http://dx.doi.org/10.5516/NET.04.2012.091

AN ANALYSIS OF TECHNICAL SECURITY CONTROL REQUIREMENTS FOR DIGITAL I&C SYSTEMS IN NUCLEAR POWER PLANTS

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

Received December 20, 2012
Accepted for Publication March 15, 2013

Instrumentation and control systems in nuclear power plants have been digitalized for the purpose of maintenance and precise operation. This digitalization, however, brings out issues related to cyber security. In the most recent past, international standard organizations, regulatory institutes, and research institutes have performed a number of studies addressing these systems cyber security.. In order to provide information helpful to the system designers in their application of cyber security for the systems, this paper presents methods and considerations to define attack vectors in a target system, to review and select the requirements in the Regulatory Guide 5.71, and to integrate the results to identify applicable technical security control requirements. In this study, attack vectors are analyzed through the vulnerability analyses and penetration tests with a simplified safety system, and the elements of critical digital assets acting as attack vectors are identified. Among the security control requirements listed in Appendices B and C to Regulatory Guide 5.71, those that should be implemented into the systems are selected and classified in groups of technical security control requirements using the results of the attack vector analysis. For the attack vector elements of critical digital assets, all the technical security control requirements are evaluated to determine whether they are applicable and effective, and considerations in this evaluation are also discussed. The technical security control requirements in three important categories of access control, monitoring and logging, and encryption are derived and grouped according to the elements of attack vectors as results for the sample safety system.

KEYWORDS : Instrumentation and Control Systems, Nuclear Power Plant, Cyber Security, Technical Security Controls, Critical Digital Assets

1. INTRODUCTION

Instrumentation and control (I&C) systems, which are important for the safety and performance of nuclear power plants (NPPs), have been digitalized for the purpose of the maintenance and precise operation of plants[1]. This digitalization, however, brings out issues related to cyber security. In particular, the cases of damage to national critical infrastructures, including nuclear facilities, owing to cyber attacks that passed over air gaps between the facility and the outside, have raised immediate needs for cyber security measures. As a response to this, many nuclear industries have isolated their I&C systems from the networks connected to the internet.

For the cyber security of NPP I&C systems, many regulatory requirement documents[2,3,4], the IAEA guide NSS-17[5], the IEEE Standard 7-4.3.2 [6] were already published, while the IEC standards are undergoing a preparatory phase. There are many documents addressing cyber security of industrial control systems (ICSs) as well as supervisory control and data acquisition (SCADA) systems [7~13]. Many of these documents focus on network security, since these systems commonly have connections with corporate business networks. In the cyber security domain, NPP I&C systems tend to be addressed from the viewpoint of ICS and SCADA systems. NPP I&C systems, however, have characteristics different from ICS and SCADA systems [14~16]., Safety regulations for NPP I&C systems require limitations in data communications between safety systems and non-safety systems, defense-in-depth and diversity, and rigorous hardware and software qualification including verification and validation, safety analysis, and configuration management. These safety regulation requirements already address some requirements for cyber security. Hence, NPP I&C system designers may encounter difficulties when trying to satisfy the newly issued cyber security requirements, while identifying additional design features and where and how to apply those to their systems.

Methods for cyber security risk and vulnerability assessments, have been studied recently by international standard organizations, regualtory institutes, and research institutes. Among these, the National Institute of Standards and Technology (NIST) risk assessment method, proposed in NIST 800-82[9], NIST 800-53[17] and NIST 800-30[18], can be considered as a representative case. Overall system characteristics including cyber threat cases are analyzed, and the possibility of malicious behaviour exploiting system vulnerabilities is then evaluated in this method. Based on assessments of availability, integrity, and confidentiality, especially through likelihood determination and impact analyses, risks owing to system vulnerabilities are rated at three levels of severity. For the IT systems, confidentiality and integrity are addressed more importantly than availability in risk assessments. When applying this method to the I&C systems in NPPs, the quantification or rating of risks may be inappropriate and hard to validate, since how and to what extent risks affect the system safety and availability cannot be assessed simply as in the IT systems.

The U.S. NRC published the Regulatory Guide 5.71 (RG 5.71)[3] for the cyber security of new and operating NPPs, and the IAEA issued NSS-17[5] as a technical guidance for computer security at nuclear facilities. These documents provide general approaches and guidance for the cyber security of I&C systems, including cyber security plans and programs, methods for cyber security assessments, and a comprehensive set of security controls. However, there are still difficulties from the system designer's point of view when it comes to decision making about which technical controls to which parts of the target I&C systems need to be applied. Practical examples for the application of technical security controls have not been available to the system designers, leading to difficulties when defining appropriate security control requirements and security design features for the individual I&C systems.

In a previous study [19], a cyber security risk assessment method for the design and development of I&C systems in NPPs was proposed. The method describes an assessment process specified in detail for NPP I&C systems, which consists of a series of steps, including system identification, security modeling, analysis of effects on critical digital assets (CDAs), threat analysis, vunlerability analysis, security control design, and penetration tests. Through this process, potential system vulnerabilities and protection measures can be identified. This approach, based on the basic understanding of NPP I&C systems, presents a way to define cyber security measures that are appropriate for a target I&C system.

This paper follows the assessment process introduced in the previous study, and addresses further studies related to an analysis of vulnerability and to the methods for the selecttion and application of the cyber security requirements and technical security controls presented in RG 5.71. In order to provide information helpful for system designers in the application of cyber security requirements to their systems, this paper describes methods and considerations to define attack vectors in a target system, to review and select the requirements in the RG 5.71, and to integrate the results to identify applicable technical security controls.

2. METHODS

The RG 5.71 provides the most complete set of requirements for NPP I&C system designers to identify security design features and apply them to their I&C systems. RG 5.71 addresses various cyber security assessment activities and presents a series of requirements for security controls. To determine which control requirements are applied to which part of the system, the system designers should analyze the systems and perform cyber security assessment activities in accordance with the guidance in RG 5.71. However, example cases of these activities, from which they can obtain information on how to conduct the activities, are not yet available publicly. In this study, to provide detailed guidance helpful to system designers, analyses on attack vectors were performed, and cyber security requirements applicable to specific CDAs in I&C systems were identified.

2.1 Analysis of Attack Vectors

"An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element[20]." Attack vectors on an I&C system may include attack entry points for code injection or other cyber attacks, such as CDAs, networks, and portable devices or media that can be attached to CDAs, as well as their vulnerabilities. Attack vectors can be identified through analyses of system architecture, properties of CDAs, and possible cyber threats to the system, together with penetration tests. As the first step to narrow down the applicable cyber security requirements, the following activities are performed in this study:

1) Analysis of an I&C system architecture at the highest conceptual level;
2) Modeling of a target system from a cyber security point of view;
3) Security level assignments to the CDAs of a target system;
4) Analysis of the elements of attack vectors based on the cyber security model of the system;
5) Investigation of the known vulnerabilties residing in the CDAs and penetration tests to identify potential malicious activities.

