Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 29-30, 2015

Considerations on Cyber Security Assessments of Korean Nuclear Power Plants

Jung-Woon Lee [a*], Jae-Gu Song [a], Kyung-Soo Han [a], Cheol Kwon Lee [a], and Mingyun Kang [b]
[a]*Korea Atomic Energy Research Institute, Daejeon, Republic of Korea*
[b]*E-Gonggam Co., Ltd, Daejeon, Republic of Korea*
[*]Corresponding author: leejw@kaeri.re.kr

1. Introduction

As digital technologies have been applied to nuclear power plants (NPPs), cyber security has become one of important issues in nuclear industries. U. S. NRC published the regulatory guide 5.71 (RG 5.71) in 2010 [1]. Korea Institute of Nuclear Nonproliferation and Control (KINAC) has prepared the regulatory standard RS-015 [2] based on RG 5.71. RS-015 defines the elements of a cyber security program to be established in nuclear facilities and describes the security control items and relevant requirements. Cyber security assessments are important initial activities in a cyber security program for NPPs. Cyber security assessments can be performed in the following key steps:

1) Formation of a cyber security assessment team (CSAT);
2) Identification of critical systems and critical digital assets (CDAs);
3) Analysis of defense-in-depth protection strategies; and
4) Plant compliance checks with the security control requirements in RS-015.

Through the assessments, the current status of security controls applied to NPPs can be found out. The assessments provide baseline data for remedial activities. Additional analyses with the results from the assessments should be performed before the implementation of remedial security controls.

The cyber security team at the Korea Atomic Energy Research Institute (KAERI) has studied how to perform cyber security assessments for NPPs based on the regulatory requirements [3,4]. Recently, KAERI's cyber security team has performed pilot cyber security assessments of a Korean NPP [5]. Based on this assessment experience, considerations and checkpoints which would be helpful for full-scale cyber security assessments of Korean NPPs and the implementation of remedial security controls are discussed in this paper.

2. Considerations and Checkpoints

In this section, considerations and checkpoints are discussed for the above four assessment steps and the additional analysis stage for the implementation of remedial security controls.

2.1 Formation of Cyber Security Assessment Team

In general, information technology (IT) cyber security experts and plant engineers form CSATs. IT security experts do not have experience with plant systems and work environments, while plant engineers are in general unfamiliar with cyber security requirements. Without a basic understanding of both domains, the assessments may not be comprehensive and the results may not be satisfactory.

For a better CSAT, IT security experts should have basic knowledge on plant systems and work environments, and plant engineers should understand the meaning of security controls as well as overall plant systems and the tasks performed by plant personnel. The quality of assessments depends on the knowledge of CSAT members on both cyber security requirements and plant environments. Hence education contents for individual CSAT members should be different based on their background knowledge.

2.2 Identification of Critical Systems and CDAs

In this step, a CSAT identifies critical systems first then identifies CDAs. According to the critical system and CDA identification criteria in RS-015, if a plant system is determined not to be a critical system, then any digital assets in the system will not be considered as CDAs. These digital assets will be placed out of scope. But any digital assets in NPPs should be managed with caution, since they can provide unexpected attack pathways to CDAs. For an example, if a digital asset, which is not a CDA, has I/O ports, then these ports can be used for attack pathways against CDAs in the plant. Hence, these ports should be managed in disabled status when they are not used. It is important in this step to identify all the digital assets in a NPP site. This identification process should cover the whole plant systems and equipment. For this purpose, there should be a comprehensive list of plant systems with which a CSAT can determine that any digital assets are not left as unidentified in this identification step.

There can be an argument regarding the level of decomposition when identifying CDAs. Decision on the level of decomposition can be made to be a level of elements for which technical security controls can be addressed.

2.3 Analysis of Defense-in-depth Protection Strategies

Korean NPPs have been constructed for generations. Defense-in-depth protection strategies are related to the

safety classification of equipment. The classification of safety grade equipment may not be the same among NPPs. It will cause a problem if defense-in-depth rules for a new NPP would be applied consistently to old NPPs. For some network connections which do not satisfy defense-in-depth protection rules, it is recommended that additional analyses are performed carefully around these connections at the system level or for a group of CDAs, rather than just around the related CDAs.

It is also recommended that the concept of physical protection areas and physical access controls is considered along with the defense-in-depth protection strategies for cyber security.

2.4 Plant Compliance Checks with the Security Control Requirements

RS-015 requires the assessments to address all the security controls. Difficulties in this step stem mostly from the assessment activities deciding which security requirements should be applied to CDAs and how to implement security controls into CDAs in order to comply with the requirements. More than one hundred security controls are mentioned in RS-015, and it is reported that there may be about a thousand CDAs in an NPP.

