http://dx.doi.org/10.5516/NET.04.2011.065

A CYBER SECURITY RISK ASSESSMENT FOR THE DESIGN OF I&C SYSTEMS IN NUCLEAR POWER PLANTS

JAE-GU SONG, JUNG-WOON LEE[*], CHEOL-KWON LEE, KEE-CHOON KWON, and DONG-YOUNG LEE
Korea Atomic Energy Research Institute
989-111 Daedeok-daero, Yuseong-gu, Daejeon 305-353, Republic of Korea
[*]Corresponding author. E-mail : leejw@kaeri.re.kr

Received November 21, 2011
Accepted for Publication March 13, 2012

The applications of computers and communication system and network technologies in nuclear power plants have expanded recently. This application of digital technologies to the instrumentation and control systems of nuclear power plants brings with it the cyber security concerns similar to other critical infrastructures. Cyber security risk assessments for digital instrumentation and control systems have become more crucial in the development of new systems and in the operation of existing systems. Although the instrumentation and control systems of nuclear power plants are similar to industrial control systems, the former have specifications that differ from the latter in terms of architecture and function, in order to satisfy nuclear safety requirements, which need different methods for the application of cyber security risk assessment. In this paper, the characteristics of nuclear power plant instrumentation and control systems are described, and the considerations needed when conducting cyber security risk assessments in accordance with the lifecycle process of instrumentation and control systems are discussed. For cyber security risk assessments of instrumentation and control systems, the activities and considerations necessary for assessments during the system design phase or component design and equipment supply phase are presented in the following 6 steps: 1) System Identification and Cyber Security Modeling, 2) Asset and Impact Analysis, 3) Threat Analysis, 4) Vulnerability Analysis, 5) Security Control Design, and 6) Penetration test. The results from an application of the method to a digital reactor protection system are described.

KEYWORDS : Cyber Security, Risk Assessment, Nuclear Power Plant, Instrumentation and Control System, Cyber Attack

1. INTRODUCTION

The instrumentation and control (I&C) systems in nuclear power plants (NPPs) collect signals from sensors measuring plant parameters, integrate and evaluate sensor information, monitor plant performance, and generate signals to control plant devices for a safe operation of NPPs. Although the application of digital technology in industrial control systems (ICS) started a few decades ago, I&C systems in NPPs have utilized analog technology longer than any other industries. The reason for this stems from the fact that NPPs require strong assurance for safety and reliability. In recent years, however, digital I&C systems have been developed and installed in new and operating NPPs. This application of digital computers, and communication system and network technologies in NPP I&C systems accompanies cyber security concerns, similar to other critical infrastructures based on digital technologies. The Stuxnet case in 2010 evoked enormous concern regarding cyber security in NPPs. Thus, performing appropriate cyber security risk assessment for the digital I&C systems of NPPs, and applying security measures to the systems, has become more important nowadays.

In general, approaches to assure cyber security in NPPs may be compatible with those for ICS and/or supervisory control and data acquisition (SCADA) systems in many aspects. Cyber security requirements and the risk assessment methodologies for ICS and SCADA systems are adopted from those for information technology (IT) systems. Many standards and guidance documents have been published for these areas [1~10]. Among them NIST SP 800-30 [4], NIST SP 800-37 [5], and NIST 800-39 [6] describe the risk assessment methods, NIST SP 800-53 [7] and NIST SP 800-53A [8] address security controls for IT systems. NIST SP 800-82 [10] describes the differences between IT systems and ICS and provides guidance for securing ICS, including SCADA systems, distributed control systems (DCS), and other systems performing control functions. As NIST SP 800-82 noted the differences between IT systems and ICS, the details of risk assessment methods for ICS should be modified from those for IT systems.

As cyber security has been an emerging concern in nuclear industries, the U.S. NRC issued the regulatory guide (RG) 1.152 revision 2 [11] in 2006. This regulatory guide addresses cyber security for the use of digital computers in the safety systems of NPPs. It describes the regulatory position by using the waterfall lifecycle phases, which consist of the following phases: 1) Concepts; 2) Requirements, 3) Design, 4) Implementation, 5) Test, 6) Installation, Checkout, and Acceptance Testing, 7) Operation, 8) Maintenance, and 9) Retirement. It is necessary that the digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle. In 2009, 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks [12]," required NPP licensees in the U. S. to submit a cyber security plan for protecting critical digital assets (CDAs) associated with the following categories of functions from cyber attacks: 1) safety-related and important-to-safety functions, 2) security functions, 3) emergency preparedness functions, including offsite communications, and 4) support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. RG 5.71 [13] was issued in 2010 for applicants and licensees to comply with the requirements of 10 CFR 73.54. This regulatory guide applies to operating NPPs, and to the application for a combined operating license. RG 5.71 provides a framework to aid in the identification of CDAs categorized in 10 CFR 73.54, the application of a defensive architecture, and the collection of security controls for the protection of CDAs from cyber threats. The issuance of RG 5.71 brought about the need for a revision of RG 1.152 due to the duplication of cyber security matters. The draft regulatory guide DG-1249 [14] for RG 1.152 revision 3 was issued for review in 2010. DG-1249 aims to eliminate reference to cyber-security and also eliminate directions to evaluate systems against intentional malicious actions or attacks. DG-1249 is clarifying its focus on the following issues: 1) protection of the development environment from inclusion of undocumented and unwanted code, 2) protection against undesirable behavior of connected systems, and 3) controls to prevent inadvertent access to the system. DG-1249 also contains a regulatory position regarding the 5 waterfall lifecycle phases from 1) Concepts to 5) Test, which are narrowed from the 9 phases in RG 1.152 revision 2. In the phases after 6) Installation, Checkout, and Acceptance Testing, regulations are handed over to RG 5.71. A draft of the IAEA technical guidance [15] provides information on a cyber security plan and policy, risk assessment and management, and other considerations for nuclear facilities. The IEEE Standard 7-4.3.2-2010 [16] was issued as a revision of the previous version, in which cyber security requirements with a lifecycle approach were newly supplemented.

