Application of Cyber Threats to PSA based on External PSA Concept

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

As the importance of cybersecurity emerges in nuclear power plants, studies to measure the risk of cyber security have also been conducted by many researchers. [1]-[8] In particular, attempts to apply cyber security to probabilistic safety assessment (PSA) was often studied, where PSA is the existing method used to analyze safety risks. [9]-[11] However, the developed methodologies have not been widely used, due to meager basis of basic probability suggestion applied to few specific scenarios.

Therefore in the paper, we endeavor to solve the limitations by applying the previously developed cyber threat scenarios and their probabilities to existing PSA. Developed cyber threat scenarios and their probabilities are shown in Table 1. [12]

Then cyber threat scenario are treated as an external event PSA, so that probabilities will be applied to each corresponding basic event.

2. Method

2.1. Existing PSA model

In the study, we chose PSA model of OPR 1000 to apply cyber threats to PSA.

2.2. External event PSA

From the Level 1 PSA perspective, cyber threats are external events, not the internal event (such as LOCAs and transients). Components and systems are not malfunctioning on its own; someone deliberately attacks them to make unavailable. Usually, an external event PSA can be modeled by following steps: 1) Draw a one-top model of an internal event with initiating event probability. 2) Write a mapping table between external events, and BE and IE, and 3) Using the previous mapping table, replace the basic event of the internal event level 1 PSA with the OR logic of the related external events. [13] Then the minimal cutsets can be calculated by removing the product of frequency units.

Table 1. Developed cyber threat scenarios and their probabilities

Threats		Type of attacker	Intentionality	Access point	Access type	Estimated probability
Threat 1		Outsider	Deliberately	Physical points	Direct access	7.20×10^{-4}/yrs
Threat 2		Outsider	Deliberately	Vulnerable points	Remote access	1.13×10^{-2}/yrs
Threat 3	3-1	Insider	Deliberately	Physical points	Direct access	1.26×10^{-3}/yrs
	3-2	Insider	Deliberately	Vulnerable points	Direct access	1.70×10^{-5}/yrs
	3-3	Insider	Deliberately	Vulnerable points	Remote access	1.21×10^{-3}/yrs
	3-4	Insider	Deliberately	Portable Media	Direct access	6.50×10^{-5}/yrs
	3-5	Insider	Deliberately	Phishing or File-sharing	Direct access	6.50×10^{-5}/yrs
	3-6	Insider	Deliberately	Supply chain	Direct access	1.70×10^{-4}/yrs
	3-7	Insider	Deliberately	Illegal S/W	Direct access	6.50×10^{-5}/yrs
	3-8	Insider	Deliberately	Illegal S/W	Remote access	6.50×10^{-5}/yrs
Threat 4	4-1	Insider	Unintentionally	Physical points	Direct access	2.04×10^{-3}/yrs
		Outsider	Deliberately	Vulnerable points	Remote access	
	4-2	Insider	Unintentionally	Portable Media	Direct access	4.23×10^{-3}/yrs
		Outsider	Deliberately	Portable Media	Remote access	
	4-3	Insider	Unintentionally	Phishing or File-sharing	Direct access	3.01×10^{-3}/yrs
		Outsider	Deliberately	Phishing or File-sharing	Remote access	
	4-4	Insider	Unintentionally	Supply chain	Direct access	9.76×10^{-4}/yrs
		Outsider	Deliberately	Supply chain	Remote access	
	4-5	Insider	Unintentionally	Illegal S/W	Direct access	1.46×10^{-3}/yrs
		Outsider	Deliberately	Illegal S/W	Remote access	

2.3. Identification of exploitable basic events

Since the applicable cyber threat scenarios are different for each basic event of the existing PSA, all the basic events in one-top model were examined to identify if they were related to cyber threat scenarios. From the one-top model, the basic events that can be affected by cyber threats are operator action, signal failure, logic failure, and their CCFs. The failure of mechanical components such as SOL and MOV is not considered as an event affected by cyber threat. Not all basic events of all internal events have the potential of cyber threats. For example, in the case of SIT injection of large LOCA, there is no exploitable basic event due to cyber threat.

2.4. The role of RS-015

RS-015 is a document published by KINAC, a Korean nuclear regulatory body, and the document deals with the minimum technical security guards to be prepared to protect cyber threats. [14] By applying RS-015 to the threat, it is possible to additionally analyze whether the actual cyber threat can affect to real system or not. Figure 1 shows the relevance between cyber threats and security guards in RS-015. If an identified basic event is related to threat 1, 2 and 3-3, then "Access control through account management", "Identification and authentication", "CDA's own features and configuration", "Session lock", "Control of mobile media that can be connected with CDA", "Malware detection and removal plan & update", "Restriction of authority upon change and termination of work", and "Network control" are the security guards that the system should have. Only when all RS-015 security guards associated with Threats 1, 2, and 3-3 are followed, the identified exploitable basic event can be said to be completely free from the impact of the threats.