2.1.1 Analysis of an I&C System Architecture

ICSs are connected in general to off-site corporate business systems or the Internet. For the cyber security of

network connections bewteen the ICS and the outer systems, many NIST documents, including NIST SP800-82 and NIST SP 800-53, describe the measures to be applied. In Korean NPPs, I&C systems have been isolated from the outside after the Stuxnet incident. This study was performed based on an assumption that the I&C systems already maintain air gaps.

At the highest conceptual level, NPP I&C systems can be categorized by safety systems and non-safety systems as shown in Fig. 1. Fig. 1 also illustrates the network connections between the two systems. Safety systems can transmit data to non-safety systems, but a data transmission in the reverse direction is not allowed by nuclear safety regulations and requirements. Defense-in-depth requirements in RG 5.71 specify very similar conditions in which data transmission from CDAs at lower security levels to those at higher security levels are not recommended. These security requirements can be met naturally by assigning security levels to CDAs in accordance with their safety classes.

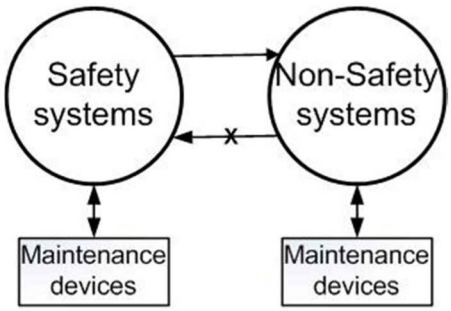

Fig. 1. Conceptual Data Flow Architecture of NPP I&C Systems (Redrawn from Ref. [16])

Because of the isolated network architecture, it is hard to compromise CDAs of I&C systems from the outside by the use of active cyber attack methods. During NPP maintenance and test activities, however, external digital devices or media can be connected to the CDAs and may provide a path to passive cyber attacks such as advanced persistent threats (APTs). For this reason, digital devices for maintenance, calibration, and tests of I&C systems, should be included in the scope of cyber security assessments during the operation phase of plants.

2.1.2 Security Modeling of Target Systems

Security modeling is a way to simplify the functions, roles, service types, and data communications of target systems for an effective security requirement analysis. In this modeling, as noted in our previous paper [19], any system configuration for redundancy may be simplified as a single train. Signal lines from sensors, analog input/output, digital input/output, and one-to-one direct data communication can be excluded or simplified. All kinds of CDAs and data transfer directions and mechanisms within the target systems, should be identified and included in the model. After the analysis of security requirements and technical security controls with this security model, the resultant security controls can be applied to the original systems at the locations corresponding to those in the model.

In this study, a plant protection system (PPS) was selected as an example target system. The PPS, based on programmable logic controllers (PLCs), has four channels. For a security model of this system, the four channels were simplified into one channel and analog lines are excluded as shown in Fig. 2. In Fig. 2, the bistable processor (BP), coincidence processor (CP), and interface and test processor (ITP) are safety-grade PLCs, and the maintenance and test

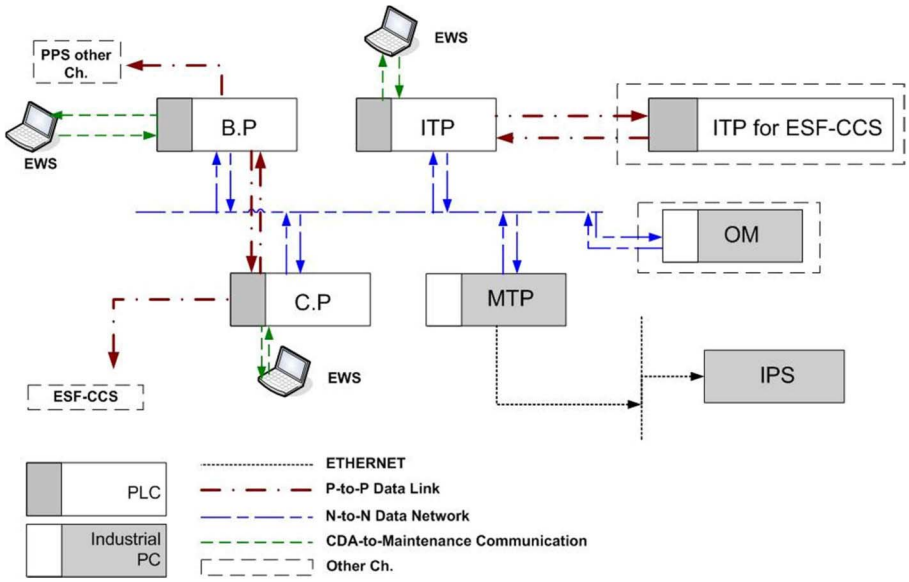

Fig. 2. Data Flow Model of PPS for Cyber Security Analysis

panel (MTP) is an industrial PC. The information processing system (IPS) is a server computer system, and the operator module (OM) is a safety-grade industrial PC installed in the main control room.

The BP transfers signals to the PLCs of other PPS channels, and similarly, the CP does so to the PLCs of another safety system (ESF-CCS: Engineered Safety Features-Component Control System). This communication in BP and CP is one-directional. For data transmission within the same channel, N-to-N type intra-channel network communications are used. Also, the BP and CP transfer information to each other directly through a P-to-P type safety data link. The MTP collects some information from the PLCs through the intra-channel network, then transfers these to the IPS through a one-directional Ethernet network and to the OM through the intra-channel network. For the maintenance and tests of PLCs, a laptop computer (EWS: Enginnering Work Station) may be connected to each PLC.

Table 1 lists data transmission networks and their types used in the PPS.

2.1.3 Security Level Assignments

Security level assignments are needed to apply a defense-in-depth strategy to a cyber security design of I&C systems to effectively protect CDAs from cyber attacks. The NIST SP 800-53[17] and IAEA technical guidance[5] recommend a graded approach in which security controls in several grades are applied to CDAs according to their assigned security levels. In contrast, in the NEI 04-04 Revision 1 [21] and RG 5.71 [3], security levels in the defense-in-depth strategy define only the limitations of data transmission, but differentiation of the grades of security controls is not addressed. These two documents state that CDAs for safety, important-to-safety, security, or control functions are assigned to security level 4, and CDAs for data acquisition functions to security level 3. In agreement with this, CDAs or systems related to plant safety or plant shutdown are assigned to security level 4 as shown in Fig. 3 in this study. CDAs or systems not related to plant shutdown, but connected to CDAs at level 4 through networks, are allocated to security level 3. Most NPP I&C systems are allocated to either security level 4 or security level 3.

Based on this argument, for the sample PPS, the security levels of the CDAs in Fig. 2 are assigned as in Table 2.