Assessments in this step are time consuming and also require considerable efforts for checking plant compliance with the requirements. Assessments in this step are very important activities for ensuring cyber security in NPPs. Once the assessments make any wrong decisions on security features, then these features will exist as hard-to-detect security flaws for a long time. The quality of assessments heavily depends on the capability of CSAT when interviewing plant system engineers and reviewing various plant documents. If the compliance are checked without careful analyses of plant environment including potential threats and attack vectors around the system to be assessed. There should be adequate training for CSATs to perform these cyber security assessments with an acceptable level of assessment quality.

From the experience of pilot assessments, it can be estimated that the compliance checks need at least 10 working days for a plant system. This implies that several months to a year may be required for the compliance checks of a whole NPP.

KAERI cyber security team has developed a software tool CSAMS based on the pilot assessment experience [6]. By using CSAMS, a CSAT can draw an overall structure of a system and obtain baseline cyber security information for CDAs in the system. CSAMS provides standardized questionnaires with the list of CDAs and detailed checkpoints relevant to each regulatory requirement. CSATs can perform the compliance checks with the regulatory requirements effectively in a consistent manner and in time lesser than the assessments without CSAMS.

2.5 Analyses for the Implementation of Remedial Security Controls

The security control requirements which are not satisfied in NPPs are identified through the compliance checks. Some security features may be not installed at all and others may need improvements. There can be many implementation options of a specific security control. Evaluations of the options, based on some criteria such as easiness and cost for the implementation and effectiveness for cyber security, should be conducted along with analyses of the impacts on existing plant systems by the implementation. It should also be considered that these evaluations and analyses must also take considerable time and may require a lot of communications with outside entities such as designers or vendors.

There are no guidance documents available for such evaluations and analyses. Practical guidance documents for the evaluations of security control implementation options and the analyses of impacts should be developed to design and implement right security controls.

Ref. [7] indicates protective measures in layers, from surface to core, ‘policies, procedures, awareness,’ ‘physical security,’ ‘perimeter defense,’ ‘network segmentation,’ ‘asset hardening,’ ‘application hardening,’ ‘protocol and transport defense,’ and ‘embedded device hardening.’ Rockwell Automation’s defense-in-depth security is a five-layer approach focusing on physical security, network security, computer hardening, application security, and device hardening [8].

It can be said that technical security controls play at the deeper layers of protective measures than operational and management security controls. It will be better to implement technical security controls as much as possible. In general, operational and management security controls can be breached more easily than technical security controls. In operating NPPs, the implementation of technical security controls may have many limitations. Operational and management security controls may be selected as alternatives to the technical security controls that are not implemented. These alternative operational and management security controls will form a sole layer of protective measures. The alternative security controls should be developed elaborately and maintained carefully. Plant guides and procedures for the alternative security controls should describe cyber security activities at digital asset level, neither at the system level nor at the plant level, such that plant engineers and/or cyber security personnel can manage the activities with each digital asset without omission.

It can also be recommended to perform another process to estimate risks that can be caused without remedial technical security controls and to design alternative operational and management security controls that can eliminate or mitigate the risks.

3. Conclusions

Cyber security assessment is one of important and immediate activities for NPP cyber security. The quality of the first assessment will be a barometer for NPP cyber security. Hence cyber security assessments of Korean NPPs should be performed elaborately. Considerations and cautions described in this paper, based on KAERI cyber security team's assessment experience, can contribute to better cyber security assessments of Korean NPPs.

ACKNOWLEDGMENT

This work was supported by the Energy Efficiency & Resources of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Trade, Industry and Energy (No. 20131520202250).

REFERENCES

[1] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, 2010.
[2] KINAC/RS-015, Cyber Security Regulatory Standard for Nuclear Facilities, KINAC, Daejeon, Republic of Korea, 2014.
[3] 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, 919-928
[4] Jae-Gu Song, Jung-Woon Lee, Gee-Yong Park, Kee-Choon Kwon, Dong-Young Lee, and Cheol-Kwon Lee, "An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants," Nuclear Engineering and Technology, Vol.45 No.5 (2013), 637-652
[5] Lee, J.W., Song, J.G., Jung, S.M., Han, K.S., Kang M., and Lee C.K., Pilot Cyber Security Assessments of a Nuclear Power Plant based on Regulatory Requirements, IAEA International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, 1-5 June, 2015, Vienna, Austria.
[6] Song, J.G., Lee, C.K., and Lee, J.W., Design Concept of Cyber Security Assessment and Management System for Digital Systems in Nuclear Facilities, IAEA International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, 1-5 June, 2015, Vienna, Austria.
[7] Robert M. Lee, ICS Cyber Attacks: Fact vs. Fiction and Why it Matters, ICSJWG June 2015 Meeting, Washington, DC.
[8] Rockwell Automation, Are You Managing Your Security Risks? http://www.rockwellautomation.com/global/news/the-journal/exclusive/2013/july4.page