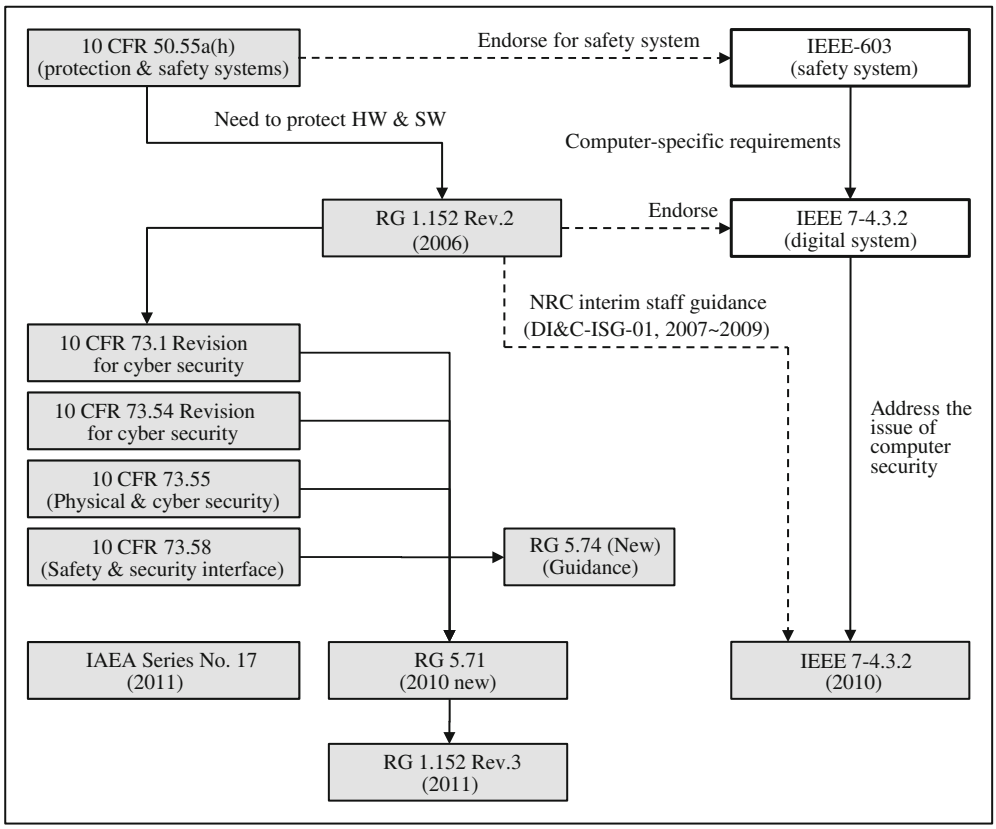

Figure 1 History and current state of cyber security requirements.

designers to develop cyber security plans and programs to protect critical assets including safety systems from cyber attacks. For specific guidance to the 10 CFR 73.54, the NRC published a new regulatory guide 5.71 in January 2010. It describes an approach complying with 10 CFR 73.54 and 73.1 and provides a template for a cyber security plan including a defensive architecture and a set of security controls.

IEEE Std 7-4.3.2-2010 [11], which was recently updated from the 2003 version, also mentions that the digital safety system/equipment development process shall address potential security vulnerabilities in proper phase of the digital safety system lifecycle, and system security features should be addressed appropriately in the lifecycle phases. The development process is almost the same as that of RG 1.152 (Rev.02). IAEA Series No. 17-2011 [12] aims to create awareness of the importance of incorporating computer security as a fundamental part of the overall security plan for nuclear facilities. The publication provides guidance specific to nuclear facilities on implementing a computer security program.The content of the publication is similar tothat of RG 5.71.

In July 2011, the NRC published RG 1.152 (Rev.03) to provide consistency with RG 5.71. First, the point of view in the guide was changed from cyber security into a secure development and operational environment. Second, phases from installation to retirement were eliminated because the RG 5.71 provides guidance for the phases. Currently, nuclear power plants directly or indirectly regulated by NRC codes and guides are enforced in conformance with above requirements. This paper refers to these requirements as the research basis and develops an application method for a research reactor from the basis for power plants.

