Development of Initiating Cyber Threat Scenarios and the Probabilities Based on Operating Experience Analysis

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

1.1 Background

As safety-critical infrastructures have become complex and increasingly adopted digital technologies and automation, cyber security became a natural issue. Nuclear power plants (NPPs), one of the safety-critical infrastructures, are generally thought to be secure from cyber-attacks, as the control/monitoring network and business network in a NPP are separate from the external network. However, consecutive incidents at nuclear facilities, such as the Hatch NPP incident in 2008, the Natanz nuclear facility incident in 2010, the Monju NPP incident in 2014, and the Gundremmingen NPP incident in 2016 have revealed the necessity of cyber security management for NPPs. Nonetheless, compared to other safety-critical infrastructure elements, such as process plants and chemical plants, the development of a cyber-risk assessment method for NPPs is in its infancy.

Several methods have been developed for assessing the levels of cyber-risk at NPPs [2][3][4][5]; however, risk assessment methods so far have been focused on engineering evaluation and expert judgement when developing cyber-attack scenarios. In addition, there was no statistical list of general cyber threats for NPP. In order to consider the applicability to conventional risk analysis method and subjectivity of the developed scenario, the 'initiating threats' has been suggested in the paper. The next section describes the concept and the necessity of the initiating threats.

1.2 Initiating events and initiating threat

Initiating events during a probabilistic safety assessment determine the points of departure of accident sequences that potentially lead to core damage. A missing initiating event in a PSA means that the core damage frequency will be underestimated, and a larger list of initiating events than necessary would result in a waste of resources due to the analyses of additional unnecessary accident sequences. Therefore, the appropriate selections of initiating events are required to assess risk. In the same vein, initiating threats also should have a tidy list for the appropriate assessment of the risks at NPPs. Therefore, in this paper, initiating threats and their estimated probabilities will be proposed as a start to the development of a cyber-risk assessment.

2. Methods and Results

2.1 Operating Experience Analysis

IAEA-TECDOC-719 suggests several methods to collect data pertaining to initiating events: 1) engineering evaluations or technical studies, 2) references to previous PSAs, 3) EPRI lists of initiating events, 4) logical classifications, 5) a plant energy balance fault tree, 6) an analysis of the operation experience of the actual plant, 7) a failure mode and effect analysis, or 8) other methods [8]. Given that there are no former lists or analysis results for assessing NPP initiating threats, operational experience was chosen as the means by which to collect data about initiating threats in this paper. Operational experience includes operational experience reports (henceforth simply OER) from NPPs, department of homeland security (DHS), department of energy (DOE), Industrial control system-cyber emergency response team (ICS-CERT), nuclear threat initiative (NTI), and repository of industrial security incidents (RISI) database [9]-[31]. Total 253 reported incidents occurred from 1988 to 2018 were investigated. Among the reported incidents, 123 incidents caused by the secured development and operational environment (SDOE) were filtered out, as the nuclear industry is the only industry that interprets the incidents caused by SDOE and cyber security separately, among safety-critical industries.

Other 130 incidents were related to the cyber security issues, and among them, 36 incidents were related to the power and utility industry and 16 incidents were directly related to the nuclear industry.

Each of the chosen incidents was documented with descriptions based on the following four characteristics: 1) type of attacker, 2) intentionality, 3) access method, and 4) access type of the attack. Characteristics 1 through 4 are for determining the initiating threat scenarios of attacks by the abovementioned 'focusing on attackers' strategy. Cyber-attack characteristics and properties are shown in table I.

2.2 Scenario Selection

All of the incidents were classified into the following initiating threat scenarios. Table II shows each scenario and the attack characteristics that constitute the scenario.

Table I: Attack Characteristics and their Properties

Attack Characteristics	Properties
Type of Attacker	Outsider
	Insider
Intentionality	Deliberately
	Unintentionally
Access Point	Physical
	Vulnerable Points
	Portable Media
	Phishing e-mail or File-sharing S/W, etc.
	Supply Chain
	Illegal S/W
Access Type	Direct Access
	Remote Access

2.3 Quantification of Threat Probabilities

The 130 security incidents occurred in last 30 years are counted. In cases where the circumstances were not clearly clarified in OER, the occurred number was divided to all possible scenarios. Prior distribution was chosen as beta, and two-stage Bayesian update was applied to prior distribution of an attack.

