Setting Component Priorities in Protecting NPPs against Cyber-Attacks Using Reliability Analysis Techniques

Moon Kyoung Choi [a],Han Seong Son [b], 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*
[b]*Department of Computer and Game, Joongbu Univiersity, 201 Daehak-ro, Chubu-myun, Geumsan-gun 32713, Republic of Korea*
[*]*Corresponding author: phseong1@kaist.ac.kr*

1. Introduction

As the main systems for managing totally about the operation, control, monitoring, measurement, and safety function in an emergency, instrumentation and control systems (I&C) in nuclear power plants have been digitalized gradually for the precise operation and its convenience [1]. However, these changes have some problems in terms of cyber security. The digitalization of infrastructure makes systems vulnerable to cyber threats and hybrid attacks. According to ICS-CERT report, as time goes by, the number of vulnerabilities in ICS industries increases rapidly [2]. Recently, due to the digitalization of I&C, it has begun to rise the need of cyber security in the digitalized I&C in NPPs [3] [4]. Many engineers insist that I&C systems of NPPs are physically isolated from external networks so NPPs are regarded safe from external cyber-attacks [3]. However, continuous cyber-attacks against NPPs have signified that NPPs are as susceptible to cyber-attacks as other critical infrastructures, and public perceptions of cyber security for NPPs have changed [4]. The representative example is Stuxnet attack to Iran nuclear facilities. On July 2010, Stuxnet destroyed about 1000 centrifuges at Iran's uranium enrichment facility in Natanz. The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a sophisticated adversary with a detailed knowledge of I&C system can be very critical on safety-related infrastructures [5].

For the cyber security of nuclear facilities, KINAC responds to cyber threats by controlling over 100 security measures based on KINAC / RS-015, a regulatory standard established according to international guidelines. The KINAC / RS-015 seeks to improve the efficiency and effectiveness of regulations, including the introduction of performance based regimes, by improving the existing Prescriptive Regulation. However, 70 ~ 80% of digital assets are being checked collectively as a regulated target, and there is a difficulty in the same management by the actual regulated object. It is necessary to identify the critical accident-related components that should be protected against cyber-attacks. Regulatory effectiveness needs to be improved through the adoption of defense-in-depth regulation requirements by adopting a graded approach.

Reliability analysis techniques such as event tree analysis and fault tree analysis are used to identify components that could evoke an accident of NPPs by cyber-attacks. First of all, target initiating events are selected, and each heading that can be affected by cyber-attacks is analyzed through event tree analysis. Minimal cut-sets of each selected heading are elicited by performing fault tree analyses. It is suggested that the importance factor is the number of basic events consisting of the minimal cut-sets rather than probabilities. Based on these steps, the process for setting component priorities in protecting NPPs against Cyber-attacks using reliability analysis techniques is suggested.

2. Elicitation of accident-related CDAs

2.1 Event tree analysis for selection of headings related to cyber-attacks

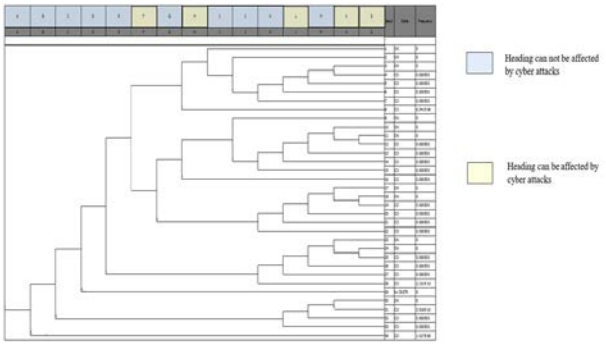

Fig. 1. Event tree analysis for if each headings can be affected by cyber-attacks

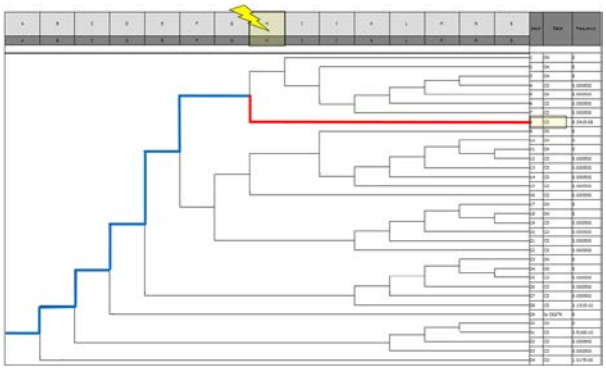

Fig.2 Event tree analysis for if each headings can be affected by cyber-attacks

In terms of cyber-attack, event tree analysis begins by analyzing the heading of the event tree to determine if each heading is capable of cyber-attack as shown in Fig. 1. If headings of event trees can be fail due to cyber-attacks, we should analyze whether they can directly cause the core damage as shown in Fig. 2. However, the headings related to only physical and chemical factors, not cyber-attacks, were excluded.