3 A cyber security lifecycle process overview

This paper establishes an integrated cyber security lifecycle process as shown in Figure 2. The process contains the primary elements of a cyber security plan for a Korean research reactor. The contribution is that it makes a cyber security strategy be designed and maintained consistently by clarifying the

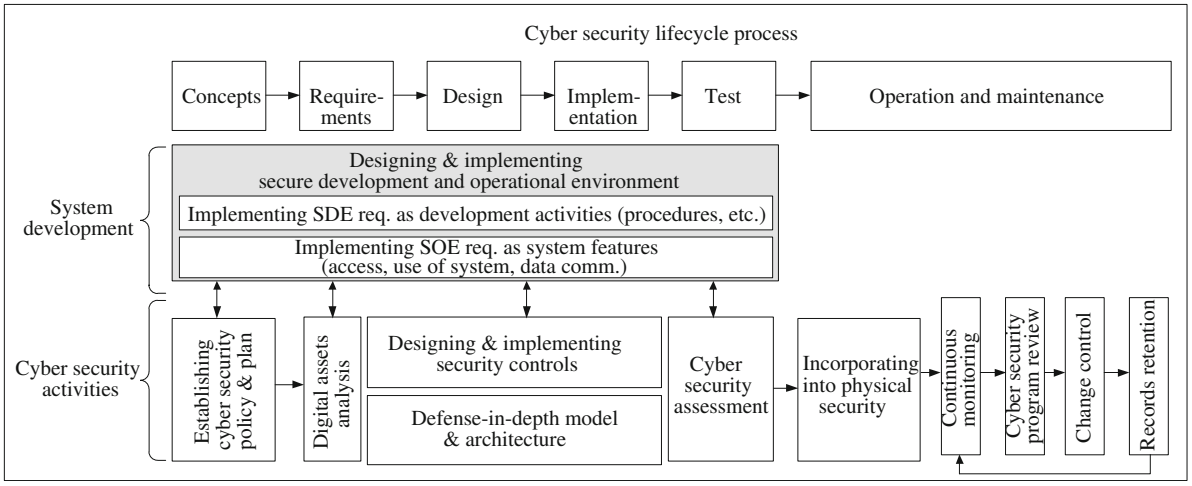

Figure 2 An integrated cyber security lifecycle process.

interface activities between the system development framework and cyber security program. That is, technical security controls required by a cyber security program are implemented within the system development phase and protective guidelines defined by the program are referred by the development phase. In addition to the collaborating works, the system development framework includes activities for a secure development environment (SDE) and a secure operational environment (SOE) to prevent any potential threats (e.g., back door, virus) from residing within the digital system during the development process.

Furthermore, the proposed processes guide a way to establish a cyber security program containing activities for cyber security in terms of a facility safeguard. The cyber security program progresses through establishing and maintaining phases, and the program consists of several main elements, digital asset identification, defense-in-depth strategy, security controls application, and continuous monitoring and assessment. The points of distinction of the proposed overall process from the regulatory guidelines are to integrate and arrange whole activities within the lifecycle process. In detail, alignments between the system development and cyber security program are defined, and interfaces between them are guided in this paper.

4 An integrated development framework of digital systems

This paper proposes a development framework for digital systems including cyber security considerations as a modification of a well-known waterfall design model, which consists of concept, requirement, design, implementation, test, and operation and maintenance phases. It also includes additional activities which are acceptable to be considered in the development process to support cyber security program required in operation phase. As discussed above, establishing and maintaining the cyber security program is very important to prevent or mitigate cyber attacks. Generally, a cyber security program includes several primary elements configuration of a cyber security team, critical digital assets identification, a defense-in-depth protective strategy, application of security controls continuous monitoring and assessment, change control, and cyber security program review. As a practice of a graded approach for a research reactor, this paper proposes a cyber security program by introducing the implementing method of the primary elements appropriately. The elements are described through the system development processes. Our framework incorporates cyber security considerations, such as interface activities with a defense-in-depth strategy for security consistency and implementation of technical security controls required in a cyber security program, into the development lifecycles. This paper explains the framework by focusing on cyber security activities because activities for the implementation of system functions are the same as original waterfall model.