For the prior distribution, beta distribution of the cyber threat probability of overall industry. In the first stage Bayesian update, the beta distributions were updated with the cyber threat probabilities of power and utility industry. At last in the second stage Bayesian update, the updated distributions were updated once more with the cyber threat probabilities of nuclear industry. Figure 2 through 9 shows the distributions. Yellow line is the prior distribution, orange line is the first-stage distribution, and blue line is the final two-stage distribution.

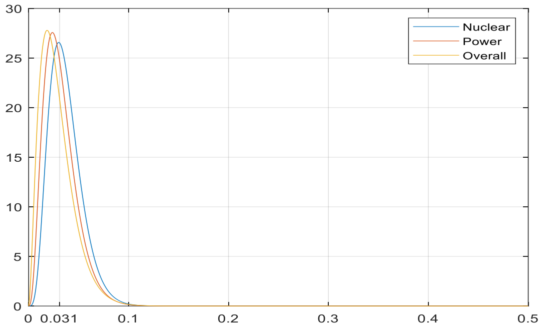

Fig. 1. Two-stage Bayesian Updated Prob. of Scenario 1

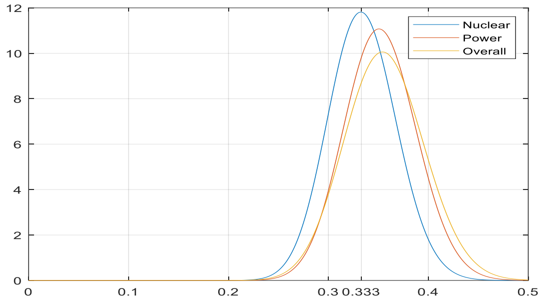

Fig. 2. Two-stage Bayesian Updated Prob. of Scenario 2

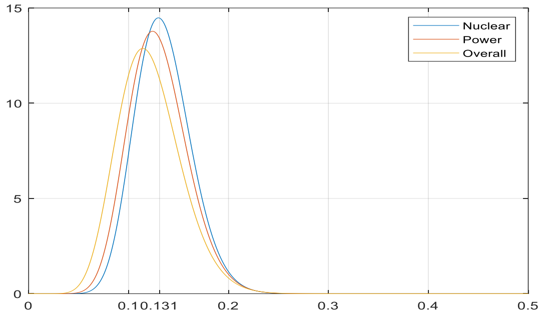

Fig. 3. Two-stage Bayesian Updated Prob. of Scenario 3-1

Table II: Threat Scenarios and their Attack Properties

Threat Scenarios		Type of Attacker	Intentionality	Access Point	Access Type
Scenario 1		Outsider2	Deliberately	Physical Points	Direct Access
Scenario 2		Outsider	Deliberately	Vulnerable Points	Remote Access
Scenario 3	3-1	Outsider	Deliberately	Portable Media	Remote Access
		Insider	Unintentionally	Physical Points	Direct Access
	3-2	Outsider	Deliberately	Phishing e-mail or File-sharing S/W	Remote Access
		Insider	Unintentionally	Physical Points	Direct Access
	3-3	Outsider	Deliberately	Supply Chain	Remote Access
		Insider	Unintentionally	Physical Points	Direct Access
	3-4	Outsider	Deliberately	Illegal S/W	Remote Access
		Insider	Unintentionally	Physical Points	Direct Access
Scenario 4	4-1	Insider	Deliberately	Vulnerable Points	Remote Access
	4-2	Insider	Deliberately	Physical Points	Direct Access