Although many standards and guidance documents have been published for cyber security risk assessments of IT systems or ICS, the methods in these documents are not well suited for NPP I&C systems due to their different characteristics. In the nuclear domain, NRC regulatory guides, IEEE Std. 7.4.3.2-2010, and the draft IAEA technical guidance are available for the cyber security of the I&C systems. However, practical guidance of the risk assessments of I&C systems compatible with the lifecycle process, especially for the development phases, is still needed by NPP system designers and equipment suppliers.

In this study, a practical approach for the cyber security risk assessment of NPP I&C systems is proposed by considering the characteristics and lifecycle of these systems, and by focusing on detail matters that can be considered when NPP I&C system designers and equipment suppliers perform cyber security risk assessment activities, based on the general procedure for cyber security risk assessments of IT systems. The results from a sample application of the approach in a reactor protection system among NPP I&C systems are described.

2. CONSIDERATIONS IN CYBER SECURITY DESIGN FOR NPP I&C

In this section, characteristics of NPP I&C systems and the relationship between NPP I&C lifecycle and cyber security design are discussed for considerations needed for the cyber security risk assessments.

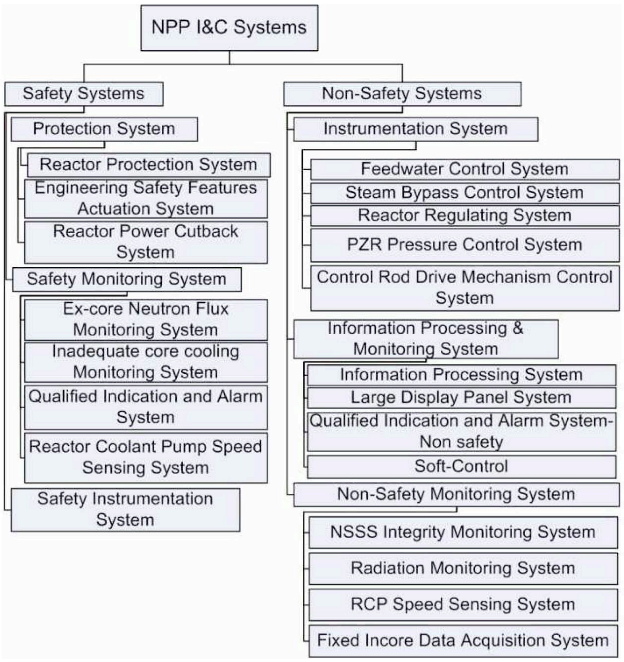
NPP I&C Systems
Safety Systems
Protection System
Reactor Proctection System
Engineering Safety Features Actuation System
Reactor Power Cutback System
Safety Monitoring System
Ex-core Neutron Flux Monitoring System
Inadequate core cooling Monitoring System
Qualified Indication and Alarm System
Reactor Coolant Pump Speed Sensing System
Safety Instrumentation System
Non-Safety Systems
Instrumentation System
Feedwater Control System
Steam Bypass Control System
Reactor Regulating System
PZR Pressure Control System
Control Rod Drive Mechanism Control System
Information Processing & Monitoring System
Information Processing System
Large Display Panel System
Qualified Indication and Alarm System-Non safety
Soft-Control
Non-Safety Monitoring System
NSSS Integrity Monitoring System
Radiation Monitoring System
RCP Speed Sensing System
Fixed Incore Data Acquisition System

Fig. 1. Safety and Non-safety I&C Systems in NPPs.

2.1 Characteristics of NPP I&C Systems

As shown in Fig. 1, NPP I&C systems can be grouped into two categories: safety systems and non-safety systems. In some regulatory requirements, safety systems can be further graded as either safety-critical or important-to-safety. Safety systems require higher reliability, functionality, and availability than non-safety systems, as they function to shutdown the reactor safely and maintain it in a shutdown condition. Likewise, their hardware should have redundancy and their software should be qualified through rigorous verification and validation processes. Failures in the non-safety systems should not cause a loss of safety function. Meanwhile, non-safety systems have a similar structure and constituents to those of in other industries.

This classification of safety and non-safety, and the requirements for safety systems affect the architecture of these systems, and the network connections between two. Hence, in cyber security risk assessments for NPP I&C systems, the activities including determination of security levels, threat and vulnerability analyses, design of security controls considering the data flow through communication networks, and testing the security controls require modification of the process and guidance for ICS.

