Methodology on Cyber Security for Digital I&C System in Research Reactors

Jinsoo Shin[1], Gyunyoung Heo[1], Hanseong Son[2]

[1]Kyung Hee University, Gyeonggi-do, Republic of Korea

[2]Joongbu University, Gyeonggi-do, Republic of Korea

E-mail contact of main author: gheo@khu.ac.kr

Abstract. Cyber security has become one of major issues in nuclear field, for both commercial power plants and research reactors. In order to support the technologies for cyber security in nuclear field, the regulatory agencies published a lot of guidance documents. According to them, it is necessary to evaluate cyber security considering the system architecture and the conformance with these regulatory guides. In this study, we propose a cyber security risk evaluation method addressing the necessity. The method incorporates a Bayesian belief network (BBN) model and the event tree which is one of tools for probabilistic safety assessment (PSA). The method is being applied for the cyber security evaluation of a digital instrumentation and control (I&C) system in research reactors. This is because research reactors are likely to be susceptible for cyber security due to frequent operators' access while their inherent safety should be much higher than the large-sized commercial power plants. The methodology can be used to analyze cyber security risk of a digital system in a research reactor and grant priority on cyber security risk factors which threaten the safety of research reactor. It may be expected to be available to back-up the cyber security analysis report for regulatory authority.

Key Words: Reactor Protection System, Cyber Security, Bayesian Network, Probabilistic Safety Assessment

1. Introduction

Cyber security has become one of major issues in nuclear field, both for commercial power plants and research reactors since they should use digital equipment such as digital programmable logic controller (PLC). Due to a series of recent events such as Stuxnet, guaranteeing stability of digital system against cyber-attacks on nuclear facilities is becoming increasingly important [1, 2]. However, rare events such as cyber-attacks cannot be observed very often, and there is difficulty in deciding the cause of the event and quantifying its frequency or probability. Such quantification issue involved with rare events is a subject of interest in nuclear field, as well as other fields. Software field also makes wide use of quantification method in order to analyze system failure caused by software fault [3]. Cyber-attacks cannot easily be observed until an event actually occurs, and they are receiving the spotlight as rare events that may lead to severe accidents accompanying the danger of radioactive materials from nuclear power facilities. General safety analysis on all risks including such threats can be divided into deterministic method and probabilistic method [4]. Probabilistic method used at nuclear power facilities generally uses event tree and fault tree at the same time to analyze an initiating event about factors that threaten safety of nuclear power facilities according to sequence, analyzing the cause of each threat. Here, the event tree is a tool used to sequentially analyze the success of safety systems about the initial event to find frequency of the final effect (for instance, core damage frequency (CDF) in the level 1 of probabilistic safety assessment (PSA)). The fault tree is generally a tool used when a safety

system shows failure to analyze the cause of failure. When applying a fault tree that analyses the cause of system failure in regards to cyber security from hardware perspective, there is a limitation in defining and constituting the basic event of a fault tree about cyber security, which has software characteristics. In this paper, Bayesian belief network (BBN) model is used in place of the fault tree to analyze the cause and quantify cyber security. Using this BBN model risk of cyber-attack can be systematically analyzed by reflecting architecture of digital system subject to analysis and cyber security activity. The methodology proposed in this paper can analyze cyber security risk in the digital system of a research reactor and grant priority on cyber security risk factors which threaten the safety of research reactor. It may be expected to be available to back-up the cyber security analysis report for regulatory authority.

2. Backgrounds

To propose a methodology on cyber security for digital I&C system in research reactors, Section 2.1 explains architecture of the research reactor subject to analysis. Section 2.2 introduces quantification methodologies studied in other fields and PSA methodology used for safety analysis in existing nuclear power plants and explains why a conventional PSA needs to be modified for cyber security. Section 2.3 introduces BBN as a quantification method for cyber security that satisfies the methodology proposed in this paper.