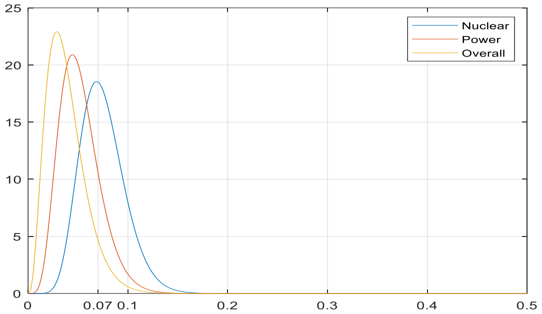

Fig. 4. Two-stage Bayesian Updated Prob. of Scenario 3-2

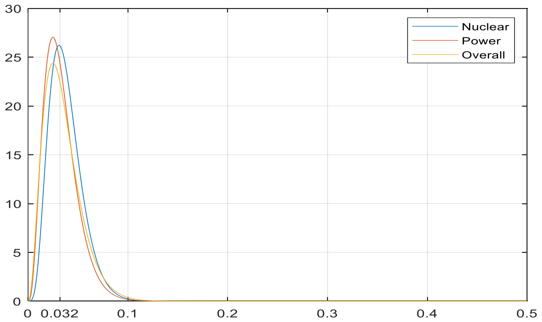

Fig. 5. Two-stage Bayesian Updated Prob. of Scenario 3-3

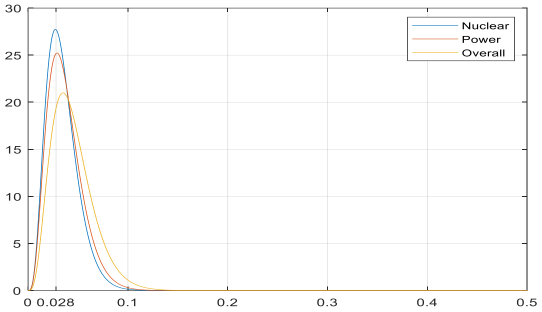

Fig. 6. Two-stage Bayesian Updated Prob. of Scenario 3-4

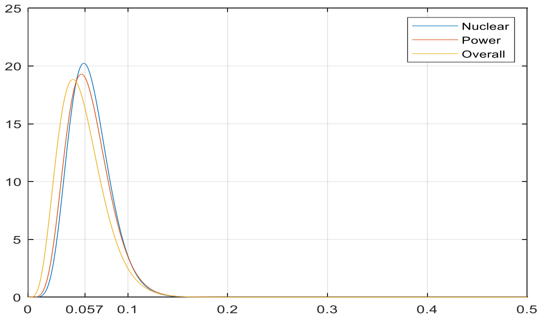

Fig. 7. Two-stage Bayesian Updated Prob. of Scenario 4-1

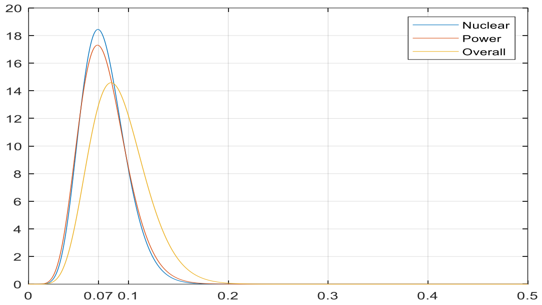

Fig. 8. Two-stage Bayesian Updated Prob. of Scenario 4-2

Maximum likelihood estimation value of each threat scenario is shown in Table III. The reason for the high probability value of threat scenario 2 is that attacks by multiple new worms (Conficker, W32/Korgo, SQL, etc.) in 2003 to 2004 was conducted on plenty of industry platforms, which resulted in prior distribution.

Table III: Estimated Probability of each Scenario

Scenario Number	Estimated Probability
1	1.03 X 10^{-3}/yrs
2	1.11 X 10^{-2}/yrs
3-1	4.37 X 10^{-3}/yrs
3-2	2.33 X 10^{-3}/yrs
3-3	1.07 X 10^{-3}/yrs
3-4	9.33 X 10^{-4}/yrs
3-5	1.90 X 10^{-3}/yrs
3-6	2.33 X 10^{-3}/yrs

3. Conclusions

In this study, to overcome the limitation that the threat scenario classifications of existing cyber security assessment methods are generally focused on the engineering evaluation and expert judgement without statistical analysis, initiating cyber threats were suggested by historical incident analysis. OERs were utilized to conduct threat analyses from the perspective of an attacker for a start of developing a new quantitative cyber security assessment method. Eight initiating threats scenarios and their probabilities were identified.

Incidents were categorized by the four descriptive characteristics: 1) type of attacker, 2) intentionality, 3) access point, and 4) access type, and all the possible eight initiating threats scenarios including subordinate scenarios were identified. Likelihood of initiating threats were estimated with two-stage Bayesian update of beta distribution from general industries. The study is powerful in that it presents all initiating threats scenarios and estimated probabilities were based on the historical data analysis. Although some values tend to be inappropriate than they actually are, the research have significance that it is the first study to probabilistically compute cyber-attacks.

