Development of a Nuclear Power Plant Safety and Cyber Security Combined Risk Analysis Method Based on Probabilistic Safety 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

Traditionally the risk of a nuclear power plant (NPP) is calculated using the mechanical failures of the components, but this is evolving and expanding via consideration of various other factors. The first NPP risk quantification using component mechanical failure was conducted in 1975 [1], and the effects of human errors and external events were analyzed from the late 1980s. NPP risk assessments have not included cyber security factors since NPPs have been generally assumed to be secure from cyber-attacks so far. However, recent cyber incidents at nuclear facilities have revealed the necessity for developing cyber risk assessment methods for NPPs. [2]-[8]

US NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Power Facilities," was released in 2010, [9] and NRC has prepared and commenced full implementation and inspection of security controls from 2017. [10] The Korean domestic regulatory body, Korea Institute of Nuclear Nonproliferation and Control (KINAC), published the RS-015 standard "Regulatory Standard on Cyber Security for Nuclear Facilities" in 2014. [11] Unlike other IT/ICS fields that have been evaluating cyber risk since the 1980s, NPPs have recently legislated regulations and implemented security controls; thus, it can be said that the development of cyber risk assessments for NPPs is still in its infancy.

The study claims that the cyber threats should be included in the external probabilistic safety assessment (PSA). The advantages of quantifying cyber risk based on PSA model are as follows: 1) It is possible to do both qualitative and quantitative assessment through cutset analysis, 2) All potential cyber attacks to a whole system can be considered at once. 3) Objectivity of the safety-cyber security risk can be achieved at the same time.

Usually, an external event PSA is modeled in the following steps: 1) Draw a one-top model and calculate minimal cutsets (MCSs) of an internal event with core damage as the one-top event., 2) Write a mapping table between external events and basic events (BEs)/internal events (IEs), 3) Using the previous mapping table, replace the initial event of the internal event level 1 PSA with the 'OR' logic of the related external events. [12],[13] For an exemplary case of external PSA with cyber threats, the PSA model is modified as shown in figure 1 and 2. In this case, a mapping table marked as yellow box is being used.

As seen in the aforementioned steps, external PSA defines the relationship between external factors and basic events or internal events using a mapping table. In this study, we will suggest a method for estimating combined risk of safety and cyber security and show the result of case study.

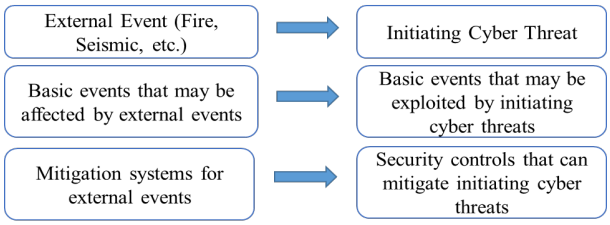

Fig 1. Relationship between external threat and cyber threat when applying cyber threats to external PSA

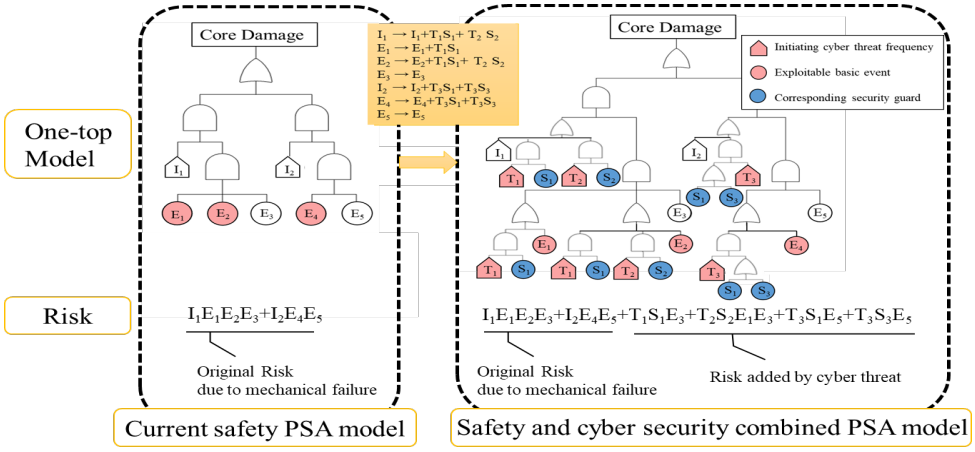

Fig 2. External PSA model with the consideration of cyber threats

2. Methods and Results

The cyber security factors were applied to the existing PSA model in the same way as the external PSA. For case study, PSA model of OPR 1000 was chosen, and the cut-off frequency was set to 1.0E-11. The cyber threat list and frequency were calculated from our previous study [14].