2.2 NPP I&C Lifecycle and Cyber Security Design

Fig. 2 shows the general lifecycle process of I&C systems in NPPs. The original figure in NUREG-0800 Ch. 7.0 [17] was modified to include the activities only for hardware and software development, and to represent the major cyber security milestones in three phases, in accordance to the organizations involved: a system design (SD) phase, a component design and equipment supply (CD/ES) phase, and an operation and maintenance phase. Since there are differences in the depth and details of cyber security risk assessments during each phase of the development, this paper tries to describe the assessment activities and corresponding considerations for NPP I&C system designers and equipment suppliers.

In the SD phase, an SD company establishes the target system concept and requirements, produces system design documents, and hands over them to the CD/ES phase. In the following phase, a CD/ES company performs the hardware and software design of the target system, and implements and integrates the system. This integrated system then goes through a validation process, and is installed at a target NPP. The utility company who owns the NPP operates the system in its NPP site.

RG 1.152 revision 2 [11] and IEEE Std. 7-4.3.2-2010 [16] require that the digital safety system development process address potential security vulnerabilities in each phase of the digital safety system lifecycle, and also that system security features should be addressed appropriately in the lifecycle phases. Therefore, cyber security features should be designed and implemented during the SD and CD/ES phases before installation, as any later treatment may cause other defects in the systems, or may be implemented with less effective security measures. Although RG 1.152 revision 2 [11] and IEEE Std. 7-4.3.2-2010 [16] mention the cyber security of safety systems, cyber security design for non-safety systems is also important, if any NPP trip events due to cyber attacks are possible.

Since cyber security features should be incorporated in the SD phase, a cyber security risk assessment should be performed in this phase, to provide the requirements for the design of target systems. System design specifications produced in this phase are translated into hardware design specifications for purchase and/or manufacturing, and software design specifications for detailed design and implementation during the CD/ES phase. The design in the CD/ES phase becomes more concrete and detailed than in the SD phase. It would be better to reassess the

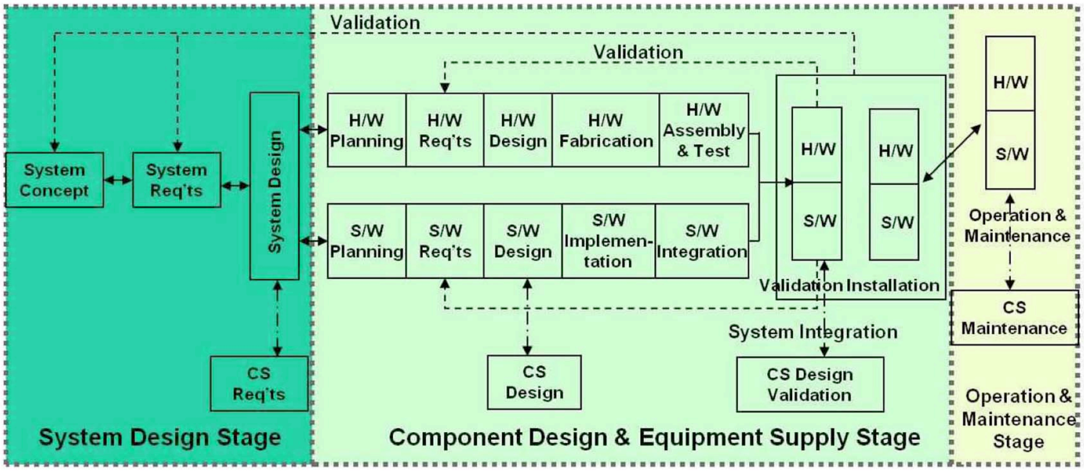

Fig. 2. General Lifecycle Process of I&C Systems in NPPs (Modified form NUREG-0800 Ch. 7.0 [17]).

cyber security characteristics in the hardware and software design during the CD/ES phase to incorporate cyber security design features in the target systems. Also in the CD/ES phase, decisions can be made on which third-party products or commercial off-the-shelf(COTS) items are utilized and how the cyber security characteristics of these items should be assessed. After completion of the design, the hardware is assembled and the software coding is implemented, then they are integrated and tested. At this time, vulnerability scanning and security testing can be performed with the integrated systems. During the SD and CD/ES phases, it is important that system functionality and reliability not be adversely impacted by the inclusion of cyber security measures into the systems. This point should be assessed carefully, once cyber security measures are included.

As both NIST SP800-64 Revision 2 [9] and DG-1249 [14] mention, another important point that should be treated with caution during the CD/ES phase is establishing and maintaining a secure development environment to develop secure software and systems, since cyber attacks may target the development environment, too. For instance, attackers may try to insert malicious codes into the systems under development which will later be installed in NPPs, or at least attempt to collect design information on the critical systems for later cyber attacks. It could be argued that tests for the end products would be enough to achieve acceptable security levels without maintaining a secure development environment. This argument may arise since maintaining a secure development environment can cause higher development expenses. However, tests may not detect all the residual weaknesses or cover all the possible events, which may be triggered by one or combinations of the residual weaknesses. Considering the defense-in-depth concepts during development, maintaining a secure development environment is necessary.

As shown in Fig. 3, to be securely developed and protected from a cyber attack, a target system is placed in a development environment during the CD/ES phase, and in an operational environment after site installation. The development environment here includes workstations, servers, network devices, development tools, and code repositories. Developing I&C systems that are secure up to an acceptable level can be achieved by considering the following two matters: 1) maintaining a secure development environment and 2) developing the proper security features.