2.1.4. Analysis of the Elements of Attack Vectors

This analysis identified CDAs, which can be infected by malware from outside of the system, or at which any malicious activities can occur. It then estimates how the infection or the activities become possible. It is important in this analysis that all digital equipment and media for the maintenance and tests should be addressed, and users

Table 1. Network Types used for the PPS

Data transmission	Network type
BP to the PLCs in other PPS channels	P to P (data diodes)
BP to CP	P to P (data diodes)
CP to ESF-CCS	P to P (data diodes)
BP, CP, ITP to EWS	Serial
BP, CP, ITP, MTP to Intra-channel Network	N to N
MTP to IPS	Ethernet
OM to Intra-channel Network	N to N

Table 2. Security Levels Assigned to the PPS Components

CDA	Assigned Security Level
BP	4
CP	4
ITP	4
MTP	4
OM	4
IPS	3
EWS	4

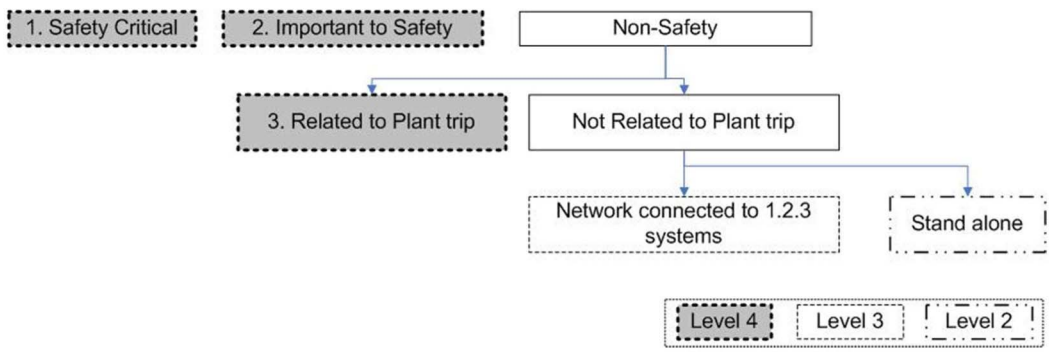

Fig. 3. Security Level Assignment Scheme

of them and corresponding task procedures should be reviewed.

In Fig. 3, for the sample PPS, safety grade PLCs such as BP, CP, and ITP are at the highest security level., Based on the assumption in this study that the safety PLCs are not infected during manufacturing and delivering phases, only one track path from the outside can be expected through the EWS being connected to the PLCs during the maintenance and tests of them,. Since the EWS communicates with each of the PLCs, the EWS can be an entry point of cyber attacks. If the EWS accept the use of external media such as USB flash drives, the external media can become additional attack entry points. Therefore, it is evident that an attack vector to a PLC can be formed through the EWS.

At least two types of cyber attacks can be anticipated here. One affects a PLC directly causing it to malfunction, another installs malware into a PLC to expand infections to other CDAs in the system. The latter is much more elaborate, and may affect not only the infected CDA but also the whole system. Additionally, it can be anticipated from Fig. 3 that some manipulated information from the EWS can be transmitted to the BP and other PLCs or the MTP, and at last to IPS through the information networks. Information on the IPS will be displayed to the operators in the main control room so that they may judge the plant state incorrectly.

Based on this discussion of potential malicious attacks, the following major attack entry points, providing a path to attack vectors, can be identified in general I&C systems:

- Network: Malware or malicious activities can be expanded to CDAs through networks;
- User: Users may access CDAs for operation, maintenance, and tests. Since users can conduct malicious activities directly to CDAs, suitable security controls for their access, authentication, and accountability will be necessary;
- External Device: The external devices or systems used for the maintenance and tests are subjects for the analysis. The external devices connected to CDAs can modify or delete the programs residing in the CDAs. Since external devices, for example, laptops for the maintenance of I&C system are portable in general, they should be treated as critical elements providing attack vectors; and
- External Media: External media are the elements that can be connected to CDAs directly or indirectly through external devices. External media are able to access to industrial PCs or other computing devices to transfer and execute malicious code to modify system software or cause the systems malfunction. They can also be used to modify or delete the installed programs, or install abormal code. According to the capability to read and write, external media are categorized into read and write media, such as USB flash drives and hard disk drives, and read-only media, such as compact discs and DVDs.

In accordance with these elements of attack entry points, the following attack vectors affecing a target CDA can be defined;

- Other CDAs to CDA: This implies that other CDAs connected to a target CDA and infected by malware or affected by malicious activities can expand the infection or malicious activities to the target CDA;
- User to CDA: A hacker can access and attack a target CDA directly;
- External Device to CDA: An external device is connected to a target CDA, and hence it can infect malware or conduct malicious activities to the CDA;
- External Media to CDA: External media can access a target CDA, and hence they can infect malware or conduct malicious activities to the CDA;
- User to CDA through External Device: A hacker can conduct cyber attacks to a target CDA by accessing an external device; and
- External Media to CDA through External Device: A hacker could use external media to attack a target CDA through an external device to which the external media are connected.

Fig. 4 shows the elements of attack vectors discussed here.

2.1.5 Investigation of known Vulnerabilties and Penetration Tests

Based on the analysis of attack vectors, a vulnerability analysis and penetration tests are performed to identify the malicious activities that can compromise the target system. To identify the kind of cyber attacks that are possible for a target system, vulnerabilities for the CDAs composing a target system should first be investigated. Vulnerabilities already residing in systems can be exploited easily by hackers. Hence, it is important to investigate the known vulerabilities and determine their exploitability. Results from this analysis can be ascertained by performing penetration tests with a test-bed.

As noted in NIST 800-82 [22], there can be a potential for a disruption of the system when penetration tests are conducted. In this study, a test-bed consisting of one set of BP, CP, ITP, MTP, and OM is constructed for the penetration tests of the sample PPS. Analyses, based on this test-bed, are performed with regard to what kinds of cyber attacks are possible and which measures can protect CDAs

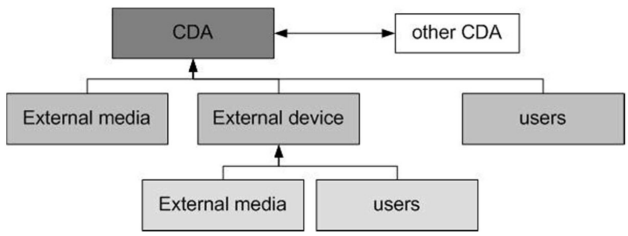

Fig. 4. Elements of Attack Vectors to a Target CDA

against the attacks, by investigating the known vulnerabilities, the types of attacks exploiting the vulnerabilities, and their impact to the CDAs or on the system.

2.1.5.1 Analysis of known Vulnerabilities

The Common Vulnerability and Exposures (CVE) [23] are helpful in collecting the known vulnerabilities. The CVEcontains detailed information about the types of vulnerabilities, as well as the kinds of attack and loss types possible due to these vulnerabilities. It also provides web site information which is the source of detailed information. The information collected through the CVE, it is possible to analyze which systems may suffer from what kind of damages, and how high the risk will be. The information from this analysis is important to grasp the possibility of exploiting vulnerabilities and the level of resultant damages before the penetration tests.