Table 1. Basic information for case study

IEs	CDF	# of exploitable MCSs /# of MCSs
ATWS	1.081E-06	81/322
GTRN	1.914E-07	510/1820
LLOCA	9.213E-09	0/104
LOCCW	3.096E-07	982/2764
LOCV	7.245E-09	24/77
LODC	6.918E-07	390/1657
LOFW	2.845E-07	231/1858
LOKV	7.556E-08	546/1379
LOOP	1.210E-06	601/6723
LSSB	2.534E-07	36/366
MLOCA	8.619E-08	132/748
SBO	1.204E-06	43/842
SGTR	1.242E-06	455/1865
SLOCA	1.326E-07	56/331
Others	3.202E-07	1/22
Total	7.107E-06	4088/20877

The relationship of exploitable BE and corresponding cyber threat/security controls used in the case study analysis is shown in Table 2.

Table 2. Mapping table between exploitable BE and cyber threat/security controls

The types of exploitable BE	**Related cyber threat**	**Related security controls**
PCS Card failure	T1, T3-1, T3-6, T4-4	1,2,3,4,5,6,7,9,10,11
Screen on MCR failure	T1, T3-1, T3-2, T3-4, T3-6, T3-7, T4-2, T4-4, T4-5	1,2,3,4,5,6,7,8,9,10,11
Wrong Bypass	T1, T3-1, T3-2, T3-4, T3-6, T3-7, T4-2, T4-4, T4-5	1,2,3,4,5,6,7,8,9,10,11
Bi stable Processor failure	T1, T3-1, T3-4, T3-6, T4-4	1,2,3,4,5,6,7,9,10,11
ESFAS signal failure	T1, T3-1, T3-4, T3-6, T4-4	1,2,3,4,5,6,7,9,10,11

Table 3 shows the result of the case study. Each combined risk was calculated for the cases when all security controls exist, one security control does not exist, and all security controls do not exist. The values marked in red are those whose CDF has increased significantly as the corresponding security control does not exist, and the blue values are values that are hardly affected by the presence or absence of the security control.

Table 3. Case study result of a combined risk analysis based on PSA

IEs	**CDF with all SCs**	**CDF w/o SC 1**	**CDF w/o SC 2**	**CDF w/o SC 3**	**CDF w/o SC 4**	**CDF w/o SC 5**	**CDF w/o SC 6**	**CDF w/o SC 7**	**CDF w/o SC 8**	**CDF w/o SC 9**	**CDF w/o SC 10**	**CDF w/o SC 11**	**CDF w/o any SCs**
ATWS	1.081E-06	3.012E-06	3.000E-06	3.072E-05	5.627E-06	2.489E-06	5.790E-06	5.961E-06	1.598E-06	5.961E-06	1.187E-06	1.187E-06	1.990E-05
GTRN	1.914E-07	8.244E-07	2.064E-07	2.077E-07	2.111E-07	2.064E-07	1.930E-07	1.930E-07	1.914E-07	1.930E-07	1.927E-07	1.927E-07	2.905E-07
LLOCA	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09	9.213E-09
LOCCW	3.096E-07	4.342E-07	3.513E-07	3.559E-07	3.685E-07	3.513E-07	3.139E-07	3.139E-07	3.096E-07	3.139E-07	3.130E-07	3.130E-07	6.513E-07
LOCV	7.245E-09	8.494E-09	7.767E-09	1.795E-07	7.911E-09	7.767E-09	7.299E-09	7.299E-09	7.245E-09	7.299E-09	7.288E-09	7.288E-09	1.040E-08
LODC	6.918E-07	1.206E-06	7.860E-07	8.094E-07	8.791E-07	7.860E-07	7.017E-07	7.017E-07	6.918E-07	7.017E-07	6.996E-07	6.996E-07	2.305E-06
LOFW	2.845E-07	3.328E-07	2.939E-07	2.960E-07	3.025E-07	2.939E-07	2.855E-07	2.855E-07	2.845E-07	2.855E-07	2.852E-07	2.852E-07	4.349E-07
LOKV	7.556E-08	1.029E-07	8.397E-08	8.502E-08	8.795E-08	8.397E-08	7.646E-08	7.646E-08	7.556E-08	7.646E-08	7.626E-08	7.626E-08	1.525E-07
LOOP	1.210E-06	1.663E-06	1.275E-06	1.296E-06	1.367E-06	1.503E-06	1.217E-06	1.217E-06	1.210E-06	1.217E-06	1.215E-06	1.215E-06	2.679E-06
LSSB	2.534E-07	3.990E-07	2.796E-07	2.796E-07	3.061E-07	1.275E-06	2.562E-07	2.562E-07	2.534E-07	2.562E-07	2.556E-07	2.556E-07	7.115E-07
MLOCA	8.619E-08	1.108E-07	9.139E-08	9.247E-08	9.559E-08	2.796E-07	8.673E-08	8.673E-08	8.619E-08	8.673E-08	8.662E-08	8.662E-08	1.617E-07
SBO	1.204E-06	1.214E-06	1.215E-06	1.219E-06	1.232E-06	1.206E-06	1.206E-06	1.206E-06	1.204E-06	1.206E-06	1.205E-06	1.205E-06	1.469E-06
SGTR	1.242E-06	1.008E-05	1.627E-06	9.267E-06	1.717E-06	1.215E-06	1.327E-06	1.329E-06	1.249E-06	1.329E-06	1.264E-06	1.264E-06	5.270E-06
SLOCA	1.326E-07	4.573E-06	1.678E-07	1.516E-06	1.893E-07	1.659E-07	1.528E-07	1.535E-07	1.345E-07	1.535E-07	1.353E-07	1.353E-07	5.846E-05
Others	3.202E-07	3.208E-07	3.203E-07	3.203E-07	3.204E-07	3.203E-07	3.202E-07	3.202E-07	3.202E-07	3.202E-07	3.202E-07	3.202E-07	3.222E-07
Total	7.107E-06	1.157E-05	9.715E-06	4.665E-05	1.272E-05	9.078E-06	1.194E-05	1.212E-05	7.625E-06	1.212E-05	7.253E-06	7.253E-06	9.283E-05