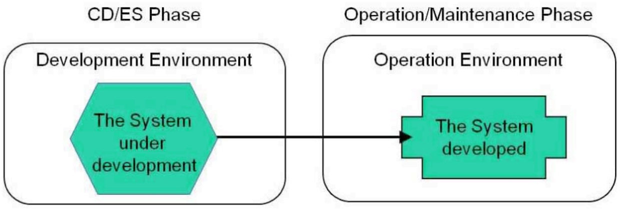

Fig. 3. Target System and Environment in the CD/ES Phase and in the Operation and Maintenance Phase.

3. A METHOD FOR CYBER SECURITY RISK ASSESSMENTS OF NPP I&C

For a practical method for cyber security risk assessments of I&C systems, the activities and considerations necessary for the assessments during the SD and CD/ES phases are developed based on NIST documents for IT systems and ICS, and on literature regarding the nuclear domain. The method consists of the following 6 steps: 1) System Identification and Cyber Security Modeling, 2) Asset and Impact Analysis, 3) Threat Analysis, 4) Vulnerability Analysis, 5) Security Control Design, and 6) Penetration test. Steps 1 through 5 are applicable in the SD phase, and all six steps are required in the CD/ES phase. The depth of analysis in each step corresponds to the design details in the SD or CD/ES phases.

3.1 Step 1: System Identification and Cyber Security Modeling

In this step, the target system for which a cyber security risk assessment is performed should be analyzed to acquire basic information about the system. Digital assets comprising the target system configuration and data flow are identified and simplified to form a model for establishing the appropriate cyber security requirements and design features. RG 5.71 [13] requires an analysis of critical digital assets (CDAs) in the digital environment of NPP sites. Since the system will be integrated with other systems and installed in the site, the location of the system within the site's digital environment, its connection with the other systems, and interfaces with other digital assets of the plant should also be considered during the analysis and modeling of this step.

The following points can be noted in the modeling:

- Any system configuration for redundancy may be simplified as a single system;
- One-to-one direct data communication, analog inpu t/output, and digital input/output can be excluded or simplified;
- The direction and mechanism of the data transfer should be identified;
- Security controls that are already included in the design, such as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), the application of encryption, or data flow control status, should be identified;
- The possible paths from outside or through portable devices used for maintenance should be investigated.

3.2 Step 2: Asset and Impact Analysis

In the risk assessment of IT systems, digital assets are analyzed in consideration of the impact and likelihood of loss in confidentiality, integrity, and availability expected by cyber threats [4]. While in the risk assessment of digital systems in NPPs, according to RG 5.71 [13], digital assets are analyzed to determine whether they are critical digital assets (CDAs) that must be protected from cyber attacks. RG 5.71 [13] describes in detail how to identify CDAs.

It is assumed in this study that the I&C systems listed in Fig. 1 have to be protected from cyber attacks. A defense-in-depth strategy should be applied and maintained in the I&C systems in order to effectively protect CDAs from cyber attacks. For this purpose, security levels should be defined, and an appropriate security level should be assigned to each CDA. NIST SP 800-82 [10] recommends a defense-in-depth strategy including the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities, and other managerial security programs. IAEA technical guidance [15] also recommends a graded approach in which computer systems are grouped into zones. A security level is assigned, and graded protective requirements are applied, to each zone. This guidance introduces the requirements for security levels 1 through 5. Based on levels of connectivity or trust, NEI 04-04 Revision 1 [18] presents a defensive strategy with 5 levels: level 4, control system network; level 3, data acquisition network; level 2, site local area network; level 1, corporate WAN; and level 0, the Internet. RG 5.71 [13] also requires employing defense-in-depth strategies to protect CDAs from cyber attacks, and suggests a defensive architecture configured with five concentric cyber security defensive levels separated by security boundaries, such as firewalls and diodes, at which digital communications are monitored and restricted. Systems requiring the greatest degree of security are located within a greater number of boundaries. The criteria for security levels in these documents are useful when discriminating the security levels at system levels. But some practical rules are still needed for assigning the security levels to the assets or devices inside a system. In this paper, a series of questions is devised for the assignment of security levels of CDAs.

In general, security levels based on the defense-in-depth strategy should be established as a part of the cyber security policy of the target NPP site. The organizations performing SD and CD/ES may follow the security level definition in the cyber security policy of the NPP site. For practicality, the cyber security defensive architecture presented in RG 5.71 was used for the security level definition in this study. When determining the security levels for digital assets of the system, their direct relationship with safety function is assessed, and it is also evaluated whether a loss of the confidentiality, integrity, and availability caused by cyber threats can impact the plant safety or plant trips adversely. With an assumption that the I&C systems in Fig. 1 are not connected to any external networks, security levels 2 through 4 are assigned at this step. The assets or systems at security levels 1 and 0 are excluded in this study. Each security level has the following characteristics:

- Security level 4: This level contains CDAs associated with safety and those important to plant trips. The CDAs at this level should be protected from the malfunctions of devices at the lower levels. Only a one-way data flow is allowed from Level 4 to Level 3. Redundant security controls or mitigation measures regarding vulnerabilities should be applied.
- Security level 3: This level contains the assets or systems that do not impact safety directly, but may cause the plant trips or are connected to other systems at security level 4 through a network. The assets or systems at this level should not receive any data from the devices at security level 2. Security controls or mitigation measures regarding vulnerabilities should be applied.
- Security level 2: This level contains independent assets or systems that do not impact plant safety or trips and are not connected to any network. Security controls or mitigation measures regarding vulnerabilities may be applied in consideration of the impact of cyber threats to an asset or system itself.