Vulnerabilities for the operating system (OS), applications, and network of sample PPS were searched at the CVE, and those for only the OS were found. Table 3 presents the vulnerabilities searched for the OS in the test-bed for PPS and their impact. With the impact data in this table, it is possible to identify of the possible kinds of cyber attacks, in turn, this identification notifies the types of attacks that may be exercised during the penetration testings to verify the impact. In Table 3, "Local Exploit" in the column "Type" means that the attacks should take place at the installed location of PPS to compromise the system with those in "Impact."

The results from these analyses may be used to define technical security measures to eliminate or restirict the known vulnerabilities. In relation to these measures, the requirements in C.7 Defense-in-Depth of the RG 5.71, "devices are free from known malicious code," and in C. 12.5 Developer Security Testing, "known insecure software components or libraries" should be considered.

2.1.5.2 Vulnerability Analysis of Maintenance Devices

It is also important to determine if the CDAs have the vulnerabilities exploitable by cyber attacks from the EWS, by identifying and analyzing local exploit vulnerabilities for attacking inside the system and their potential impact. It should be considered that a code for attacking inside the system from the EWS can be developed to exploit the known vulnerabilities of CDAs.

It is necessary to analyze the vulnerabilities of all digital assets that can affect the CDAs in the development environment as well as in a target system. Maintenance devices such as EWS are identified in section 2.1.4 as major attack entry points. During the development phase, the EWS is usually put in the same environment as the target system, and also has a possibility to be handled with less caution than the target system. It is important to identify and respond to potential threats from those devices. In detail, the possible threats and their effects from maintenance devices should be analyzed in consideration of the problems that may exist in those devices, such as 'Insecure network /Internet access,' 'Insecure movable device use,' and 'Insecure configuration of System.' Measures against cyber threats from the maintenance devices should be defined by performing the identification of types of threats to target CDAs, conditions enabling the threats and the consequences of the threats to take place,.

In this study for the sample PPS, it is assumed that the EWS for PPS PLCs is managed under a flexible security

Table 3. Target System Vulnerabilities Searched from the CVE

Operating System	Category	Vulnerabilities	Type	Impact
QNX Neutrino RTOS 6.x	Not-Fix	QNX insecure permissions	Local Exploit	Privilege Escalation DoS
		QNX RTOS "inputtrap" Information Disclosure Vulnerability	Local Exploit	Exposure of sensitive information
		QNX RTOS "crrtrap" Privilege Escalation Vulnerability	Local Exploit	Privilege Escalation
		QNX reveals content of clipboard	Local Exploit	Exposure of sensitive information
		QNX Neutrino RTOS Multiple Privilege Escalation Vulnerabilities	Local Exploit	Privilege Escalation
		QNX RTOS "dhcp.client" File Permission Weakness	Local Exploit	DoS
		QNX RTOS local DoS	Local Exploit	DoS
		QNX RTOS phgrafx Buffer Overflow Vulnerability	Local Exploit	Privilege Escalation
		QNX RTOS FTP Client "QUOTE" Command Format String Vulnerability	Local Exploit	Privilege Escalatio
		QNX privilege escalation	Local Exploit	Privilege Escalation
Private OS	-	N/A	-	-

environment, and has the same configuration as general IT devices that may be connected intermittently to outside networks. Possible threats under the specific conditions of the EWS and their results are identified. Table 4 shows the results of this identification performed with the EWS for PPS PLCs.

An 'Insecure network' in this table can be treated with the requirements for B.1 Access Control, especially B.1.18 Insecure and Rogue Connections of RG 5.71 Appendix B, and 'insecure movable device use' with those in C.7 Defense-in-Depth and B.1.16 Open/Insecure Protocol Restrictions.

2.1.5.3 Analysis of Malicious Activities through Penetration Tests

Malicious activities that can take place in the CDAs and systems and their consequences can be evaluated in detail through penetration tests, which are performed on a test-bed based on the information from the analyses of attack vectors and vulnerabilities. Penetration tests, in this case, are to confirm the results from the previous analyses and verify the consequences of malicious activities. The results from these tests will help to define suitable security measures to protect the system from the malicious activities. Penetration tests can also be performed after the implementation of technical security controls into a target system to verify their effectiveness.

For the penetration tests with the test-bed, two attack vectors are defined, based on the discussion in section 2.1.4 and the vulnerability analyses in sections 2.1.5.2 and 2.1.5.3. Attack vector 1 starting from the EWS to a PLC and further to other CDAs in the system, and attack vector 2 from users to the MTP and to the sysem are defined. Fig. 5 shows these attack vectors in the test-bed. In the penetration tests, to identify malicious activities and their impact on the CDAs and throughout the whole system, conditions such as malware implementation, successful remote exploitation, and non-validated code execution are tested and possible malicious activities under these conditions are investigated.

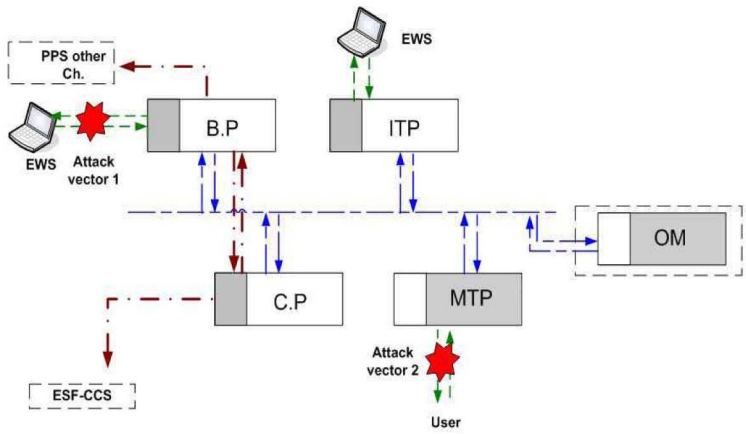

Fig. 5. Attack Vectors on the PPS Test-bed.

Table 4. Vulnerability Assessment Results for the EWS

Entry	Condition	Threats	Results
EWS	Insecure network /Internet Access	Client Side Attack by XSS, Pishing, Java Deserialization	Reverse Shell execution
			Malware Implementation
			System Compromise
	Insecure movable device use	Malware Attack	System Compromise
	Misconfigured network	Malware Attack	Malware implementation
			System Compromise
		Network Attack from other insecure Hosts	System Compromise
	Insecure configuration of system	Firewall Bypass	Vulnerability Exploit
			Malware Implementation

As the results of penetration tests, Table 5 shows possible malicious activities and the conditions required for initiating the malicious activities. Security measures eliminating the conditions can be identified and applied in order for the corresponding malicious activities not to take place.