4.1 Concept phase

During the concept phase, functional concepts and conceptual architectures for all I&C systems are defined. This phase includes several cyber security activities. Initially, an analysis of a site operation environment is performed and functional concepts required to establish a secure operational environment for digital systems are identified. The identified concept features become the inputs for the design requirements in the requirement phase. Also, an assessment is performed to identify potential challenges to maintaining a secure operational environment for the system and a secure development environment during the development process. The results of the analysis are used to establish secure requirements for both hardware and software.

Furthermore, it is necessary that a cyber security plan be prepared for aligning with the concept phase. The reason for this is that the cyber security scope, policy, team, and implementation schedules should be referred continuously during entire lifecycles. Also, cyber security team is organized in this phase. In case of a Korean research reactor, two cyber security teams for the development and operation phases are made as they are different organizations. During the development phase, there is no dedicated cyber security team, but the system development members are responsible for the supervision and implementation of security controls as a cyber security team (CST). The I&C system design manager concurrently holds the position of cyber security manager because most digital systems belong to the I&C area. Cyber security specialists within the CST are responsible for (1) performing cyber security evaluations of digital systems and (2) maintaining expert skill and knowledge in the area of cyber security. System developers are responsible for (1) establishing cyber security requirements of systems, (2) designing cyber security items of systems, (3) implementing and testing I&C systems, and (4) applying a cyber security plan and policy for the implementation, testing, and installation of the systems.The cyber security team for operation phase is organized in the operation and maintenance phase.

4.2 Requirement phase

In this phase, design requirements of digital systems are established and the results of the previous phase are carefully addressed for cyber security. System features required to maintain a secure operating environment and ensure reliable system operation are defined as part of the overall system requirements. The system design requirements also include well-known cyber security requirements, such as blocking the external interface, communication networks, high reliable modification procedures, the exclusion of remote access, and access control. Activities to identify critical systems (CSs) and critical digital assets (CDAs) are performed together with this phase. It is useful that functional requirements and security requirements of systems be considered together. If the potential vulnerabilities of digital assets are induced by their functional requirements, the results are fed back to developers, and the design problems are resolved directly in the same phase. In the same manner, a defensive architecture is also drawn in this phase.

4.2.1 *Critical digital assets identification*

The common I&C systems of a Korean research reactor consist of computer-based systems with digital communication networks as shown in Figure 3. There are two control rooms; main control room (MCR) and supplementary control room (SCR). All monitoring and control actions are performed in the MCR and a reactor shutdown action is performed in the SCR under situations in MCR inaccessible. There are two safety grade systems, a reactor protection system (RPS) and a post-accident monitoring system (PAMS). The RPS is a safety control system, which is the most important to protect reactor safety, and the PAMS is a safety monitoring system for monitoring the reactor facility continuously under normal and abnormal conditions. Other monitoring and control systems are classified as non-safety systems.

Based on the conceptual design, system developers must identify critical digital assets (CDAs) because not all digital systems can be protected from cyber attacks. However, it is difficult to identify CDAs without first conducting a wider assessment of all of the systems within the facility. Thus, a qualitative consequence analysis of the systems is conducted, as shown in Figure 4.