2.2 Fault tree analysis of selected headings

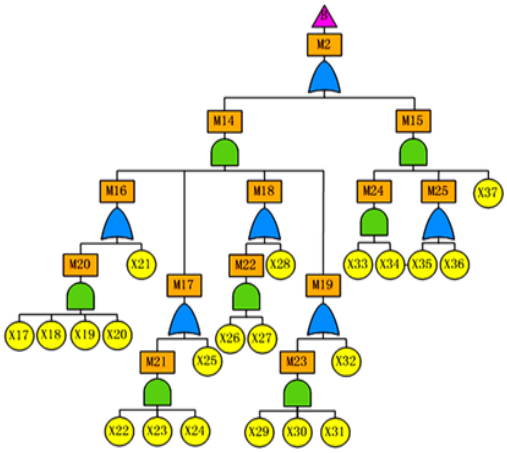

Fig.3 Fault tree analysis for selected headings

Fault tree analysis (FTA) is a top down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. This analysis method is mainly used in the fields of safety engineering and reliability engineering to understand how systems can fail, to identify the best ways to reduce risk or to determine event rates of a safety accident or a particular system level (functional) failure. It is necessary to identify the both roles and success criteria of safety functions and operators required to construct fault tree. For selected headings, fault trees are drawn as shown in Fig. 3, and these are analyzed for getting minimal cut-sets.

2.3 Consideration for setting priorities of components against cyber-attacks

The safety assessment methodology based on probabilistic analysis generally uses failure probability of systems. This value reflects a mechanical fault or the operator's mistake. However, it is difficult to predict when a malicious attacker will intentionally cause system and device malfunctions. Thus, using quantitative probability values is not appropriate in the case of a malfunctioning device due to cyber-attack. There is a limitation in deriving accident-related CDAs by using mechanical failure rate.

Several cyber security researchers believed that cyber security level could be increased as the effort expended by an attacker increases [7]. With this regard, two assumptions were suggested.

1) Probability of active attack is inversely proportional to difficulty of an actions needed for active attack.

2) Difficulty of actions is proportional to effort expended by an attacker.

In the original PSA method so far, the case where the probability value is high is given priority, but when analyzing the failure due to the intentional attack, it is necessary to consider the degree of effort of the attacker rather than the probability value of the accident. It is important to determine how few of the basic events constitute the minimum cut-sets that result in failure of selected important headings, rather than how high the probabilities are. In other words, the fewer basic events systems have, the greater the vulnerability is. In specially, the cases consisting of only one basic event should be secured thoroughly compared to others. In general, the cases consist of a basic event related to common cause failure of components. In terms of cyber-attacks, the redundancy of components is not important. If attacks already know the specific information of one of components having redundancy, attackers can easily compromise other redundant components. Therefore, the minimal cut-sets consisting of a basic event related to common cause failure should be protected than those consisting of different basic events.