In a broad sense, the CDF increase is maximal for the ATWS sequence without security control, and the CDF increases are minimal for the LLOCA, LOOP, and Other(ISL, RVR, and CSGTR) sequences. The more devices that need to be actually operated, the greater the influence on the CDF increase, whereas the automatically mitigation sequence did not affect the CDF increase. Individually, the exploitable BEs that primarily increase the CDF are as follows: DPSKAPLC1,2 (Failure probability before exploitation: 7.253E-03), DPSKAPLCALL (Failure probability exploitation: 2.396E-03), RPBIKALL (Failure probability before exploitation: 4.836 E-06), and RPOPVTRIP (Failure probability before exploitation: 1.110E-02). First two basic events are the cases when the failure probability of the exploitable BE itself is large, and others are the BEs when the failure probability of the exploitable BE is not large but the failure probability of operator manual trip bound with the same MCS is large.

Assuming that none of SCs are implemented, the CDF increases by a factor of 13 compared to its original value, (7.107E-6 to 9.283E-05) and from the results of sensitivity analysis, the security control “Identification and Authentication” is observed to significantly increase CDF. In other words, the security control “Identification and Authentication” is the most effective security control in nuclear power plants.

3. Conclusions

In this study, we suggested a method to estimate combined risk of the NPP by applying cyber security factors to external PSA model. The merits of the suggested method is as follows:

1) Unlike most of the previous studies, the developed combined safety and cyber security risk analysis method can evaluate the full scope NPP risk as well as the effects of proposed security controls such as RS-015 quantitatively.
2) The developed risk analysis method is useful in the security control implementation phase as well as security requirement analysis, security function design, and maintenance phases.
3) In the proposed method, the mapping table can be easily modified via the developed S/W, unlike other methods that require modifications of the entire models for changes. The combined risk can also be calculated within a short time with the developed S/W.

REFERENCES

[1] Rasmussen, Professor Norman C.; et al. (October 1975). "Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants. Executive Summary". WASH-1400 (NUREG-75/014). Rockville, MD, USA: Federal Government of the United States, U.S. Nuclear Regulatory Commission.

[2] Lewis, Ted G. Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons, 2019.

[3] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5.6 (2011): 29.

[4] David Albright, et. al, Stuxnet Malware and Natanz, Institute for Science and International Security, 16 Feb. 2011 https://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf (accessed 2 February 2021)

[5]Japan Today, Monju power plant facility PC infected with virus, 07 January 2014. http://www.japantoday.com/category/national/view/monju-power-plant-facility-pc-infected-with-virus (accessed 2 February 2021)

[6] Maiziere, T. D. "Die lage der it-sicherheit in deutschland 2015." Bundesamt für Sicherheit in der Informationstechnik (2015).

[7] Steitz, Christoph, and Eric Auchard. "German nuclear plant infected with computer viruses, operator says." http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS (accessed 17 Apr. 2016).

[8] Baylon, Caroline et al., Chatham House, "Cyber Security at Civil Nuclear Facilities: Understanding the Risks", 6 Oct. 2015 https://www.chathamhouse.org/2015/10/cyber-security-civil-nuclear-facilities-understanding-risks (accesssd 2 February 2021)

[9] US. NRC. Status of NRC Licensees’ Implementation of Cyber Security Plans NRC/FERC Joint Commission Meeting February 23, 2017

[10] US Nuclear Regulatory Commission. *Cyber security programs for nuclear facilities*. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2010.

[11] KINAC/RS-015.01, “Regulatory Standard on Cyber Security for Nuclear Facilities”, December, 2016

[12] J.E. Yang, J.J. Ha, et al. KR100856500B1, A method for quantitive evaluation of the damage frequencies of reactor core on external accidents at nuclear power plant, 2008

[13] J.E. Yang, KR101594418B1, PSA Quantification system and method for the combined external hazards, 2016

[14] 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, May 21-22, 2020