Each security guard is subdivided into several implementation practices, which are tied to OR gate. For example, the security guard, "Identification and authentication" have several implementation practices, as shown in Figure 2. If all practices in the security guard are followed, it can be said that the identified basic event is not affected by Threat 1, Threat 2, and Threat 3-3.

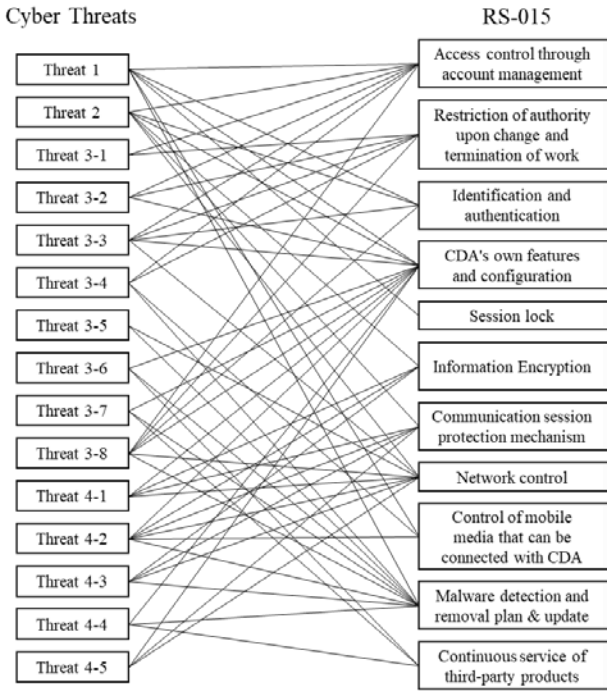

Fig 1. Relationship between cyber threats and RS-015 security guards

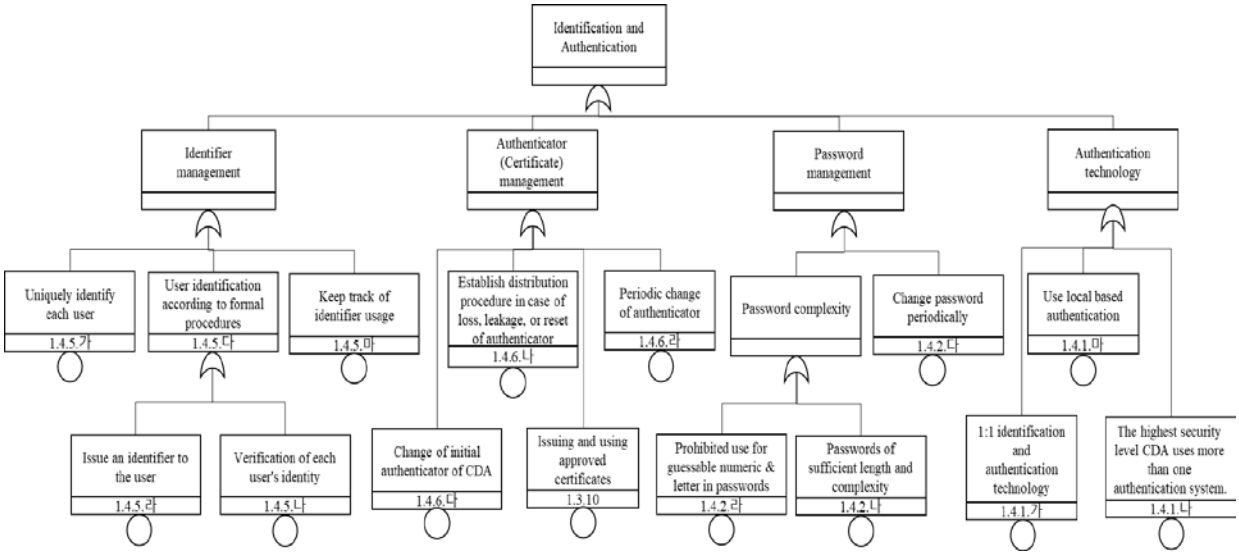

Fig 2. An example of security guard and its sub-practices

3. Results

As mentioned in section 2.3, exploitable basic events in existing PSA are currently being listed up for 12 initiating events. Mainly, relays and logic matrices that send manual or automatic trip signals were selected as related basic events, and CCFs that could occur in the relays and logic matrices were also identified to be related. The example of mapping table is shown in table 2. Table shows exploitable basic events of 2 mitigation systems, FW and BD in initiating event of general transient among numerous mitigation systems.

