Suggestion of Initiating Threats and Bounding Groups for NPP Cyber Risk Assessment

Sang Min Han [a*], Poong Hyun Seong [a]
[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*
[*] *Corresponding author: gkstkdals@kaist.ac.kr*

1. Introduction

The aim of this study is to propose initiating threats and their bounding groups in order to identify cyber threats in NPPs (Nuclear Power Plants). NPP has been generally thought to be secure from cyber-attacks, since the control/monitoring network and business network in NPP are separated from the external network. However, consecutive incidents in nuclear facilities, such as Hatch NPP incident in 2008, Natanz nuclear facility incident in 2010, Monju NPP incident in 2014, and Gudremmingen NPP incident in 2016, revealed the necessity of cyber security management for NPPs.

2. Methods and Results

To enhance cybersecurity of a system, CSF (Cyber Security Framework) ver.1.1 have been suggested by NIST (National Institute of standards and Technology) on 2018 NIST Cybersecurity Risk Management Conference. [1]

Figure 1. CSF and its main functions

CSF focuses 5 functions to enhance cyber security: 1) Identify, 2 Protect, 3) Detect, 4) Respond, and 5) Recover. Nuclear industry is in its very first phase to implement CSF functions to the NPPs. Identify function which implies development of the organizational understanding to manage cyber security risk to system, assets, data, and capabilities, includes the development of a cyber risk assessment method. Several methods have been developed for assessing cyber risks on NPPs, [2,3,4,5] however, threats of risk assessment methods are often dealt without considering the sequences of violations regarding confidentiality, integrity, and availability. In order to consider the logical sequences of threats on NPPs, the term 'initiating threats' have been suggested. Initiating events in probabilistic safety assessment determine the points of departure of the accident sequences that leads potentially to core damage. [6] A missing initiating events in a PSA means that the core damage frequency would be underestimated, and a larger list of initiating events that necessary (for example, due to inappropriate grouping) would result in waste of resources because of the analyses of additional unnecessary accident sequences. Therefore, appropriate selection of initiating events and their bounding groups are required to assess risk. In the same vein, initiating threats also should have tidy list to appropriately assess risks on NPPs.

IAEA-TECDOC-719 suggests several methods to identify the necessary initiating events: 1) Engineering evaluation or technical study, 2) Reference to previou PSAs, 3) EPRI list of initiating events, 4) Logical classification, 5) Plant energy balance fault tree, 6) Analysis of operation experience for actual plant, 7) Failure mode and effect analysis, or 8) other methods. Since there is no former lists or analysis results for assessing NPP initiating threats, to determine threats and their bounding groups for NPP, operational experience, engineering evaluation, and deductive analysis methods were chosen. Operational experience report (OER) and repository of industrial security incidents (RISI) database [7] were utilized to collect the actually occurred threat scenarios. Impractical threats were removed from the threat list through engineering evaluation, and then vulnerability reports published from several IT and operational technology (OT) vendors were reviewed for deductive supplemental analysis. [8,9,10] Every chosen events were documented with the descriptions based on the five characteristics for determining the bounding groups of threats: 1) by whom, 2) why, 3) how, 4) via what, and 5) for knowing what. In here, incidents caused by SDOE (secured development and operational environment) were filtered, since we focused on the cyber threats.

Figure 2. Working sheet for RISI database analysis

As a result, initiating threats and their bounding groups were suggested.

3. Conclusions

Suggested initiating threats and their bounding groups for NPP have an accent on first attempt to consider the breaching sequences in determining threats, and they could be further applied to descript the scenarios and model of NPP cyber risk assessment as shown in figure 3.

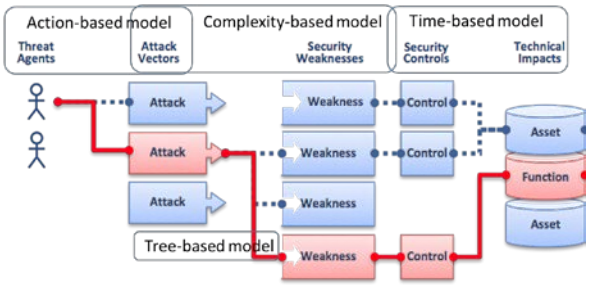

Figure 3. Relationship between risk assessment model and scenario [10]

REFERENCES

[1] https://www.nist.gov/cyberframework
[2] W. Ahn, et. Al., “Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs,” International Journal of Distributed Sensor Networks, 32, 2015.
[3] S. Jajodia and S. Noel, “Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response,” Algorithms, Architectures and Information Systems Security, World Scientific, New Jersey, 2009.
[4] I. Kotenko and A. Chechulin, “A Cyber Attack Modeling and Impact Assessment Framework,” Proceeding of the 5th International Conference on Cyber Conflict, Tallinn, Estonia, June 4 – 7, 2013.
[5] A. Varuttamaseni, et al. “Construction of a Cyber Attack Model for Nuclear Power Plants”, 10th NPIC-HMIT, May, 2017.
[6] IAEA-TECDOC-719, “Defining Initiating Events for Purposes of Probabilistic Safety Assessment”, IAEA, September, 1993.
[7] http://www.risidata.com/Database
[8] Cisco, 2017 Annual Cybersecurity Report, 2017
[9] A. Hristova, R. Schlegel, and S. Obermeier, Security Assessment Methodology for Industrial Control System Products, The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, June 4-7, 2014, Hong Kong, China
[10]https://www.owasp.org/index.php/Category:OWASP_Top_ Ten_Project