Technical security control requirements in accordance with the malicious activities identified in this way can be treated with the requirements in the RG 5.71. In detail, B.3.4 Denial of Service Protection for 'DoS attack,' B.5.2 Host Intrusion Detection System for 'illegal task create,' and B.1.4 Information Flow Enforcement for 'packet modification' should be considered.

2.2 Analysis of Technical Security Control Requirements in RG 5.71

The RG 5.71 contains a comprehensive set of security control requirements that should be applied to NPP I&C systems to protect them against cyber attacks. The RG 5.71 Appendix B contains°∞Technical Security Controls," and Appendix C lists "Operational and Management Security Controls." Appendix B lists requirements that are not considered as technical control requirements, and Appendix C includes some requirements that should be regarded as technical control requirements designed and implemented during the development of I&C systems. Therefore, it is necessary to review the requirements carefully for their applicability to the I&C systems.

2.2.1 Selection of Technical Control Requirements

Some parts of the technical security control requirements address security policy or procedures, which are not necessary for the design of security features to be implemented into the I&C systems. These will be excluded in this review. Also, the requirements that can be applicable to a general IT environment, but not appropriate to NPP I&C systems (e.g., Automated Marking), and those that are already incorporated into the I&C system design inherently as a part of development activities of safety systems, e.g., system verification and validation, can also be excluded. During this review, every sentence in the requirement descriptions should be evaluated, and in some cases, even a sentence may be separated into several items.

These criteria are also applicable when reviewing the requirements in Appendix C. There are requirements that can be regarded as technical security control requirements, for example, Malicious Code Protection, Monitoring Tools and Techniques, Information Input Restrictions, Maintenance Tools, Error Handling, Defense-in-Depth, Recovery and Reconstitution, Configuration Settings, Component Inventory, and Developer Security Testing.

Table 6 below lists examples that are excluded or limitted in its application for a review of the requirements in Appendix B, and table 7 presents example requirements in Appendix C which can be regarded as technical security control requirements.

2.2.2 Use of Vulnerability Analyses and Penetration Tests

The requirements selected as in the previous section should be evaluated individually for their applicability and effects on the target I&C systems. If all the requirements are incorporated into the systems, there must be adverse effects on the function or performance of systems. Also, individual technical security control requirements that are selected to achieve the security of a CDA may result in duplication for the same security purpose. There is a possiblity that the cost will increase enormously if security control requirements derived from service-oriented IT systems are applied to safety and reliability centered NPP I&C systems. For example, if security controls, such as a real-time access control for device-to-device identification, authentication, authorization, and data encryption, may be

Table 5. Analysis of Malicious Activities of the Potential Attack Vectors

Potential attack vector	Conditions	Malicious activities
Attack vector 1	Malware Implementation Successful, Reverse Shell execution	DoS attack Network Scan (port, service etc) Network Sniffing Packet Modification Local Exploit to Escalate Privilege Improper Command Execution
Attack vector 2	Malware Implementation Successful	Local Exploit to Escalate Privilege DoS attack through Serial Key Logging Illegal Command Execution through Serials
	Non-validate code Exploit Vulnerability Exploit	Illegal Task Create Processor Resource Exhaust Attack

Table 6. Example Requirements in Appendix B not Considered as Technical Control Requirements

Titles of Control Requirements	Requirements	Reason for Exclusion or Limitation in Application
1. Account Management	Managing and documenting CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts	"managing and documenting CDA accounts" are related to operation and management controls
2. Account Management	Reviewing and documenting CDA accounts at a maximum interval consistent with the most recent version of Nuclear Energy Institute (NEI) 03-12 [24], "Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan," endorsed by the U.S. Nuclear Regulatory Commission	"reviewing and documenting CDA accounts" are related to operation and management controls
3. Unsuccessful Login Attempts	Real time alerting of designated personnel with the security expertise for the CDA through alarms when the number of defined consecutive invalid access attempts is exceeded.	Limitted application to safety systems. Applicable to the systems that need login. Seek alternative controls if real time alerting is impossible.
4. Auditable Events	Implementing alternative controls and documenting the justification for alternative controls and countermeasures for situations in which a CDA cannot support the use of automated mechanisms to generate audit records and employs non-automated mechanisms and procedures	Automated auditable event logging is important. It is better not to take alternatives easy.
5. Secure Name/Address Resolution Service (Authoritative/Trusted Source)	Configuring systems that provide name/address resolution to CDAs, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.	Normal practice during system design or implementation
6. Removal of Unnecessary Services and Programs	Documents all required applications, utilities, system services, scripts, configuration files, databases, and other software and the appropriate configurations, including revisions or patch levels, for each of the computer systems associated with the CDAs.	Normal practice during system design or implementation

Table 7. Example Requirements in Appendix C to be Treated as Technical Controls

Titles of Control Requirements	Requirements	Reason for Inclusion
1. Error Handling	Error conditions are identified, Error messages are revealed only to authorized personnel.	Should be implemented into the system
2. Defense-in-Depth	Omitted	Should be considered during system design.
3. Incident Monitoring	[Licensee/Applicant] tracks and documents security incidents on an ongoing basis using automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	Automated mechanisms should be implemented into the system.
4. CDA Backups	Backing up CDAs at an interval identified for the CDA or based on trigger events, protecting system backup information from unauthorized modification	Function for "protecting system backup information" may be implemented into the system.
5. Developer Security Testing	The static source code vulnerability analysis performed to inspect the developed code for potential security defects, poor programming practices, hidden functions, and vulnerable features within the code during the implementation of the code base and methods applied to eliminate these vulnerabilities	Should be considered during system implementation.

applied to safety systems, it is evident that the availability of the systems will be adversely affected. As indicated in this argument, security controls should be applied to the systems with caution by analyzing if there are no adverse impacts during the implementation of the controls into the systems. There may be some limitations dependent on the target system when applying technical security control requirements. In cases of safety systems, which do not use general IT devices, the direct application of technical security controls to the CDAs will be very restricted. Critical security requirements with high priorities should be identified first through the vulnerability analyses and penetration tests, to assess the security requirements in a more objective way.

Security measures are identified to protect CDAs against the malicious activities resulting from the vulnerability analyses and penetration test in section 2.1.5. Table 8 shows these measures, and Fig. 6 shows the arrangement of these measures for the PPS security model.

As shown in Table 8 and Fig. 6 above, it is identified that access control, monitoring & logging, and encryption are the most critical technical security controls for the PPS. These security controls are general for safety systems, since the components and structures of the other safety systems are similar to the PPS, and can also be extended to non-safety systems because they have attack vectors similar to the PPS case.

- Access Control: For both safety and non-safety systems, identification and authentication, system and data restrictions, system use notification, domain, session, portable and mobile media, unauthorized access and use, communications access, etc.
- Monitoring & Logging: Monitoring and analyzing conditions for both safety and non-safety systems.
- Encryption: Network and data encrtyption mainly for non-safety systems.