This advance can also be further applied to probabilistic safety assessment (PSA), which is the most widely-using risk assessment method, to describe scenarios and models of NPP cyber-risk and also to quantify cyber-risks.

REFERENCES

[1] https://www.nist.gov/cyberframework, National institute of standard and technology, cyber security framework, 2018.
[2] W. Ahn, et. al., Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs, International Journal of Distributed Sensor Networks, Vol.11, 2015.
[3] S. Jajodia & S. Noel, Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection, and Response, Algorithms, Architectures and Information Systems Security, World Scientific, pp.285-305, New Jersey, 2009.
[4] I. Kotenko & A. Chechulin, A Cyber Attack Modeling and Impact Assessment Framework, Proceeding of the 5th International Conference on Cyber Conflict (CyCon), 2013 5th International Conference on, pp.1-24, Tallinn, Estonia, 2013.
[5] Varuttamaseni, et al., Construction of a Cyber Attack Model for Nuclear Power Plants, 10th NPIC-HMIT, Upton, NY, 2017.
[6] C. KAFOL & A. BREGAR, Cyber Security-Building a sustainable protection, DAAAM INTERNATIONAL SCIENTIFIC BOOK 2017, pp. 081-090, 2017.
[7] A. Shostak, Threat Modeling, Designing for Security, John Wiley & Sons, 2014.
[8] IAEA-TECDOC-719, Defining Initiating Events for Purposes of Probabilistic Safety Assessment, IAEA, September, 1993.
[9] http://www.risidata.com/Database, The repository of industrial security incidents, RISI Online Incident Database, 2015.
[10] P. Neumann, Computer-Related Risks, ACM Press, Addison Wesley, 1995.
[11] M. Bartelt, Group Questions Software's Reliability after Bruce Accident, Canadian Press, 1990.
[12] T. Forester, & M. Perry, Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, Massachusetts Institute of Technology, 2001.
[13] C. Baylon, et al., Cyber Security at Civil Nuclear Facilities: Understanding the Risks, Chatham House, 2015.
[14] http://www.nti.org/gsn/article/russian-warns-of-cyber-terror-against-nuclear-sites, Nuclear Threat Initiative, Russian warns of cyber terror against nuclear sites, 2006.
[15] C. Pfleeger P. & S.L. Pfleeger, Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach, Prentice Hall, 2012.
[16] B. Kesler, The Vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insights, vol. 10, no. 1, pp. 15-25, 2011.
[17] http://www.nrc.gov/docs/ML0329/ML032970134.pdf. Markey, E. J., EDO Principal Correspondence Control, 2003.
[18] U.S. Nuclear Regulatory Commission Office of Nuclear Reactor Regulation, Effects of Ethernet-based, Related Controls on the Safe and Continued Operation of Nuclear Power Stations, 2007.
[19] K. Zetter, Mossad Hacked Syrian Official’s Computer Before Bombing Mysterious Facility, Wired, 2009.
[20] E. Follath, & S. Holger, The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor, Spiegel, 2009.
[21] B. Krebs, Cyber Incident Blamed for Nuclear Power Plant Shutdown, The Washington Post, 2008.
[22] K. Poulsen, Ex-Employee Fingered in Texas Power Company Hack, Wired, 2009.
[23] Symantec Security Response, Stuxnet 0.5: The Missing Link, Symantec, 2013.
[24] J. Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, CCSA Publication, 2013.
[25] D. Albright, et al., Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report. Institute for Science and International Security, Washington, D.C., 2010.
[26] K. Zetter, Top Federal Lab Hacked in Spear-Phishing Attack, Wired, 2011.
[27] V. Arène, Le réseau informatique d'Areva piraté, Le Monde Informatique, 2011.
[28] P. Paganini, Malware based attack hit Japanese Monju Nuclear Power Plant, Security Affairs, 2014.
[29] J. Park & M. Cho, South Korea blames North Korea for December hack on nuclear operator, 2015.
[30] S. Gallagher, German nuclear plant's fuel rod system swarming with old malware, Ars Technica, 2016.
[31] C. Cimpanu, Hackers Steal Research and User Data from Japanese Nuclear Research Lab, Softpedia, 2016.