2.1.Architecture

Nuclear power facilities are divided according to their primary purpose into commercial power plants intended to generate electricity and research reactors intended to conduct education and experiment. Due to this difference, many aspects of facilities ranging from size of power plants to architecture are different. Especially, since research reactors are built to allow many people to get educated and perform experiments, they are regarded as more important for cyber security because it is sensitive to accessibility. I&C system architecture of research reactors is generally classified into reactor protection system (RPS), post-accident monitoring system, reactor regulating system, alternate protection system, information processing system, process instrumentation and control system, radiation monitoring system, automatic seismic trip system, and control room [5, 6, 7]. When attempting a cyber-attack on a research reactor, a reactor regulating system would become the first target of attack. However, the attacker can be assumed to simultaneously execute RPS attack because the cyber-attack scenario cannot be carried out as intended by the attacker unless RPS is attacked at the same time. For this reason, RPS, a safety facility, was selected in this study as the target system of the methodology on cyber security for digital I&C system in research reactors.

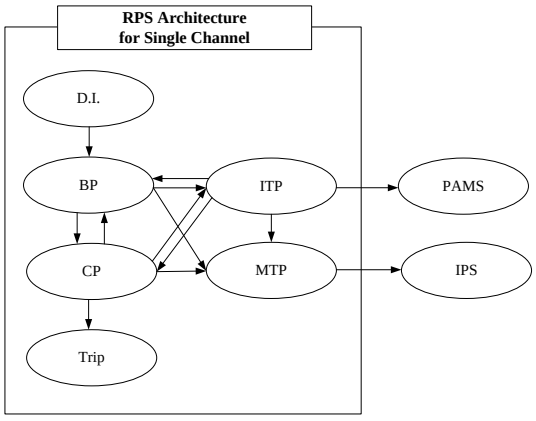

FIG. 1. The single-channel RPS architecture for research reactor.

RPS plays the role of tripping and shutting down the reactor when an emergency occurs in the research reactor. As shown in FIG.1, RPS consists of bi-stable processor (BP), coincidence processor (CP), maintenance and test processor (MTP), and interface and test processor (ITP) in a channel, and this channel is connected to other channels of same composition using fiber cable [8]. The BP generates trip signals based on the measurement channel value exceeding a set-point. It offers trip signals to CP positioned in the three redundant channels to power down its associated coincidence trip relays when any trip parameter reaches its set-point. Each BP sends status data to the MTP and the ITP through the PLC data communication module. The CP votes the two-out-of-three or two-out-of-four logic based on the state of BP trip signals. It signals are used in the generation of the initiation signals for reactor trip and engineered safety features (ESF) actuation. The MTP is a human-machine interface for the RPS. It is used for system observation testing or maintenance. The ITP monitors the status of each RPS channel and provides the channel status information to the MTP. It provides the interface between ITPs in other redundant RPS channels and interfaces to external system for status indication. Even for a research reactor that uses a network disconnected from outside, cyber-attacks can still be done by persons who have access to engineering work station (EWS) connected to BP, CP, ITP and MTP of RPS [9]. Therefore, when studying cyber security for research reactors, it is necessary to not only focus on cyber-attack itself but also to pay attention to the architecture applied with digital system subject to analysis.

2.2.Quantification Methods

The importance of quantification in non-quantified issues is already well known, and studies are underway from various angles. Software V&V field also uses many methods for quantification of software fault such as software reliability growth model, input domain based model, architecture based model, metric-based model, context-based software risk model, test-based model, and BBN model [10]. NASA quantifies software fault using context-based software risk model (CSRM) in order to analyze launch failure from software fault in launchers and to identify the cause [11]. CSRM used by NASA makes use of event tree model and dynamic flowgraph methodology (DFM) model to quantitatively analyze software fault. It can be applied to both preliminary assessments of yet-to-be-written software and in-depth assessment of existing, testable software.

Safety analysis methods include deterministic method and probabilistic method. Among them, PSA is one of representative probabilistic methods for analyzing safety of nuclear power facilities. PSA methodology consists of event tree and fault tree. Event tree method is a convenient method to characterize the event progress process according to time progress of event, and fault tree method is a proper method to comprehend the fault induction factor according to the connection relationship with equipment [12]. From the perspective of cyber security, it is extremely difficult to constitute a fault tree that defines system failure from cyber-attack as top event. This is because there is great difficulty in defining the criteria of basic event of cyber-attack for fault tree and deciding quantitative value of basic event.