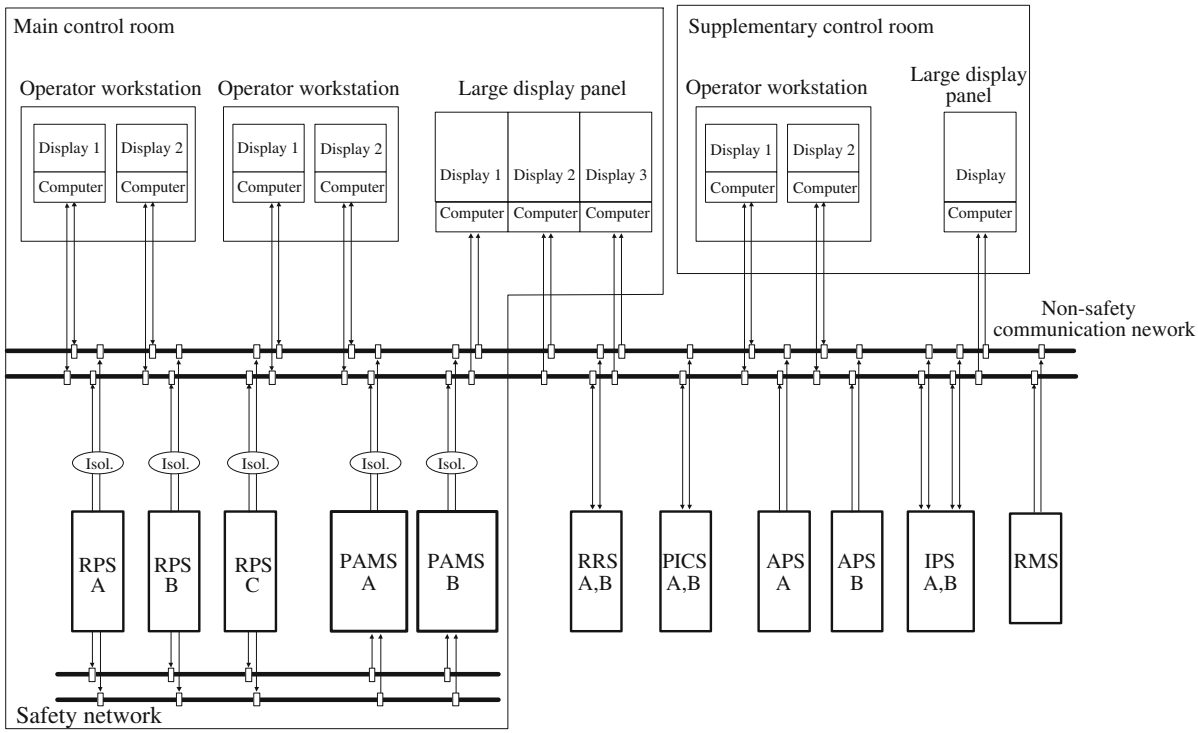

Figure 3 An example of fully-digitalized systems of a research reactor.

Table 2 Results of CDA identification in a research reactor

Critical systems	**Critical digital assets**
Reactor protection system	Bistable processor, maintenance and test processor, interfaces and test processor
Post-accident monitoring system	Signal processor, maintenance and test processor
Safety network	Isolator, optical communication cable
Non critical systems	**Non critical digital assets**
Reactor regulating system	Control computer, maintenance computer
Alternate protection system	Bistable controller, maintenance computer
Information processing system	Processing server
Process instrumentation and control system	Control computer, maintenance computer
Radiation monitoring system	Monitoring computer, maintenance computer
Operator workstation/large display panel	Workstation computer, display control computer
Non-safety network	Network switch, communication cable

Generally, the CST identifies and selects critical systems (CSs), such as digital systems, equipment, communication systems, and networks that are associated with safety, security, and emergency preparedness (SSEP) functions. The CST also identifies CDAs that have a direct, support, or indirect role in the proper functioning of CSs. Additionally, one more condition, the quality class of the system, is used during decision making process. The reasons for this are that the quality class is determined by its importance to safety during the initial concept phase, and it helps to distinguish between CDA and non-CDA more precisely.

Table 2 shows results of critical systems and critical digital assets identification, through the decision making mechanism, in the digital systems of a Korean research reactor. In the analysis results, digital safety systems and a safety network are determined as critical systems. That is, a compromise of these systems can result in radiological sabotage (i.e. core damage) and therefore has the potential to adversely impact the public health and safety. Other systems are classified into non critical systems because the reactor facility is assured of safety status under the failure of these systems.