Based on this argument, the requirements selected as in section 2.2.1 can be classified into four groups including access control, monitoring and logging, encryption, and others. Table 9 lists the titles of the technical security control requirement in the RG 5.71 selected as in section 2.2.1 and classified in four groups.

3. RESULTS AND DISCUSSION

To define applicable technical security requirements, attack vectors described in section 2.1 and technical requirements analysis in section 2.2 are integrated. Attack vectors in Fig. 4 need to be refined in more detail in accordance with the analysis of the requirements. Fig. 7 shows the results from this refinement. Among digital devices for the maintenance and tests, there can be non-authenticatable ones such as a digital tester. Although these devices do not have an authentication function, they may allow the use

Table 8. Security Measures Against the Malicious Activities Drawn in Section 2.1.5 for the PPS

Malicious activities	Technical security measures
DoS attack	Network Monitoring
Network Scan (port, service etc), Network Sniffing	Network/Host Monitoring
Packet Modification	Network/Host Monitoring, Encryption
Local Exploit to Escalate Privilege	Host Monitoring, Access Control
Improper or Illegal Command Execution	Access Control
Processor Resource Exhaust Attack	Network/Host Monitoring,

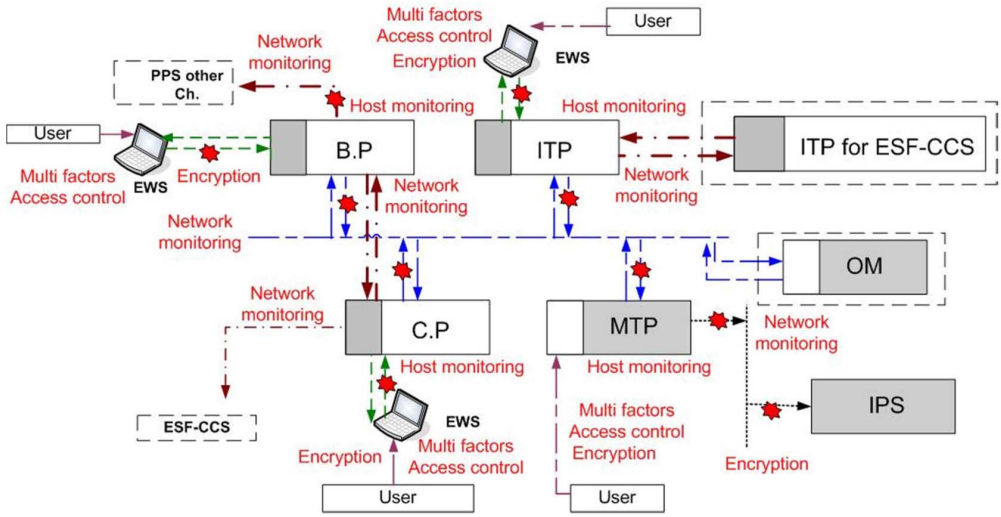

Fig. 6. Security Measure Arrangement for PPS

of external media for data loading and backup purposes. Another point to consider in the identification of applicable requirements is that there are two different kinds of external media. A group of external media such as USB flash drives and HDDs has a read and write capability, and another group such as CD and DVD is read-only. According to this capability, applicable security requirements will be different from each other.

Where to apply the requirements grouped in Table 9 can be evaluated with the attack vectors in Fig. 7. The requirements are reviewed for the following elements:

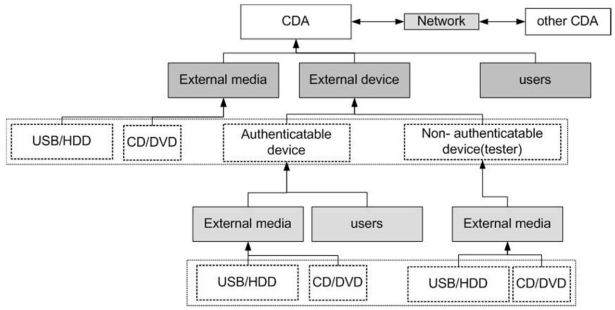

Fig. 7. Refined Attack Vectors

Table 9. Titles of Technical Security Control Requirements Selected for the PPS and Classified in four Groups

Access Control	Monitoring & Logging	Encryption	Others
(Appendix B) • Access Control Policy and Procedures • Access Control Policy and Procedures • Account Management • Application Partitioning and Security Function Isolation • Authenticator Feedback • Device Identification and Authentication • Hardware Configuration • Identification and Authentication Policies and Procedures • Nonauthenticated Human Machine Interaction Security • Password Requirements • Previous Logon Notification • Session Authenticity • Session Lock • Trusted Path • Unauthorized Remote Activation of Services • Unsuccessful Login Attempts • Use of External Systems • User Identification and Authentication (Appendix C) • Defense-in-Depth • Information Input Restrictions • Maintenance Tools • Media Access	(Appendix B) • Audit Generation • Audit Reduction and Report Generation • Audit Review, Analysis, and Reporting • Audit Storage Capacity • Auditable Events • Changes to File System and Operating System • Content of Audit Records • Denial of Service Protection • Fail in Known State • Hardware Configuration • Host Intrusion Detection System • Information Flow Enforcement • Mobile Code • Proprietary Protocol Visibility • Protection of Audit Information • Removal of Unnecessary Services and Programs • Response to Audit Processing Failures • Secure Name/Address Resolution Service (Authoritative/Trusted Source) • System Use Notification Permissions • Time Stamps (Appendix C) • Defense-in-Depth • Developer Security Testing • Error Handling • Incident Moniotoring • Information Input Restrictions • Maintenance Tools • Malicious Code Protection • Monitoring Tools and Techniques	(Appendix B) • CDA Backups • Confidentiality of Information at Rest • Cryptographic Key Establishment and Management • Cryptographic Module Authentication • Information Flow Enforcement • Transmission Confidentiality • Transmission Integrity • Use of Cryptography	(Appendix B) • Authenticator Management • Changes to File System and Operating System Permissions • Identifier Management • Insecure and Rogue Connections • Installing Operating Systems, Applications, and Third-Party Software Updates • Least Privilege • Network Access Control • “Open/Insecure” Protocol Restrictions • Public Key Infrastructure Certificates • Separation of Functions • Shared Resources • Supervision and Review—Access Control • Third Party Products and Controls

