IDENTIFICATION OF THE ACCIDENT-RELATED CRITICAL DIGITAL ASSETS BASED ON PROBABILISTIC SAFETY ANALYSIS RESULTS

Moon Kyoung Choi and Poong Hyun Seong*
Korea Advanced Institute of Science and Technology (KAIST)
Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,
291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
stsk9107@kaist.ac.kr; phseong1@kaist.ac.kr*

Han Seong Son
Department of Computer and Game
Joongbu Univiersity
201 Daehak-ro, Chubu-myun, Geumsan-gun 32713, Republic of Korea
hsson@jbm.ac.kr

ABSTRACT

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 (CDAs) to be inspected in digitalized NPPs. In order to reduce the inefficiency of regulation in nuclear facilities, the critical digital assets that are directly related to an accident are elicited by using the probabilistic safety assessment results. Target initial events are selected, and their heading are analyzed through event tree analysis. Among the headings, the headings that can be proceeded directly to the core damage by the cyber-attack are finally selected as the target of deriving the minimum cut-sets. Based on success criteria of each heading, 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. Finally, the process for identifying accident-related CDAs is suggested based on PSA results. 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.

Key Words: Cyber Security, Event tree analysis, Fault tree analysis, Minimal Cut sets

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 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]. For example, on January 25, 2003, the Davis-Besse nuclear power plant in Oak Harbour Ohio was infected with the MS SQL 'Slammer' worm. As a result, for four hours and fifty minutes, plant personnel could not

access the Safety Parameter Display System (SPDS), which shows sensitive data about the reactor core collected from coolant systems, temperature sensors, and radiation detectors—these components would be the first to indicate meltdown conditions. Another 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.

Too many digital assets are being checked collectively as a regulated target, and there is a difficulty in the same management by the actual regulated object. Current cyber security regulations on nuclear power plants are inefficient due to the same cyber security regulations applied to digital assets that perform safety, security, and emergency response functions [6]. In addition, because cyber-attacks evolve as a way of avoiding defenses, it is necessary to analyze the critical digital assets (CDAs) related to nuclear accidents. Regulatory effectiveness needs to be improved through the adoption of defense-in-depth regulation requirements by adopting a graded approach by deriving critical digital assets that directly relate to accidents.

Probabilistic Safety Analysis (PSA) results are analyzed in order to identify more CDAs that could evoke an accident of NPPs by digital malfunction or cyber-attacks. Minimal cut-sets 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 eliciting accident-related CDAs is suggested, and finally CDAs that must be secured from attackers are elicited.

2 ELICITATION OF ACCIDENT-RELATED CDAS

2.1 Event Tree Analysis for Selection of Headings Related to Cyber-attacks

In an ordinary level 1 PSA, an event tree analysis consists of an event tree for selected initial events to identify all critical events that lead to core damage. The event tree shows how an accident develops depending on whether the systems successfully operates or not. In addition, when each initial event occurs, the accident scenario is logically constructed in the form of a binary tree according to the success or failure of each headings.

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.