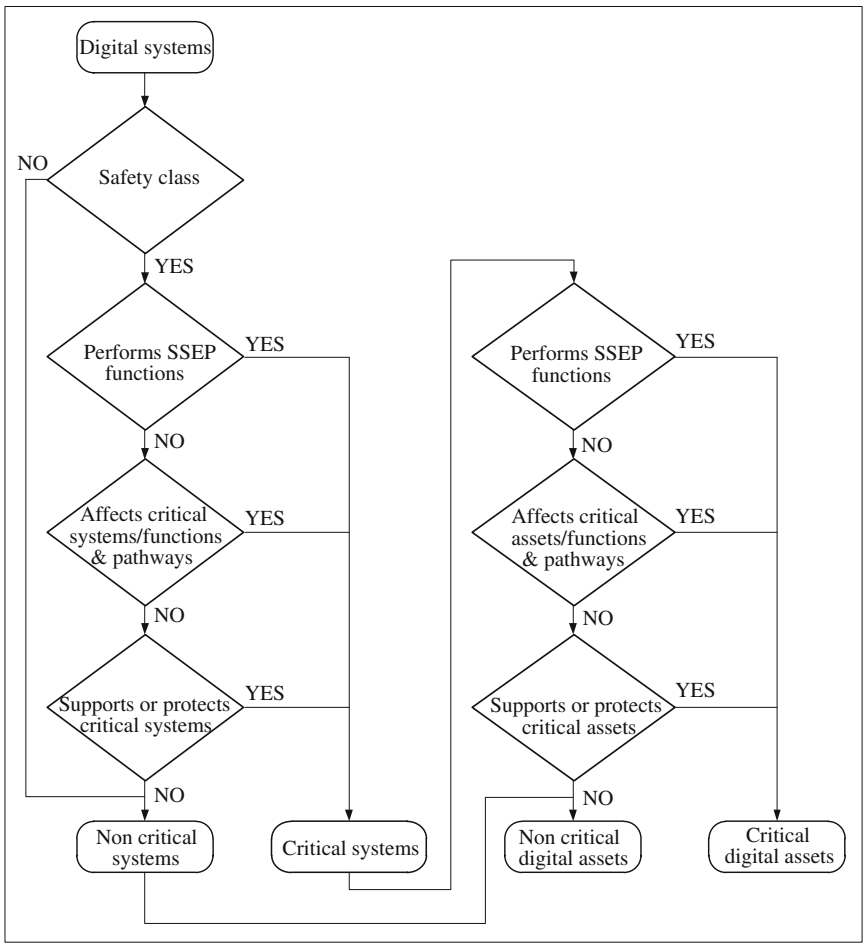

Figure 4 Decision making mechanism of critical systems and digital assets.

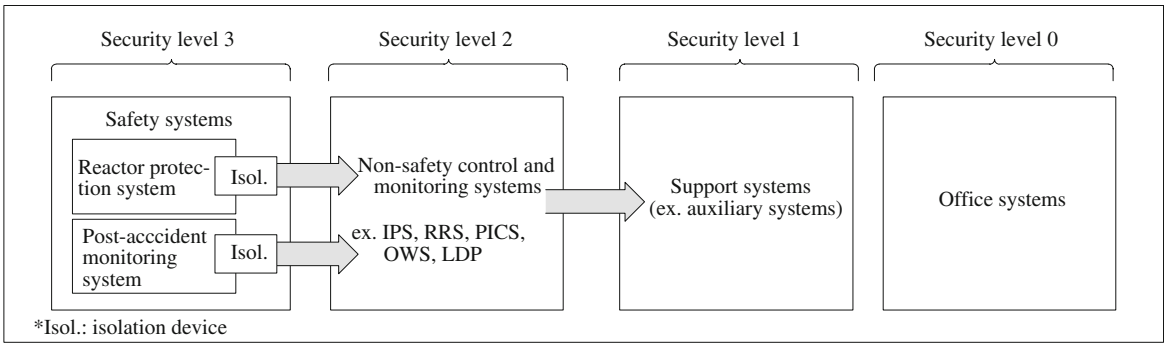

Figure 5 A cyber security defensive architecture.