Fig. 4 shows this security level classification.

The detailed procedure used to determine security levels for this evaluation consists of the following questions:

Question 1) Does the digital asset or system belong to a safety I&C system?
- if yes, then go to Question 2),
- if no, then go to Question 3).

Question 2) Does the asset or system directly perform the safety function?
- if yes, then assign security level 4,
- if no, then assign security level 3.

Question 3) Does the asset or system impact the plant trips?
- if yes, then go to Question 5),
- if no, then go to Question 4).

Question 4) Does the asset or system have any network connections with any other I&C systems at security level 3?
- if yes, then assign security level 3,
- if no, then assign security level 2.

Question 5) How adversely does improper modification or unauthorized changes made to the data of the asset affect the plant safety or trips?
- if high, then assign security level 4,
- if medium or low, then go to Question 6).

Question 6) How adversely does an unauthorized disclosure of the information affect the plant safety or trips?

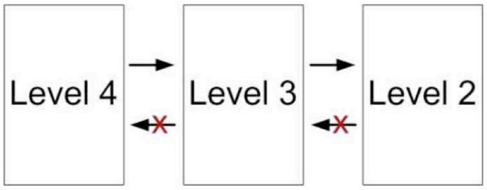

Fig. 4. A simplified Cyber Security Defensive Architecture.

- if high, then assign security level 4,
- if medium or low, then go to Question 7).

Question 7) How adversely does loss of availability of the asset affect the plant safety or trips?
- if high, then assign security level 4,
- if medium or low, then assign security level 3.

Fig. 5 illustrates this procedure.

3.3 Step 3: Threat Analysis

There are differences in the cyber threats to NPP digital I&C systems and to general IT systems. A major reason for this is that NPP I&C systems generally use closed data and communication networks or air-gaps, such that access through the Internet to these systems becomes difficult. However, non-Internet cyber threats are still possible. As in the recent Stuxnet case, NPP I&C systems may be infected by malware designed with codes enabling cyber attacks through portable devices such as laptops and USB flash drives. These systems are comprised of various digital devices and terminal units that are connected through a network. Hence, when a device is compromised or infected by malicious code, the damage can expand to other devices sharing the network.

In this study, cyber attack methods that are possible against NPP I&C systems, rather than aspects of cyber threat sources, are considered as cyber threats. These are sniffing, scanning, spoofing, and denial-of-service (DoS) attacks. The following attack scenario is assumed as possible and harmful to NPP I&C systems in consideration of the network architecture.

(Attack scenario)

Stage 1: Reconnaissance / Foot printing

Attackers study methods to collect information necessary for accessing NPP digital I&C systems. For example, they use Google search, and collect information on the I&C system design. To find detailed design information that cannot be obtained through an Internet search, they try to obtain information on personnel involved in the I&C system research, design, or operation, including e-mail addresses, work sites, jobs, and conference meeting participation. Based on the collected personnel data, they distribute malware specially made to infect PCs of the personnel and collect detailed information. They research the information while collecting it for a few months, select a target system, and make a list of devices related to the system. They may select a system that needs periodic maintenance and can provide attack paths toward the target system. They devise malware to infect the attack paths and distribute it to the maintenance organization by mailing PDF files containing the malware. Once this malware infects any PC of the organization, it can be expanded throughout the whole through use of USBs, internal networks, or file sharing, and finally to the portable devices used for maintenance.

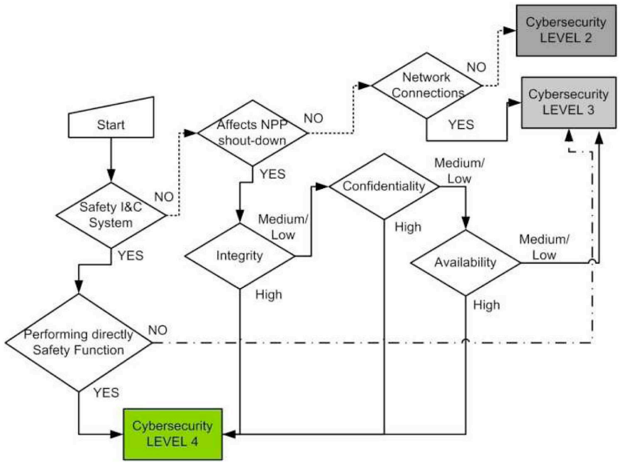

Fig. 5. The Procedure used to Determine Cyber Security Levels.

Stage 2: Scanning

If the malware successfully infects, attackers continue to collect information, arrange attack paths to send the information to their ghost sites, and update the malware as needed, until they obtain the information on the target system. The following sequence of an attacker's activities can be repeated: malware distribution, USB or network infection, maintenance device infection, information scanning, sending it to a device connected with the network, sending the collected information to the ghost sites, managing and analyzing the information, and collecting additional information by updating the malware. With this sequence, attackers can collect information they want, while concealing their intrusion routes. This passive scanning method is less effective than active methods, but can easily conceal an attack route.