2.3.Bayesian Network

In this paper, BBN methodology was used to quantitatively analyze cyber security. The BBN is a directed acyclic graph of arc to represent the dependencies between nodes and variables using Bayes' theorem [13]. The Bayes' theorem is represented as the equation (1)

$$P(C|x) = \frac{P(C)P(x|C)}{P(x)} \tag{1}$$

Where, p(x) is the probability distribution of the variable x at the entire population, p(C) is the prior probability that the some sample belongs to class, p(x/C) is the conditional probability of obtaining the value of the variable x, and p(C/x) is the posterior probability that the value of the variable x belongs to class at given situation. When the learned posterior information on the conditional probability, it can achieve the improvement of the probability by calculating the relationship between the posterior and prior probability. A BBN is composed of node, arc and node probability table (NPT). The node and arc mean a variable and the cause-and-effect relationship. The nodes have two types like the parent node and the child node. The child node has cause element and the parent node has result element of the child nodes. NPT means the probability table that summarizes the occur probability between the causal relationship nodes. Because NPT value can be used as observable quantities, latent variables, unknown parameters, or hypotheses, it is useful for changing from the qualitative problems to quantitative ones. Although a BBN has some limitations such as difficulty to defining the NPTs with expert opinions, representing the continuous data, and describing the feedback loops, yet it has strength for application in availability and cyber security of I&C system due to flexibility of input, ease of modeling and less impact of large uncertainties.

The BBN has been selected for reliability analysis because this approach works better than fault tree analysis for two reasons. The construction of a BBN model is easier than developing a fault tree and a BBN yields exact results because its analysis is based on conditional probabilities. In this article, we are more interested in importance of components in terms of risk contribution not in detail failure mechanism of system. It is also used to develop the cyber security risk model for I&C system for overcoming lack of information when analyzing and modeling about cyber security against cyber-attack by using the benefit of the BBN. The BBN is often used in order to overcome this difficulty by the conversion from the qualitative value to quantitative value [14]. The model with BBN can analyze the cyber security risk when cyber-attack occurs to I&C system. It can be utilized for the quantitative analysis by the cyber security evaluation index (CSEI), which means the probability of cyber-attack occurrence or the completeness of mitigation measure and/or the extent of activity-quality, as well as for various qualitative analyses. The CSEI is represented the node of BBN model.

3. Cyber Security Risk Evaluation

This paper proposes a quantification of cyber security risk using BBN as a methodology to evaluate cyber security risks in research reactors. This methodology can reflect sequence of events using an event tree. Section 3.1 explains a cyber security evaluation model that reflects architecture of a research reactor that used BBN. Section 3.2 explains the event tree methodology and BBN model methodology, which use the event tree to analyze scenarios in which cyber-attack risk quantified by the BBN model can affect the research reactor.

3.1.Cyber Security Risk Model

The cyber security risk model largely consists of an architecture model that analyzed architecture of digital I&C where cyber-attack can occur and activity-quality model that analyzes various cyber security activities (fulfillment of regulatory guidelines, etc.) in shown FIG.2 [15]. As mentioned in Section 2.1, it is essential to analyze architecture of digital system in order to evaluate cyber security because cyber-attack is ultimately executed based on such architecture. Architecture must be analyzed before analyzing cyber-attack that can occur in the corresponding architecture. In this paper, RPS was selected as the target of analysis as a critical safety system, and the cyber security risk model was created using the BBN model. The activity-quality model originated from the idea that cyber security activities