4.2.2 *Defense-in-depth strategy*

After CDAs identification, a defense-in-depth strategy is prepared to establish multiple layers of protections to guard CDAs safely. Its purpose is that the failure of a single layer should not result in the compromise of CDAs. This paper proposes a strategy composed of a defensive architecture and associated policies for control access to multiple layers. Figure 5 briefly shows a defensive architecture for Korean research reactor.

In this practice, there are 4 security levels (or layers), and the CDAs are located at the highest level. Control and monitoring systems reside in security level 2, other auxiliary support systems in security level 1, and office systems in security level 0. In addition to the decomposition of security levels, several

policies are defined to protect the CDAs. Basically, only one-way data flow is allowed between levels 3 and 2. In addition, data flow is only allowed through dedicated devices having security checking capability between levels. Also, the initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited. These policies are implemented using both technical controls (e.g., the boundary devices) and management controls (e.g., limitation of communication software).

4.3 Design phase

Based on the requirement documents, a detailed design is provided in this phase. The design features are translated into specific design configuration items. From the SDOE point of view, measures are taken to prevent the introduction of unnecessary design features or functions. For the measures, specific procedures for the development environment are applied. Security controls for the CDAs or the defense-in-depth architecture are also mapped into specific design items as part of the systems in this phase. For example, password, session lock, and isolation devices become design items for the control of access requirements. To decide whether the design is acceptable, a security assessment to identify potential cyber security vulnerabilities to CDAs is performed using detailed design documents.

One way to address potential cyber risks of CDAs at the highest security level is to develop cyber security controls described in RG 5.71. The guide includes about 150 security controls classified as technical controls, operational controls, and management controls. Technical controls are safeguards or protective measures that are executed through automatic mechanisms contained within the hardware or software, and controls within this class include access controls, accountability, system protection, and so on. Operational controls are protective measures typically performed manually rather than automated means, and controls within this class include activities involving media protection, physical protection, maintenance, and training. Management controls are to concentrate on risk management and a security policy, and controls within this class cover activities involving system acquisitions, security assessment, and the modification of digital assets. Nuclear power plants have been enforced to apply all of the cyber security controls to their facilities.

A selection method of mandatory security controls based on characteristics analysis of a research reactor can be an acceptable method as a graded approach. This paper introduces a practice for the application of security controls to a Korean research reactor.It has been analyzed that about half of the controls can be applied to the research reactor completely. For the remaining controls, the environmental conditions of the research reactor are additionally considered. In a research reactor, the number of operation and maintenance staffs is fewer than power plants, and jobs for access control are also relatively simple. Furthermore, digital systems and CDAs are very few in number compared with power plant facilities. These enable the use of manual controls as a substitute for security controls that are hard to implement an automatic mechanism. Under these considerations, several controls, *account management, system use notification, supervision and review, access control for portable and mobile devices*, can be sufficiently implemented manually through the procedure. For a similar reason, the security control, *separation of functions*, can be eliminated. Furthermore, related controls, *access enforcement and least privilege*, can be integrated into *account management control*. Some controls, *information flow enforcement, network access control, wireless access restriction, and use of external systems*, can be partially applied because attack paths do not exist or partially exist. In addition to the access control, other types of security controls have also been analyzed in similar manner. As a result, about 70 security controls are selected for application to Korean research reactor through the analysis. The security controls are summarized in Table 3.

4.4 Implementation phase

During this phase, all design items are transformed into specific hardware and software representations. System developers implement secure development environment procedures to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The procedures include testing to address undocumented codes or functions. Security controls are also implemented and verified by aligning with this phase.