Stage 3: Gaining Access

Once malware has infected a system, it can be spread to a connected target system through internal networks. The malware is updated according to the attackers' intention and will contain attack codes made by the attackers after the system analysis. Attackers hold their attacks until they find the best time. They may test information modification or file deletion within a limit that does not affect the system operation.

Stage 4: Maintaining Access

After the scanning stage, attackers maintain a passive access route to gather information continuously for making an easy-to-attack environment. In this situation, the malware does not provide information in real time, but acts as a backdoor. If attackers decide that they have obtained enough information to initiate an attack, they develop codes suitable for an attack exploiting vulnerabilities in the target system.

Stage 5: Attack

By using emails again, attackers try to infect the I&C systems with the malware that includes codes for carrying out an attack. When an attack is started, the malware infection is spread to any other systems that receive data from, or share data with, an infected system, and may incur heavy data traffic. In order to erase an attack track, hackers stop system logging, and perform a back-up of the usual existing files. Possible attack methods can be listed as follows:

- DoS attacks through buffer overflows,
- system manipulation or shut down through elevation of privilege by password attacks,
- unauthorized collection and discharge of system information,
- incurring abnormal system behavior by deleting system processes,
- disruption of a system by deleting system files,
- and modification of system status information through man-in-the-middle (MitM) attacks

Stage 6: Covering Tracks

Attackers rewrite and recover the files that they backed-up previously, and revive system logging functions to cover the attack tracks. By doing this, they can prohibit any changes to the systems from being recorded during the attack.

3.4 Step 4: Vulnerability Analysis

In this analysis, vulnerabilities reported previously should be reviewed first. There are many references for obtaining ICS vulnerabilities [10,19~24]. The NIST National Vulnerability Database (NVD) [23], and especially the Common Vulnerability and Exposures (CVE) system [24] are helpful for collecting this data. The CVE system includes well-known vulnerabilities and mitigation, and provides useful data regarding digital I&C cyber security. When collecting vulnerability data from this database, a keyword search, for example, 'Control,' 'PLC,' 'SCADA,' 'DCS,' or 'Realtime OS (Vxwork),' can be used. The data collected in this way should be evaluated to determine whether the detailed vulnerability information corresponds to the characteristics of I&C systems.

In the SD phase, vulnerability data collection and evaluation should be based on the system architecture, network design, and system design requirements. Considering the previous threat analysis with the attack scenario, security design features that are absent in the current design, but should exist to comply with the definition of assigned security levels, should also be treated as vulnerabilities.

Meanwhile, in the CD/ES phase, vulnerability data collection and evaluation should be based on the hardware and software design specifications, which need more specific vulnerability information for cyber security risk assessments. Reported vulnerabilities specific to the COTS and third-party products to be included in the systems, such as operating systems, application programs, or hardware devices, should be investigated also.

3.5 Step 5: Security Control Design

In this step, security controls that can eliminate or mitigate the vulnerabilities collected and evaluated at the previous step are included in the system design. The possibility and consequence of exploiting the vulnerabilities may be assessed in terms of their importance, in order to decide if they need specific security design features that should be implemented in the system, or can be mitigated by other means such as operational and management security controls based on the utility security program. When selecting the proper security design features, Appendix B (Technical Security Controls) and Appendix C (Operational and Management Security Controls) to RG 5.71 [13] are useful sources of security controls. These controls are developed by incorporating selected controls from NIST SP 800-53 [7], NIST SP 800-82 [10], and other DHS ICS security guidance.

In the SD phase, designers or assessors can select security controls from individual controls of RG 5.71 and include them in their security design requirements. Some security controls in RG 5.71 Appendix B cannot be implemented technically, but are rather handled as operational and management controls. In contrast to this, some controls in RG 5.71 Appendix C contain items that should be implemented in the system design. An IDS for monitoring and auditing is one such example.

In the CD/ES phase, security controls dependent on the system hardware and software should be selected and implemented. Since most security controls in RG 5.71 Appendices B and C are described at the requirement level, they may not be enough for implementation during the CD/ES phase. For detailed techniques regarding how to implement the required technical controls, designers or assessors may refer to guidance such as NIST SP 800-53 [7], NIST SP 800-53A [8], or other IT standards. In both the SD and CD/ES phases, a security control should not be applied if the control adversely impacts plant safety and security functions, or performance. If an adverse affect is expected, alternate controls should be considered.

As mentioned in Section 2 in this paper, since the system is implemented in the CD/ES phase, maintaining the secure development environment is also important. As a way to achieve this, a risk management process consisting of a risk assessment, security control implementation, and monitoring may be applied here. The subject of this risk management is the development environment, which includes workstations, servers, network devices, development tools, and code repositories. The configuration of the development environment may be changed during the system hardware and software implementation. Hence, it is important to keep the system under development in a secure state by managing this changing environment.