- User to CDA: The requirements for access controls should be considered. Those for monitoring and logging may in part be applicable to the record information on users' access to the CDA, if the CDA provides that logging function. Encryption requirements may be applied in part to a function handling user input for access controls. This can be dependent on the capability of CDA.
- External Devices (Authenticatable) to CDA : When external devices are connected to the CDA, the requirements of the access control should be considered. At least either the external devices or the CDA, which can process the authentication and recording the related information, should have security functions for access control and logging. The requirements for monitoring the data transmission along this path can be applied, if possible. Encryption of data transmitted between digital devices may not be necessary, if man-in-the-middle (MitM) attacks are not possible.
- External Media to the CDA: The requirements for access control should be considered, if external media may be connected to the CDA. The CDA should have functions of access control and real-time monitoring of data transmission, if this is not possible, the media record the history of access and data transmission. There can be access control provisions in both the media and the CDA. Encryption may not be needed here.
- External Media to External Device (Authenticatable): The requirements for access control and monitoring should be considered, at least for the items such as automated access control and management, monitoring, device identification, and error handling. Encryption may not be needed here.
- External Device (Non-Authenticatable) to CDA: In most cases, both devices cannot implement security functions, hence, device user, device identification, and related user tasks may be recorded manually. This is rather related to the security policy or management controls.
- External Media to External Devices (Non-Authenticatable): This may not be allowed in NPPs. But if any, operation and management controls similar to External Device (Non-Authenticatable) to CDA can be applied.
- Other CDAs to a target CDA: Data transfer between CDAs occur through networks. The newtwork architecture can be reviewed with the defense-in-depth requirements. Monitoring and logging for the data transmission should be considered. Access controls are very difficult to apply here, since there must be adverse impact to the function of CDAs. Encryption may bring similar impact, but for the non-safety systems, data storage servers and netwroks may consider the application of encryption.
- User to External Devices (Authenticatable): This can be treated similar to User to CDA. The requirements for access control and monitoring and logging should be considered in the external devices.

RG 5.71 requires that security controls should not cause any adverse impact on the safety function and performance of CDAs. If a security control requirement belongs to this category, alternative control requirements should be considered. For example in cases where, it may not be easy to implement real-time authentication functions for safety-grade PLCs. There are many cases addressing both basic requirements for technical security controls and alternatives in RG 5.71. In these cases, the alternatives address physical and/or management control requirements in general, and the basic requirements for technical security controls will be better than the alternatives for the security purpose. The alternatives may be considered, only if a specific security control requirement cannot be implemented because of the adverse impact.

The main purpose of encryption is to protect CDAs against man-in-the-middle (MitM) attacks. This may not be an effective form of control for safety systems, since MitM attacks are hard to expect in the environment where the safety systems are placed. The non-safety systems, which have computer systems and networks similar to industrial control systems or general IT systems, may consider the application of encryption for the confidentiality and integrity of the data stored and transmitted within the non-safety systems.

Security control devices for monitoring and logging are not currently avaliable in the nuclear domain. Host-based intrusion detection systems (HIDS) required in RG 5.71 may cause an adverse impact on the system function. In this case, HIDS specially developed for NPP I&C systems not affecting system function or network-based intrusion detection systems (NIDS) can be candidates for monitoring and logging. All the IDS in local CDAs or networks may be integrated to provide plant-wide security monitoring, logging, and alarming services. This addition of security control devices will be followed by additional cyber security risk assessments. They will be treated as separate systems located in the same defensive architecture of the I&C systems with suitably assigned security levels. They may need to apply security control requirements such as those for access controls and encryption.

Based on the above discussion, technical control requirements are collected for the sample PPS., Table 10 shows the list of technical security control requirements for the sample PPS, collected from the classified RG 5.71 requirements in Table 9, according to the refined attack vector analysis in Fig. 7. If the configuration of other safety I&C systems in NPPs is considered, this table can be applied extensively to the safety systems. Table 10 also includes the technical security control requirements that should be addressed commonly in the design and development of I&C systems. Fig. 8 shows the application of technical security control requirements to the sample PPS.

Table 10. Technical Security Control Requirements for the Sample PPS Identified with the Elements of Refined Attack Vectors

User to CDA	External Device(Authenticatable) to CDA
(Access Control) • Audit Reduction and Report Generation • Audit Review, Analysis, and Reporting • Auditable Events • Authenticator Feedback • Identification and Authentication Policies and Procedures • Information Input Restrictions • Nonauthenticated Human Machine Interaction Security • Password Requirements • Previous Logon Notification • Session Authenticity • Session Lock • Unsuccessful Login Attempts • User Identification and Authentication (Monitoring & Logging) • Error Handling • Information Input Restrictions • System Use Notification (Encryption) • CDA Backups • Confidentiality of Information at Rest	(Access Control) • Account Management • Authenticator Feedback • Device Identification and Authentication • Identification and Authentication Policies and Procedures • Information Input Restrictions • Maintenance Tools • Previous Logon Notification • Session Authenticity • Session Lock • Unsuccessful Login Attempts • Use of External Systems • User Identification and Authentication (Monitoring & Logging) • Auditable Events • Error Handling • Information Input Restrictions • Maintenance Tools • Malicious Code Protection • Mobile Code • System Use Notification
External Media to CDA	**External Media to External Devices (Authenticatable)**
(Access Control) • Access Control Policy and Procedures • Account Management • Authenticator Feedback • Identification and Authentication Policies and Procedures • Information Input Restrictions • Maintenance Tools • Password Requirements • Previous Logon Notification • Trusted Path • Unsuccessful Login Attempts • User Identification and Authentication (Monitoring & Logging) • Audit Reduction and Report Generation • Audit Review, Analysis, and Reporting • Audit Storage Capacity • Auditable Events • Content of Audit Records • Error Handling • Information Input Restrictions • Maintenance Tools • Malicious Code Protection • Mobile Code • Response to Audit Processing Failures • System Use Notification (Encryption) • CDA Backups	(Access Control) • Access Control Policy and Procedures • Account Management • Identification and Authentication Policies and Procedures • Information Input Restrictions • Password Requirements • Previous Logon Notification • Trusted Path • Unsuccessful Login Attempts • User Identification and Authentication (Monitoring & Logging) • Audit Reduction and Report Generation • Audit Review, Analysis, and Reporting • Audit Storage Capacity • Auditable Events • Content of Audit Records • Error Handling • Maintenance Tools • Malicious Code Protection • Mobile Code • Response to Audit Processing Failures • System Use Notification (Encryption) • CDA Backups

Table 10. Technical Security Control Requirements for the Sample PPS Identified with the Elements of Refined Attack Vectors