Table 3 A list of selected security controls for a research reactor

Control category	Security controls applied to research reactor
Access control	Access control policy and procedure, account management, information flow enforcement, unsuccessful login attempts, system use notification, previous login notification, session lock, supervision and review-access control, permitted actions without identification or authentication, automated marking/labeling, network access control, open/insecure protocol restrictions, wireless access restriction, insecure rogue connections, access control for portable and mobile devices, proprietary protocol visibility, third party products and controls, use of external systems, publicly accessible content
Audit	Audit and accountability policy and procedure, auditable events, content of audit records, audit review, analysis, and reporting
CDA and communication protection	CDA and communication protection policy and procedure, shared resources, DoS protection, transmission integrity/confidentiality, trusted path, mobile code, fail in known state
Identification and authentication	Identification and authentication policy and procedure, user identification and authentication, password requirements, identifier management, authenticator management
System hardening	Removal of unnecessary services and programs, host intrusion detection system, hardware configuration, installing OS, applications, and third-party software updates
Media protection	Media protection policy and procedure, media access, media labeling/marking, media storage, media transport, media sanitation and disposal
Personnel security	Personnel security policy and procedure, personnel termination or transfer
Physical and environmental protection	Physical and environmental protection policy and procedure, third party/escorted access, physical and environmental protection, physical access authorization, physical access control (transmission/display medium), visitor control access records
Incident response	Incident response policy and procedure, incident response training, incident response testing and drills, incident handling, incident monitoring, incident reporting
Configuration management	Configuration management policy and procedure, baseline configuration, configuration change control, security impact analysis of changes and environment
System and service acquisition	System and service acquisition policy and procedure, supply chain protection, trustworthiness, integration of security capabilities, developer security testing, licensee/applicant testing
Security assessment and risk management	Threat and vulnerability management, risk mitigation

4.5 Test phase

During this phase, it is verified that the implementation results meet the design requirements completely. Through tests on the system hardware, software, and communication devices, it is validated that the system is implemented appropriately in terms of system functions, the effects of the connected system, and SDOE. Additionally, penetration tests are prepared to identify the remaining potential security vulnerability. These tests are only focused on important assets such as CDAs, CSs, and communication networks.

4.6 Operation and maintenance phase

The cyber security team for the operation phase is responsible for maintaining of the cyber security program established in the development phase. The security team conducts (1) continuous monitoring and assessment, (2) change control, and (3) cyber security program review. The team members receive cyber security training in order to manage the defense-in-depth strategy and security controls.

In the operation and maintenance phase, a continuous monitoring and assessment strategy is prepared. This is performed to maintain high security capabilities from cyber attacks. The strategy for Korean research reactor is summarized as (1) an assessment to verify that the security controls remain in place, (2) verification of whether the rogue assets are connected to the I&C network infrastructure, and (3) a periodic assessment of the effectiveness of the security controls.In particular, a periodic assessment

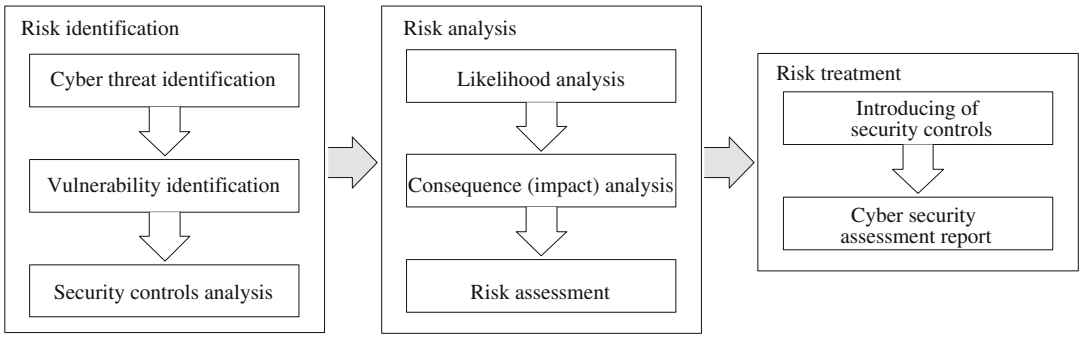

Figure 6 A cyber security assessment process for a research reactor.