3.6 Step 6: Penetration Test

Vulnerability scans and penetration tests can be used for validation of the cyber security design and implementation. A penetration test can be performed after integration of the system in the CD/ES phase as a part of the functional performance tests of the system. As studied in the threat

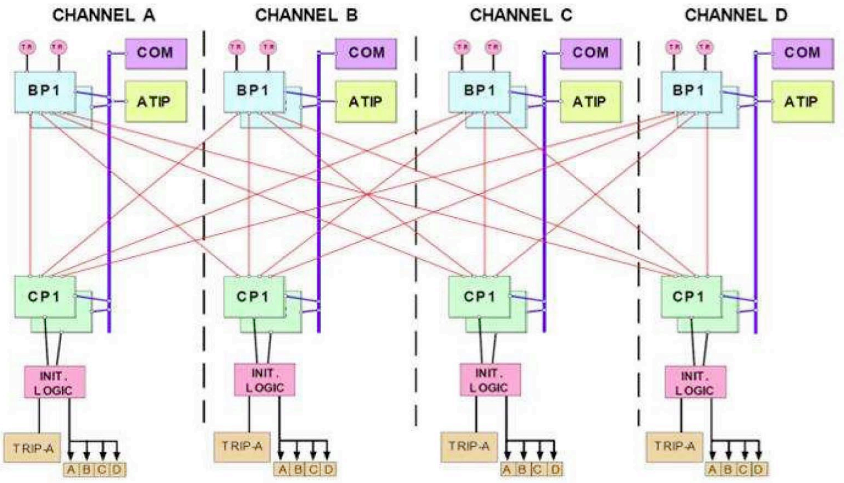

Fig. 6. Configuration of RPS (Adopted from [25]).

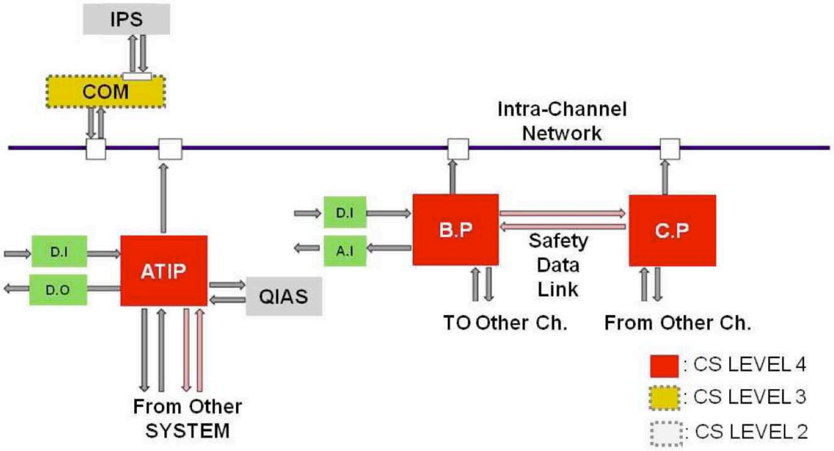

Fig. 7. Cyber Security Model of RPS Single Channel.

analysis, possible attack scenarios can be used for the test. As noted in NIST 800-82 [10], there can be a potential for a disruption of the system when simulated attacks are conducted. It is recommended to perform this test on a test bed or on extra products.

4. RESULTS

A risk assessment for a digital reactor protection system (RPS) was conducted for an example application of the method described in Section 3. In this study, design documents from only the SD phase were used. An assessment for the CD/ES phase and a penetration test were not performed. The PLC-based RPS has four channels, each of which includes a bistable processor (BP), a coincidence processor (CP), an automatic test and interface processor (ATIP), and a cabinet operator module (COM). Fig. 6 shows this RPS system.

Table 1. Security Levels Assigned to the RPS Components.

RPS components	Assigned Security Level
BP	4
CP	4
COM	3
ATIP	4
Intra-Channel Network	3

The four channels were simplified into one channel as shown in Fig. 7. The network configuration and data flow in this system were analyzed and are illustrated in Fig. 7.

Using the results from the impact analysis described in step 2 of Section 3, ATIP, BP, and CP are assigned to Security Level 4, but COM is assigned to Security Level 3, as this does not perform a safety function directly. Table 1 lists the security levels assigned to the components.

Table 2. The Results of Risk Assessments of the RPS.

	BP	CP	ATIP	COM	Intra-Channel Network
Network Input	DI/BP	BP	BP/CP/D.I	BP/CP/ATIP/Intra-Channel Network	BP/CP/COM/ATIP
Network Output	CP/Intra-Channel Network	BP/Intra-Channel Network	QIAS/D.O/ BP/CP/ Intra-Channel Network	IPS(Information Processing System)	COM
Security Controls	none	none	none	none	none
Blocking of Data traffic by the security level difference	data receipt from Intra-Channel Network	data receipt from Intra-Channel Network	data receipt from Intra-Channel Network	-	data transmission to BP/CP/ATIP
System dependency	direct communication with CP	direct communication with BP	data transmission to BP & CP/ data transmission to QIAS (Qualified Informa-tion and Alarm System)	data receipt from BP, CP, and ATIP	Network connection with BP, CP, ATIP, and COM
Access by maintenance work	yes	yes	yes	yes	-
Vulnerabilities[1)]	V1/V2/V3	V1/V2/V3	V1/V2/V3	V1/V2/V3/V4/V5/ V6/V7	V7
Impact to	CP/Intra-Channel Network	BP/Intra-Channel Network	BP/CP/QIAS	IPS	BP/CP/ATIP/COM
Risk range	Local	Local	Local	Local	Local
Possible Mitigation Measures[2)]	M1/M3/M4/M6	M1/M3/M4/M6	M1/M3/M4/M6	M1/M2/M3/M6/M7	M4/M5/M6
Application of the measures by considering the security levels	More than two among M1/M3/M4/M6	More than two among M1/M3/M4/M6	More than two among M1/M3/M4/M6	One of M1/M2/M3/M6/M7	One of M4/M5/M6