Table 2. An example of mapping table between exploitable basic events and cyber threats

Initiating event	Mitigation system	Exploitable basic events	Related cyber threats (T)
General Transients	Deliver main or auxiliary feed water (FW)	CCF of interface relay/contact (FSXRWX12343S6)	T1, T3-1, T3-2, T3-3, T3-6, T4-1, T4-4
		CCF of initiation K-relays in panel (FSKRWK1234S6)	T1, T3-1, T3-2, T3-3, T3-6, T4-1, T4-4
		CCF of all interposing R/C (FSQRWQ6-ALLS6) (FSQRWQRAJ3005)	T1, T3-1, T3-2, T3-3, T3-6, T4-1, T4-4
		No signal from logic matrix trip paths for interposing relay (GFSS6Q61LM-SN) (GFSS6Q62LM-SN) (GFSS6Q63LM-SN) (GFSS6Q64LM-SN)	T1, T3-1, T3-2, T3-3, T3-6, T3-7, T3-8, T4-1, T4-4, T4-5
		CCF of manual trip push buttons (FSMWWHS106ABCD)	T1, T3-1, T3-2, T3-3, T3-6, T3-7, T3-8, T4-1, T4-4, T4-5
		Operator fails to manually generate AFAS (FSOPVAFAS)	T1, T3-1, T3-2, T3-3, T3-6, T3-7, T3-8, T4-1, T4-4, T4-5
		Failure of DPS signal Processor (DPSKAPLC1) (DPSKAPLC2)	T1, T2, T3-1, T3-2, T3-3, T3-4, T3-6, T3-7, T3-8, T4-1, T4-2, T4-4, T4-5
		CCF of DPS signal processors (DPSKWPLCALL)	T1, T2, T3-1, T3-2, T3-3, T3-4, T3-6, T3-7, T3-8, T4-1, T4-2, T4-4, T4-5
		DPS is in Bypass (DPSKMPLC)	T1, T2, T3-1, T3-2, T3-3, T3-4, T3-6, T3-7, T3-8, T4-1, T4-2, T4-4, T4-5
		SG to LVL transmitter fails to provide proper output during operation (FWLTYLT1115X) (FWLTYLT1115Y)	T1, T3-1, T3-2, T3-3, T3-6, T4-1, T4-4
		CCF of SG to LVL transmitter (FWLTKLT1115XY)	T1, T3-1, T3-2, T3-3, T3-6, T4-1, T4-4
		Measurement loop for SG Lo LVL fails to provide proper output (PNMLYLT1115X) (PNMLYLT1115Y)	T1, T3-1, T3-2, T3-3, T3-6, T3-7, T3-8, T4-1, T4-4, T4-5
		CCF of measurement loops for SG Lo LVL (PNMLKLT1115XY)	T1, T3-1, T3-2, T3-3, T3-6, T3-7, T3-8, T4-1, T4-4, T4-5
	Bleed RCS (BD)	Operator fails to perform F&B operation (SDOPHLATE)	T1, T3-1, T3-2, T3-3, T3-6, T3-7, T3-8, T4-1, T4-4, T4-5
		Failure of PCS card (SDISAMV101) (SDISAMV102) (SDISAMV102) (SDISAMV102)	T1, T3-1, T3-2, T3-3, T3-6, T4-1, T4-4

The case when outsider directly approached and attempted an attack should be included (Threat 1), but there is few path for outsider to remotely attack due to the network separation (Threat 2). In the case of insider threats, almost all exploitable basic events were involved (Threat 3). In most cases of exploitable basic events, threats such as Threat 3-4, Threat 3-5, and Threat 3-8 were excluded because portable media cannot be connected to the actual circuit board or malicious programs cannot be run. The situation is similar for the insider-outsider combined threat. (Threat 4)

4. Further Work

After mapping table is completed, it is possible to finally obtain the CDF change due to the cyber threat by applying the corresponding cyber threat probabilities and security guards to each exploitable basic event.

Through cutset analysis and changes in CDF, it is possible to determine which cyber threats have the largest impact on the system and which security guards should be followed to reduce CDF.

5. Conclusion

In this preliminary study, we applied the previously developed initiating cyber threat scenarios and their probability values to the existing PSA. If we proceed to further work, it is possible to confirm the CDF change, and find out the most influential basic events induced by cyber threat. The study has significance that it applied security to the existing PSA model with properly suggested probability values, and further it can be the basis for analyzing security issues with the safety aspects

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] A. 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] J.W. Park and S.J. Lee. Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants. Nuclear Engineering and Technology Vol. 51 pp.138-145, 2019.
[10] H.E. Kim, et al. Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants. Reliability Engineering & System Safety 167, pp.290-301, 2017.
[11] J.,S. Shin, et al. Methodology for Applying Cyber Security Risk Evaluation from BN Model to PSA Model, 2014.
[12] S.M Han and P.H. Seong, Development of Initiating Cyber Threat Scenarios and the Probabilities Based on Operating Experience Analysis, Transactions of the Korean Nuclear Society Spring Meeting, Jeju, Korea, 2020.
[13] KR20080095535A, A method of quantifying external events PSA including inter-compartment propagation, 2008.
[14] KINCA, RS-015, Computer and information system security of nuclear facilities, 2016.