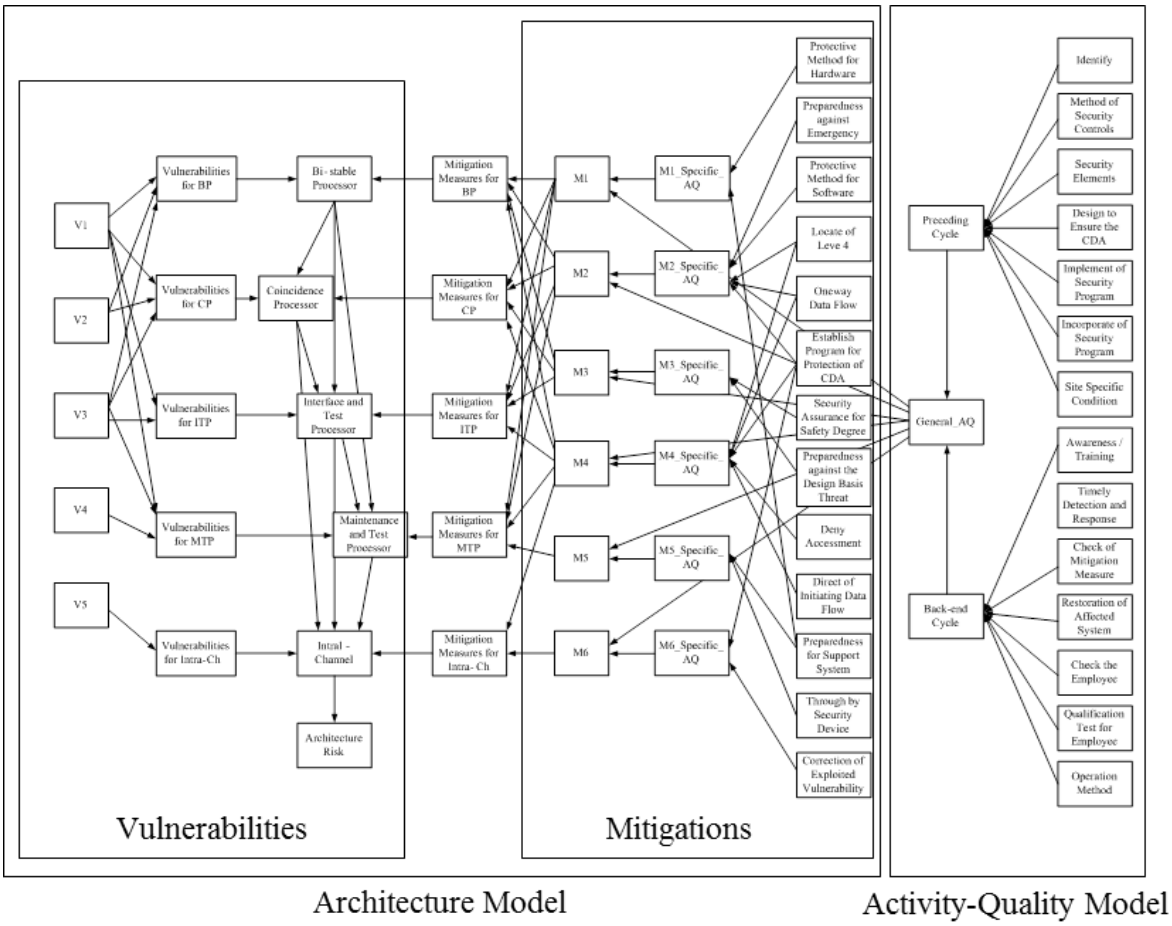

FIG. 2. The BBN model for the cyber security risk evaluation of digital RPS for research reactor.

are evaluated on documentary, operational and managerial aspects and that such cyber security activities can be reflected as mitigation measures against cyber-attacks. The BBN model uses causality between vulnerability and mitigation of cyber security, as shown in FIG.3. The higher the activity-quality of cyber security, the higher the degree of mitigation measure on cyber security and the lower the vulnerability to cyber threats in architecture model. On the contrary if the importance of cyber security is neglected and activity-quality of cyber security is lowered, vulnerability of cyber security in architecture model will be increased to a serious level. The BBN model can quantitatively find the initial CSEI by constituting NPT information using expert opinion on cyber security as prior information based on architecture of a RPS, performing cyber security risk evaluation on the research reactor. If additional information such as penetration test or cyber-attack were to occur later on, a CSEI value is calculated on the additional information using Bayes theorem. Cyber security risk evaluation can be done with posterior information.