Note 1) Vulnerabilities
V1:DoS attacks and malware execution on systems communicating with a system infected by maintenance works
V2:System shut-down by malware infected by maintenance works
V3:Data modification by malware infected by maintenance works
V4:Seizure of system authority due to vulnerabilities residing in the OS
V5:DoS attacks and malware execution on other systems by vulnerabilities residing in the system
V6:Eavesdropping, data forgery, and attacks by malware
V7:Data modification by using known vulnerabilities of standard communication protocols
2) Mitigation measures
M1:Establishment of managing infection detection systems for PC, USB, and external storage media used for PLC maintenance works
M2:Establishment of device authentication policies
M3:Monitoring of running services: White list generation by checking running processes, and detection and blocking of unnecessary services
M4:Network monitoring
M5:Firewalls/IPS/IDS
M6:Data encryption
M7:Vulnerability patches

The system does not have any cyber security controls. Assuming that cyber attacks through portable devices used for maintenance may occur as described in the attack scenario of step 3 in Section 3, vulnerabilities are assessed for the system. Also, mitigation measures considering the security levels are devised. Table 2 shows the results.

5. CONCLUSION

The applications of computers and communication system and network technologies in NPPs have expanded recently. This application of digital technologies in NPP I&C systems brings about cyber security concerns similar to other critical infrastructures. Cyber security risk assessments for the digital I&C systems of NPPs become more crucial in the development of new systems, and also in the operation of existing systems. Although NPP I&C systems are similar to ICS, NPP I&C systems have features different from ICS in terms of the architecture and the functions for satisfying the safety requirements, which need different practices in the application of cyber security risk assessment methods.

In this paper, the characteristics of NPP I&C systems are described, and the considerations needed when conducting cyber security activities during the SD and CD/ES phases within the lifecycle process of the I&C systems are discussed. It is claimed that 1) maintaining a secure development environment and 2) developing the proper security features of the I&C systems are two important goals in cyber security designs or assessments. For a method for cyber security risk assessments of the I&C systems, activities and considerations important to the assessments during the SD and CD/ES phases are presented for the following 6 steps: 1) System Identification and Cyber Security Modeling, 2) Asset and Impact Analysis, 3) Threat Analysis, 4) Vulnerability Analysis, 5) Security Control Design, and 6) Penetration test. The method was applied to cyber security risk assessments of a digital reactor protection system. As a result from this application, the vulnerabilities of the system, and security measures to mitigate them, were obtained. It is concluded that the proposed method provides a useful and practical way for the risk assessment of NPP digital I&C systems. For further studies, applications of the method in the systems developed in the CD/ES phase, including non-safety systems, and a penetration test with a test-bed for the systems, can be suggested.

ACKNOWLEDGEMENT

This work was supported by the Nuclear Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant, funded by the Korea government Ministry of Knowledge Economy(No. 2010161010001E).

REFERENCES

[1] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements, October 2005.

[2] ISO/IEC 27002:2005, Information technology - Code of practice for information security management, June 2005.

[3] ISO/IEC TR 19791:2010(E), Information technology - Security techniques - Security assessment of operational systems, April 2010.

[4] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.

[5] NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010.

[6] NIST Special Publication 800-39, Managing Information Security Risk, March 2011.

[7] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, August 2009.

[8] NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems, 2010.

[9] NIST Special Publication 800-64 Revision 2, Security Considerations in the System Development Life Cycle, October 2008.

[10] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, June 2011.

[11] Regulatory Guide 1.152 revision 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, January 2006.

[12] 10 CFR Part 73.54, Protection of Digital Computer and Communication Systems and Networks, U.S. Nuclear Regulatory Commission, Washington, DC.

[13] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.

[14] Draft Regulatory Guide DG-1249, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, June 2010.

[15] Draft IAEA Technical Guidance, Computer Security at Nuclear Facilities, International Atomic Energy Agency, 2010.

[16] IEEE Standard 7-4.3.2-2010, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, August 2, 2010.

[17] NRC Standard Review Plan NUREG-0800 Chapter 7.0 Instrumentation and Controls – Overview of Review Process, Revision 6, May 2010.

[18] NEI 04-04 Revision 1, Cyber Security Program for Power Reactors, Nuclear Energy Institute, November 18, 2005.

[19] Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems, GAO-04-354, United States General Accounting Office, March 2004.

[20] Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments, Department of Homeland Security, July 2009.

[21] Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies, Department of Homeland Security, October 2009.

[22] INL/EXT-10-18381, NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, Idaho National Laboratory Idaho Falls, Idaho 83415, May 2010.

[23] NIST National Vulnerability Database version 2.2, http://nvd.nist.gov/home.cfm.

[24] Common Vulnerability and Exposures (CVE), http://cve.mitre.org.

[25] Dong-Young Lee, Jong-Gyun Choi, and Joon Lyou, A Safety Assessment Methodology for a Digital Reactor Protection System, International Journal of Control, Automation, and Systems, vol. 4, no. 1, pp. 105-112, February 2006.