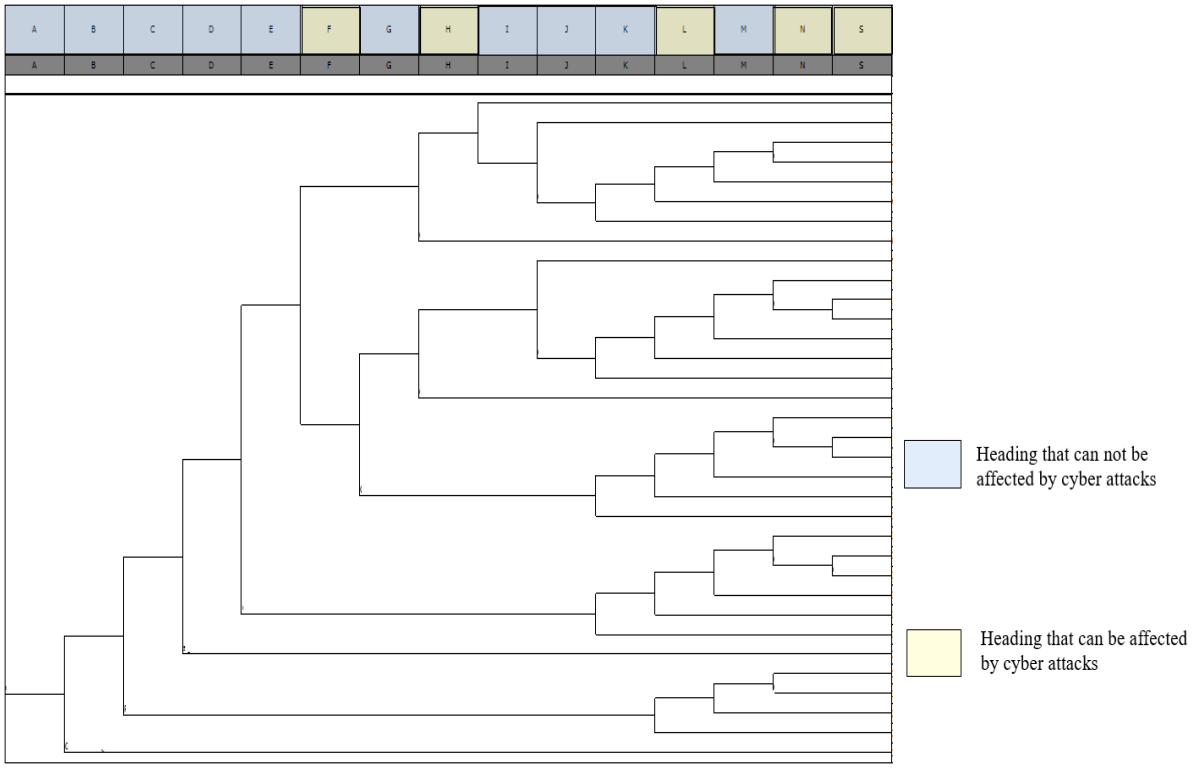

Fig.1 Event tree analysis for if each headings can be affected by cyber-attacks

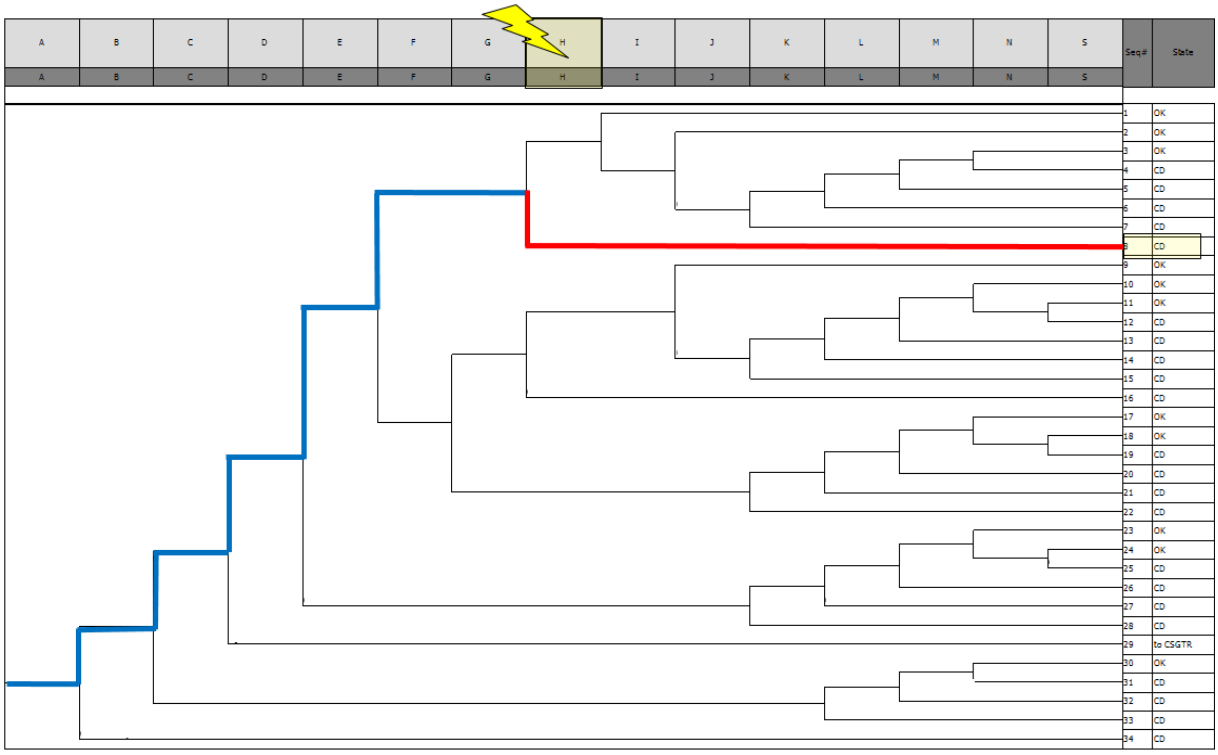

Fig.2 Event tree analysis for if each headings can be affected by cyber-attacks

2.2 Fault Tree Analysis of 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 [7]. 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, and these are analyzed for getting minimal cut-sets as shown in Fig. 3.