includes an analysis of the system features, identification of the vulnerabilities, and a risk assessment. The overall process of assessment is shown in Figure 6. In risk identification, the CST identifies new cyber threats and vulnerability to such threats, and then analyzes the defense capabilities of existing controls against these threats. In risk analysis, the CST analyzes the incident likelihood from a cyber threat, the consequences to the facility and public safety, and assesses the total risk by combining the possibility and impact. Finally, the CST proposes new security controls to prevent or mitigate cyber threats and reports the assessment results to the supervisor.

The change control of Korean research reactor is exhaustively managed under specific procedures because it can generate a new vulnerability in the existing configuration. Changes to the environment of the CDAs, such as addition, deletion, or modification, are planned, approved, tested, and documented to sure that the CDAs are protected from cyber attacks. The changes are made to the CDAs according to the configuration management procedures. During the retirement phase, the configuration management procedures include safety, reliability, and security engineering activities.

The elements of a cyber security program for Korean research reactor are periodically reviewed by the CST. The review is performed (1) when a change occurs to the personnel, procedures, equipment, or facilities that can adversely affect security, or (2) as necessary based upon site-specific analyses, assessments, or other performance indicators conducted. The CST documents the results and recommendations of program reviews, management findings regarding program effectiveness, and any actions taken as a result of recommendations from a prior program review.

5 Conclusion

In this paper, we introduced the cyber security application issues and problems related to a research reactor facility, and surveyed the current state of references, which are a lack of research works, reports, and practices. As a reasonable solution, we proposed an integrated development framework forthe cyber security establishment of a research reactor facility based onthe practices experienced ina research reactor. Based on international guides, we clarified the cyber security lifecycle process integrating the activities required at the system and facility levels. Furthermore, we suggested a development framework that incorporates security considerations, implementation of technical controls and interface activities with a protective strategy, into the development lifecycle phases in terms of system development.As important security considerations, we discussed the identification of critical digital assets, establishments of defensive architecture, and application of security controls on the development lifecycle processes using practices at a research reactor. We expectthe system lifecycle processes of this paper to be useful to researchers and practitioners with an interest in designing and creating cyber security for digital systems in nuclear area.

Our work is on-going and this is focused on the elements of a cyber security plan. Thus, the issue of incorporating a cyber security program into a physical protection program, development of a security assessment model for the feasibility study of security controls, and a method of revising a cyber security program at the site remain as further studies.

References

1 Kesler B. The vulnerability of nuclear facilities to cyber attack. Strategic Insights, 2011, 10: 15–25
2 Saleh Z I, Refai H, Mashhour A. Proposed framework for security risk assessment. J Inf Secur, 2011, 2: 85–90
3 Nai Fovino I, Guidi L, Masera M, et al. Cyber security assessment of a power plant. Elec Power Syst Res, 2011, 81: 518–526
4 Lee C K, Park G Y, Kwon K C, et al. Cyber security design requirements based on a risk assessment. In: Proceedings of the Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Knoxville, 2009. 1638–1646
5 USNRC. Regulatory Guide 1.152 Revision 3. Criteria for use of computers in safety systems of nuclear power plants, 2011
6 USNRC. Regulatory guide 5.71. Cyber security programs for nuclear facilities, 2010
7 USNRC. 10 CFR 50.55a(h). Protection and safety systems, 1971
8 USNRC. 10 CFR 73.1. Physical protection of plants and materials, 2007
9 USNRC. 10 CFR 73.54. Protection of digital computer and communication systems and networks, 2009
10 USNRC. Regulatory guide 1.152 revision 2. Criteria for use of computers in safety systems of nuclear power plants, 2006
11 IEEE. IEEE Std. 7-4.3.2-2010. Criteria for digital computers in safety systems of nuclear power generating stations, 2010
12 IAEA. Nuclear Security Series No. 17. Computer Security at Nuclear Facilities, 2011