External Devices (Non-Authenticatable) to CDA	Other CDA to CDA (including Networks)
(Access Control) • Device Identification and Authentication • Maintenance Tools • User Identification and Authentication (Monitoring & Logging) • Maintenance Tools • System Use Notification	(Access Control) • Defense_in_Depth (Monitoring & Logging) • Auditable Events • Defense_in_Depth • Denial of Service Protection • Host Intrusion Detection System • Information Flow Enforcement • Proprietary Protocol Visibility • Response to Audit Processing Failures • Secure Name/Address Resolution Service (Authoritative/Trusted Source) (Encryption) • Cryptographic Key Establishment and Management • Cryptographic Module Authentication • Information Flow Enforcement • Transmission Integrity (Others) • Insecure and Rogue Connections • Network Access Control • "Open/Insecure" Protocol Restrictions
External Media to External Devices (Non-Authenticatable)	
(Monitoring & Logging) • Maintenance Tools • System Use Notification	
User to External Devices (Authenticatable)	**Additional items**
(Access Control) • Access Control Policy and Procedures • Account Management • Authenticator Feedback • Identification and Authentication Policies and Procedures • Password Requirements • Previous Logon Notification • Session Authenticity • Session Lock • User Identification and Authentication (Monitoring & Logging) • Auditable Events • Error Handling • Information Input Restrictions • System Use Notification	(Access Control) • Application Partitioning and Security Function Isolation • Hardware Configuration • Unauthorized Remote Activation of Services (Monitoring & Logging) • Developer Security Testing • Fail in Known State • Hardware Configuration • Monitoring Tools and Techniques • Protection of Audit Information • Removal of Unnecessary Services and Programs

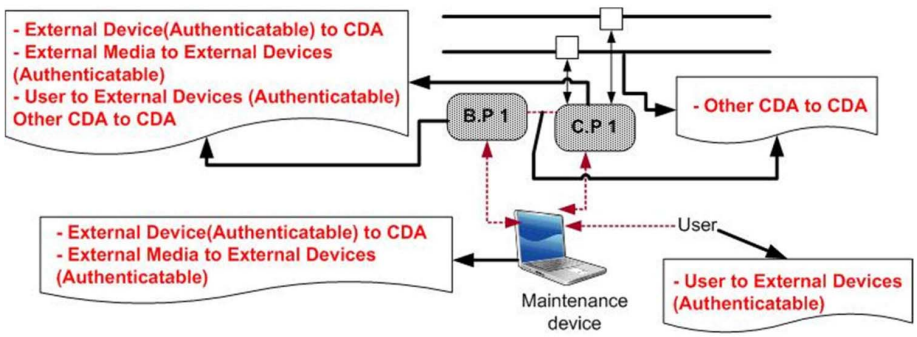

Fig. 8. Example Application of Technical Security Control Requirements to the PPS

4. CONCLUSION

Due to the digitalization of NPP I&C systems, cyber security has become an important issue. The RG 5.71 published by the U.S. NRC provides guidance for the cyber security of I&C systems, including cyber security plans and programs, methods for cyber security assessments, and a comprehensive set of security controls. There are still difficulties, from the system designer's point of view, when trying to apply the requirements to target systems.

In order to provide helpful information for system designers in the application of cyber security requirements to systems, this paper describes methods and considerations to define attack vectors in a target system, to review and select the requirements in RG 5.71, and to integrate the results from these activities to identify applicable technical security controls according to the attack vectors.

The attack vector analyses are performed in a process consisting of the following activities: 1) Analysis of an I&C system architecture at the highest conceptual level; 2) Modeling of a target system in cyber security point of view; 3) Security level assignments to the CDAs of a target system; 4) Analysis of the elements of attack vectors; 5) Investigation of the known vulnerabilities residing in the CDAs and penetration tests to identify potential malicious activities.

The RG 5.71 provides the most complete set of requirements for the cyber security of NPP I&C systems. Among the security control requirements listed in Appendices B and C of RG 5.71, those that should be implemented into the systems are selected and classified in groups of technical security control requirements using the results from the attack vector analyses. For the attack vector elements of CDAs, all the requirements in the groups of technical security controls are evaluated in their applicability and effectiveness, and considerations in this evaluation are also discussed.

The methods proposed in this paper are practiced with a sample PPS system, and the technical security control requirements grouped according to the elements of attack vectors are presented as a result.

In conclusion, the proposed methods provide useful and practical information for NPP I&C system designers for the identification of appropriate technical security controls and their locations in the systems. Further studies are needed to search detailed practices of those control requirements, and to develop security devices and technologies best fitted to NPP I&C systems.

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] Kee-choon Kwon and Myeongsoo Lee, Technical review on the localized digital instrumentation and control systems, Nuclear engineering and technology Vol.41 No.4 May 2009 – Special issue in celebration of the 40th anniversary of the Korean Nuclear Society, 2009.
[2] 10 CFR Part 73.54, Protection of Digital Computer and Communication Systems and Networks, U.S. Nuclear Regulatory Commission, Washington, DC., 2009.
[3] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.
[4] KINS/RG-N08.22, Cyber Security of Instrumentation and Control Systems, Korea Institute of Nuclear Safety, 2009.
[5] IAEA Nuclear Security Series No.17 Technical guidance Computer security at nuclear facilities, 2011.
[6] IEEE Standard 7-4.3.2-2010, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, August 2, 2010.
[7] Marcelo Masera, Igor Nai Fovino, Bogdan Vamanu, ICT aspects of power systems and their security, Institute for the Protection and Security of the Citizen, Joint Research Centre, November 2010.
[8] Igor Nai Fovino, Luca Guidi, Marcelo Masera, and Alberto Stefanini, Cyber security assessment of a power plant, Electric Power Systems Research, (81), pp518–526, Elsevier, 2011.
[9] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, June 2011.
[10] Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments, Homeland Security, July 2009.
[11] Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies, Homeland Security, October 2009.
[12] Control Systems Cyber Security: Defense in Depth Strategies, INL/EXT-06-11478, David Kuipers, Mark Fabro, Idaho National Laboratory, Idaho Falls, Idaho, May 2006.
[13] Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems, GAO-04-354, United States General Accounting Office, March 2004.
[14] Gee-Yong Park, Cheol Kwon Lee, Jong Gyun Choi, Dong Hoon Kim, Young Jun Lee, and Kee-Choon Kwon, Cyber Security Analysis by Attack Trees for a Reactor Protection System, Transactions of the Korean Nuclear Society Autumn Meeting PyeongChang, Korea, October 30-31, 2008.
[15] Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Dong-Young Lee, Cyber Security Considerations in the Development of I&C Systems for Nuclear Power Plants, The 2011 International Conference on Security and Management (SAM'11), Las Vegas, USA, July 18-21, 2011.
[16] Jung-Woon Lee, Jae-Gu Song, Cheol-Kwon Lee, and Dong-Young Lee, A Conceptual Framework for Securing Digital I&C Systems in Nuclear Power Plants, The 2012 International Conference on Security and Management (SAM'12), Las Vegas, USA, July 16 - 19, 2012.
[17] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, August 2009.
[18] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.

[19] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, and Dong-Young Lee, A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nuclear engineering and technology, Vol.44 No.8 December 2012.
[20] http://searchsecurity.techtarget.com/definition/attack-vector
[21] NEI 04-04 Revision 1, Cyber Security Program for Power Reactors, Nuclear Energy Institute, November 18, 2005.
[22] NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, June 2011.
[23] Common Vulnerability and Exposures (CVE), http://cve.mitre.org.
[24] NEI 03-12 Revision 6, Security Plan, Training and Qualification Plan, and Safeguards Contingency Plan, Nuclear Energy Institute.