A Cyber Security Risk Assessment Procedure for Digital I&C Systems in NPPs

J. G. Song, J. W. Lee, C. K. Lee, K. C. Kwon, D. Y. Lee
Korea Atomic Energy Research Institute
1045, Daedeok-Daero, Yuseong, Daejeon, 305-600, Republic of KOREA
{jgsong, leejw, cklee1, kckwon, dylee2}@kaeri.re.kr

1. Introduction

Digital Instrumentation and Control (I&C) systems in nuclear power plants (NPPs) use general digital technologies similar to those used in IT systems. However, one of significant differences between the two systems resides in the duration of their service life. The I&C systems in NPPs operate for more than 20 years. IT systems, on the other hand, are in service for about 3 to 5 years. Hence, a one-time risk assessment for IT systems is normally acceptable. In contrast, the risk assessment for the I&C systems in NPPs should be recursively performed during their longer operation life.

A recursive procedure for cyber security risk assessment of the I&C systems in NPPs is studied and proposed in this paper.

2. Cyber security risk assessment procedure

In the risk assessment of IT systems, digital assets in IT systems are analyzed in consideration of the importance and likelihood of loss in the confidentiality, integrity, and availability expected by cyber threats [1,2]. While in the risk assessment of digital I&C systems in NPPs, digital assets are analyzed whether they are critical digital assets (CDAs) [3]. In addition, activities for cyber security for the I&C systems, which range from CDA identification to the application of mitigation measures are needed to be performed whenever the development phases revolve of any changes to the CDAs occur[4]. In the consideration of this point, a cyber security risk assessment procedure for the I&C systems in NPPs is designed as follows.

Step 1: Establishment of cyber security plan and policy
Step 2: Identification of CDAs
Step 3: Analysis of threat, vulnerability, and response methods
Step 4: Defining of risk table
Step 5: Collection of mitigation measures
Step 6: Implementation and testing of mitigation measures
Step 7: Input to best practice data base for digital I&C risk assessment

Figure 1 shows the cyber security risk assessment procedure.

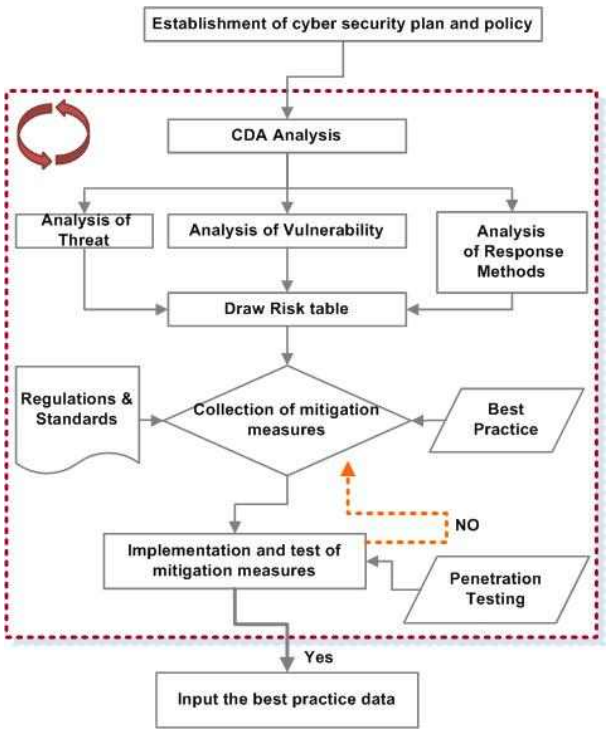

Fig. 1. Digital I&C risk assessment procedure.

These steps are described in details here.

Step 1. To analyze the cyber risk, security policy and plan should be established first. The security plan is the implementation of cyber security policy in the form of organizational roles, responsibilities, and procedures. The plan specifies and details the means for achieving the security goals at the facility[5].

Step 2. In this step, the characteristics of critical digital assets are categorized. A comprehensive analysis of CDAs in a nuclear facility includes[5]:

- functions/tasks and operational modes of all existing computerised systems
- identification of relevant interconnections including power supplies
- dataflow analysis, to determine what communicates with what, and how and why
- procedures that initiate communication, frequency of communication, protocols

Step 3. In this step, several security standards and technical resources should be investigated for analyzing cyber security of threat, vulnerability and response methods.

Table 1: A sample of risk table

Requirements	RG 5.71 Code	Contents	Mitigations	Link data
Access Enforcement	B.1.3	Assigning all user rights and privileges on the CDA consistent with the user authorizations	Rewrite the software to require both username and password before validating credentials	CVE-2010-xxx
			Avoid storing hard-coded credential information, or store password hashes instead of plaintext passwords	
			Change default accounts and passwords	
Denial of Service Protection	B.3.4	Configuring CDAs to protect against or limit the effects of denial of service attacks	Detection of unusual network traffic	CVE-20xx-xxx
System Hardening	B.5.5	Notification to authorized personnel of patches affecting cyber security	Update patches	CVE-20xx-xxx
			Administrative policies to ensure periodic review	
Etc.	-	-	-	-

The information helpful for the analyses can be obtained from appendix B and C in the NIST Regulatory Guide (RG) 5.71, the NIST National Vulnerability Database (NVD), and especially the Common Vulnerability and Exposures (CVE) system [6]. The CVE system includes well-known vulnerabilities and mitigation, and provides useful data regarding digital I&C cyber security [7]. Many security assessment systems uses CVE for IT systems. To determine which CVE to use, cyber security managers must know the details of their systems first .

Step 4. In this step, cyber risk factors and mitigations to the digital I&C in NPPs are defined. Table 1 shows a sample of the defined risk table.

Step 5. This step describes how to achieve high assurance that CDAs are adequately protected against cyber attacks by using possible mitigation candidates. The information used in this step can be obtained from several standards, regulation requirements and best practice related with digital I&C cyber security.

Step 6. This step is used to determine whether the mitigation measures in Step 5 can be implemented as security controls for the digital I&C systems. If the mitigation methods cannot be implemented or affect the functionality and performance of the digital I&C systems, go back to Step 5 in order to find alternative security controls. After the implementation of security controls, perform penetration testing on a target CDAs for discovering substantial vulnerabilities. If new vulnerabilities are found, go back to Step 5 again. If there are changes about security factors, it should be recursively processed from Step 2 to step 6.

Step 7. Although Step 7 is not a base step of this procedure, Keeping proven risk assessment data is important to other similar systems.

3. Conclusions

Cyber security risk is growing daily and many nuclear power plants are not well aware of what are vulnerable, in their digital I&C systems, and how protect their systems from cyber attacks.

In order to help in handling this cyber security situation in NPPs, this research introduced a cyber security risk assessment procedure for digital I&C systems. In this procedure, a recursive performance of the steps is emphasized to achieve cyber security of digital I&C systems in NPPs.

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] Christopher Alberts, Audrey Dorofee, Managing Information Security Risk : The OCTAVESM Approach, Addison-Wesley Professional, July 09, 2002.

[2] Gary StoneBurner, Alice Goguen, Alexis Feringa, Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, July, 2002.

[3] USNRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.

[4] 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 International conference on Security and Management(SAM), 2011.

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Security Series, COMPUTER SECURITY at NUCLEAR FACILITIES, 2010.

[6] NIST National Vulnerability Database version 2.2, nvd.nist.gov.

[7] Common Vulnerability and Exposures (CVE), cve.mitre.org.