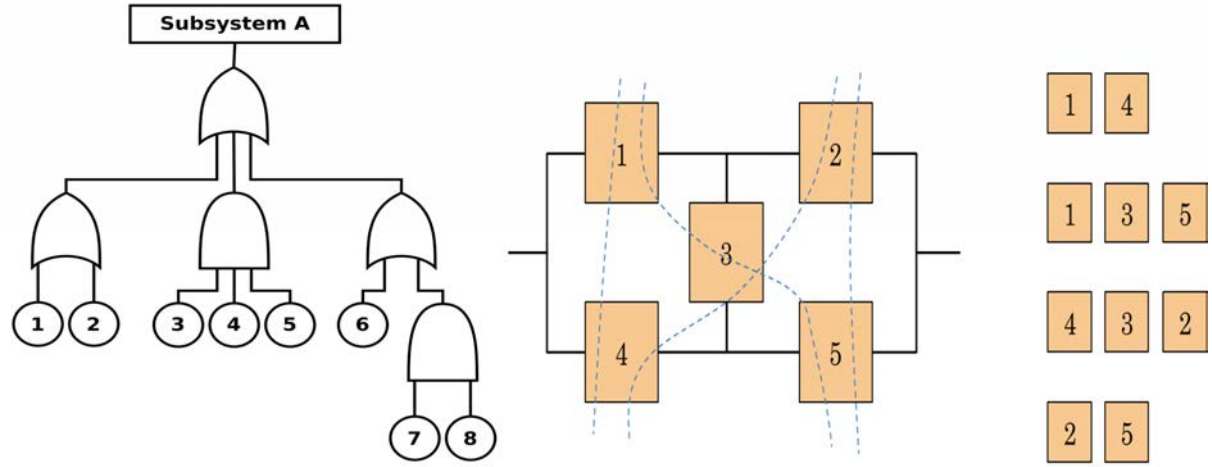

Fig.3 Fault tree analysis for selected headings

2.3 Elicitation of Minimal Cut-sets and Considerations for Cyber security

Fault tree analysis for the elicited headings is conducted for getting minimal cut-sets, and minimal cut-sets are deducted. Fig.4 indicates the example of minimal cut-sets.

No	Value	F-V	BE#1	BE#2	BE#3	BE#4
1	9.54E-05	0.292	AAMPK123T	GG-AA-PP04-T		
2	5.67E-05	0.173	AABBWW501&4			
3	3.25E-05	0.099	AAMPWPP1234			
4	2.59E-05	0.079	AAISABB534	AAISABB536		
5	2.59E-05	0.079	AAISABB501	AAISABB504		
6	0.000024	0.073	AARRBREGRR			
7	1.8E-05	0.055	OOP	AAMPW123T-L	GG-AA-PP04-T	
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		
12	2.4E-06	0.007	AATKBRWT00			
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		
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
35	9.22E-08	3E-04	AAAAOCH190	AABBT0530B		

Fig. 4 Example of minimal cut-sets for selected heading

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 [8]. 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 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.

A case with a very low probability value but with a small number of basic events constituting a minimal cut-set is more important than a that with a very high probability value but with a large number of basic cases constituting a minimal cut-set in terms of perspective of cyber security. For example, the probability of No.1 minimal cut-set is 9.54E-05 and that of No.2 is 5.67E-05 in Fig.5. In terms of original PSA, No.1 case is more important than No.2. However, in terms of cyber security, No.2 case is vulnerable to attack because the number of basic events consisting of No.2 minimal cut-set is fewer than that of No.1 minimal cut-set. Generally, No.35 case is considered as not that important because of very low failure probability. However, It consists of two basic events, so it should be considered important than No.7, No. 33, 34 cases.

2.4 Rearrangement of Minimal Cut-sets according to the Number of Basic events

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.5 Example of rearrangement of minimal cut-sets according to the number of basic events

Fig.4 is rearranged according to the number of basic events constituting the minimal cut-sets as shown in Fig 5. This will show the importance of digital assets related to basic events. However, we excluded cases where cyber-attacks were impossible due to mechanical and material related basic events. In the future, we will consider ways to express importance by considering weighting factors or other methods. In Fig.5, No.7 case consisting of three basic events has relative high probability value rather than No.10 case consisting of two basic events, but No. 10 case is more vulnerable to cyber-attacks than No. 7 case in terms of security. In specially, the cases consisting of only one basic event should be secured thoroughly compared to others.

3 CONCLUSIONS

Today, digital technologies such as computers, control systems and data networks play an essential role in modern NPPs. We are also considering the introduction of new digital technologies. This digital technology makes NPP operations more convenient and economical. However, they are inherently vulnerable to problems such as component malfunctions or cyber-attacks [9]. In recent years, there is a growing demand for cyber security for digitized nuclear instrumentation and control systems. However, there are too many digital assets in the NPP, making it difficult to control effectively. Analyze PSA results to identify critical CDAs associated with NPP accidents with cyber-attacks.

First, some initiating events (IEs) that can be caused by cyber-attacks or digital malfunction are selected. In each selected IEs, the headings that can be affected by cyber-attacks or digital malfunction are selected by event tree analysis. Headings that are only related to material, structural, and mechanical factors are excluded. Among the selected headings, the headings where failure directly causes serious problems on NPP's status are only considered. Fault tree analysis for the elicited headings is conducted for getting minimal cut-sets. In terms of the original PSA, the probability values for the cut-sets are used for safety assessment. However, the probability is not important for the cyber security of the NPP. An important factor is the number of basic events consisting of a minimum cut-set. The process of deriving an incident-related CDA based on probabilistic safety assessment results is proposed. This research could contribute to effective cyber security regulations and CDA security.

4 ACKNOWLEDGMENTS

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)

5 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. "Fault tree analysis", https://en.wikipedia.org/wiki/Fault_tree_analysis
8. 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)
9. Woogeun Ahn ., et al. "Development of Cyber-attack Scenarios for Nuclear power Plants Using Scenario Graphs", *International Journal of Distributed Sensor Networks*, v**ol. 11** (2015)