2.4 Consideration for setting priorities of components against cyber-attacks

No	Value	F-V	BE#1	BE#2	BE#3	BE#4
2	5.67E-05	0.173	AABBWW501&4			
3	3.25E-05	0.099	AAMPWPP1234			
6	0.000024	0.073	AAHXBREGHX			
12	2.4E-06	0.007	AATKBRWT00			
1	9.54E-05	0.292	AAMPK123T	GG-AA-PP04-T		
4	2.59E-05	0.079	AAISABB534	AAISABB536		
5	2.59E-05	0.079	AAISABB501	AAISABB504		
8	7.07E-06	0.022	AAISABB536	AABBOCH534		
9	7.07E-06	0.022	AAISABB534	AABBOCH536		
10	7.07E-06	0.022	AAISABB501	AABBCCH504		
11	7.07E-06	0.022	AAISABB504	AABBCCH501		
13	2.08E-06	0.006	AAISABB536	AABBT0530B		
14	1.93E-06	0.006	AABBCCH501	AABBCCH504		
15	1.93E-06	0.006	AABBOCH534	AABBOCH536		
16	1.15E-06	0.004	AAAAOCH191	AAISABB536		
17	1.15E-06	0.004	AAAAO0305B	AAISABB536		
18	1.15E-06	0.004	AAAAOCH190	AAISABB534		
19	8.81E-07	0.003	AAISABB534	AALTYL226		
20	8.81E-07	0.003	AAISABB504	AALTYL226		
21	8.81E-07	0.003	AAISABB501	AALTYL227		
22	8.81E-07	0.003	AAISABB536	AALTYL227		
23	7.51E-07	0.002	AAAVTCH532	AAISABB534		
24	5.69E-07	0.002	AABBOCH536	AABBT0530B		
25	3.13E-07	1E-03	AAAAOCH191	AABBOCH536		
26	3.13E-07	1E-03	AAAAO0305B	AABBOCH536		
27	3.13E-07	1E-03	AAAAOCH190	AABBOCH534		
28	2.41E-07	7E-04	AALTYL227	AABBCCH501		
29	2.41E-07	7E-04	AALTYL226	AABBCCH504		
30	2.41E-07	7E-04	AALTYL227	AABBOCH536		
31	2.41E-07	7E-04	AALTYL226	AABBOCH534		
32	2.05E-07	6E-04	AAAVTCH532	AABBOCH534		
7	1.8E-05	0.055	%U3-LOOP	AAMPW123T-L	GG-AA-PP04-T	
33	1.32E-07	4E-04	AAMPK12D	AAMPSCHGP3	GG-AA-PP03-SB	GG-AA-PP04-T
34	9.54E-08	3E-04	AAMPK12D	AAMPMCHGP3	GG-AA-PP03-SB	GG-AA-PP04-T

Fig.4 Example of arrangement of minimal cut-sets according to priorities

Fig.4 indicates an example of arrangement of minimal cut-sets according to priorities. In Fig.4 no.1 case consisting of two basic events has relative high probability value rather than no.3 case consisting of

only one basic events, but no. 3 case is more vulnerable to cyber-attacks than no. 1 case in terms of cyber security.

3. Conclusions

Digital I&C systems have been developed and installed in nuclear power plants, and due to installation of the digital I&C systems, cyber security concerns are increasing in nuclear industry. However, there are too many critical digital assets to be inspected in digitalized NPPs. In order to reduce the inefficiency of regulation in nuclear facilities, the critical components that are directly related to an accident are elicited by using the reliability analysis techniques. Target initial events are selected, and their headings are analyzed through event tree analysis about whether the headings can be affected by cyber-attacks or not. Among the headings, the headings that can be proceeded directly to the core damage by the cyber-attack when they are fail are finally selected as the target of deriving the minimum cut-sets. We analyze the fault trees and derive the minimum set-cuts. In terms of original PSA, the value of probability for the cut-sets is important but the probability is not important in terms of cyber security of NPPs. The important factors is the number of basic events consisting of the minimal cut-sets that is proportional to vulnerability.

The results of this study are expected to be used to derive the linkage between cyber-attack and accident, and to develop the final core digital asset identification methodology and effective regulatory method.

REFERENCES

[1] Y.D. Kang, “A study on Cyber Security Assessment Methodology of Instrumentation & Control Systems for Nuclear Power Plants”, Ph.D. thesis, 2011

[2] National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team, “NCCIC/ICS-CERT Year in Review”, Homeland Security, pp.7-19, 2015

[3] J.Park and Y. Suh, “A development framework for software security in nuclear safety systems: integrating secure development and system security activities,” *Nuclear Engineering and Technology*, vol. 46, pp. 47-54 (2014)

[4] Baylon, Croline, Roger Brunt, and David Livingstone, “*Cyber Security at Civil Nuclear Facilities Understanding the Risks*”, London: Chatham House, 2015

[5] Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack”, Strategic Insights, Vol 10, pp 15-25, 2011

[6] I.H. Shin, “ROK’s Regulatory Framework for Cyber Security of Nuclear Facilities”, KNS, Kyeongju, May 11-13, 2016

[7] Dacier, Marc, Yves Deswarte, and Mohamed Kaanichel, “Quantitative assessment of operational security: Models and tools”, Information Systems Security, Ed. By SK Katsikas and D.Gritzalis, London, Chapman & Hall, pp.86-179, 1996

Acknowledgement

This work was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety (KOFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea (Grant code: 1605007-0116-WT111)