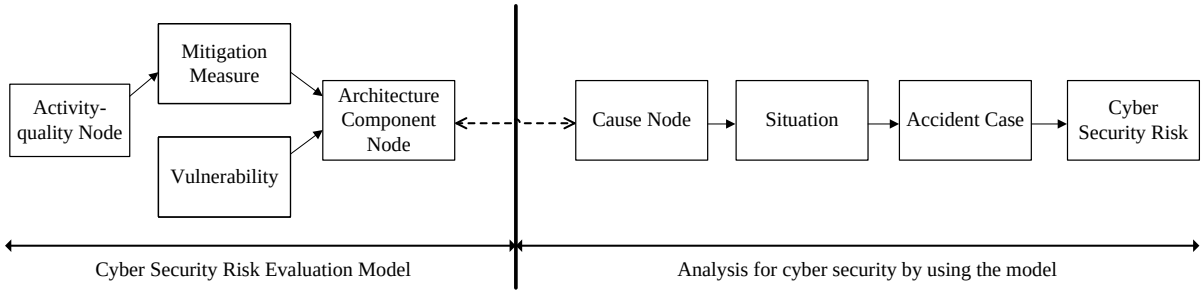

FIG. 3 Flow chart for cyber security risk evaluation with BBN model

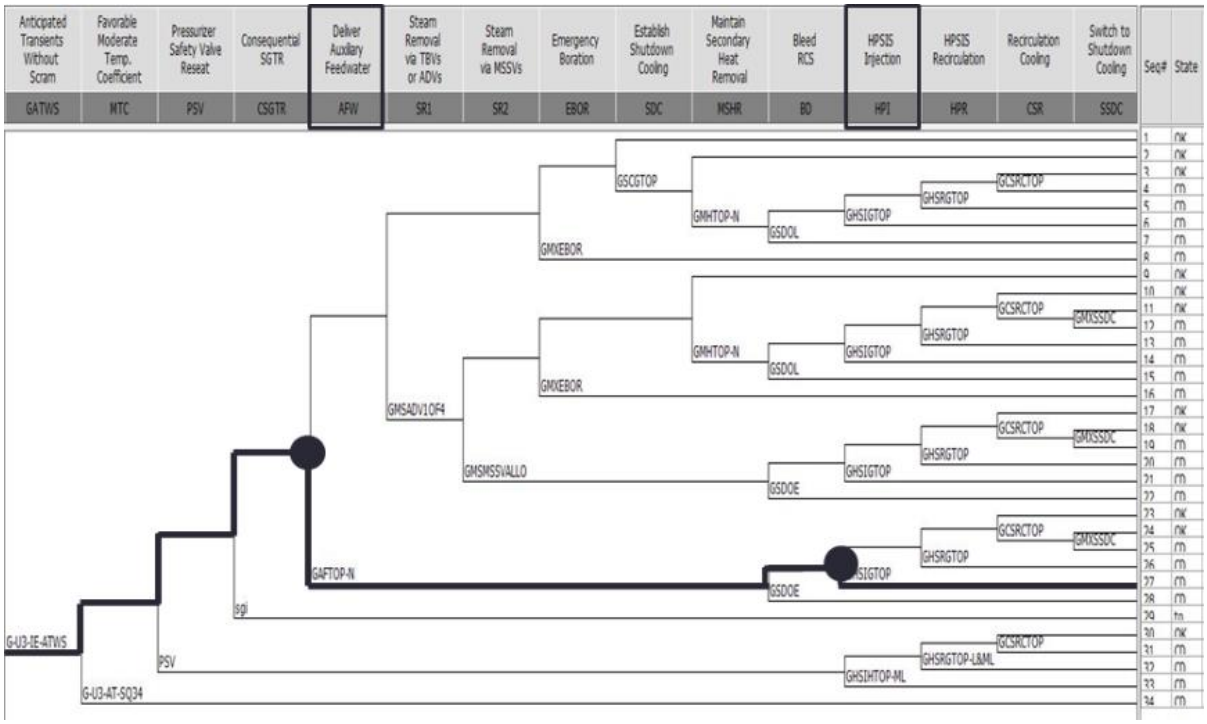

FIG. 4. An example for cyber-attack scenario where RPS is involved

3.2.Cyber Security Evaluation with Event Tree and BBN Model

An event tree is a methodology that analyzes final risk according to success of a safety system, which reduces risk of initial event until initial event arrives at final event along the given sequence. PSA on research reactor that uses event tree does not include cyber security part. In this paper, a methodology is proposed to analyze cyber security in a research reactor using cyber security risk evaluation model based on event tree methodology and BBN of the research reactor [16]. The methodology on cyber security for digital I&C system in research reactors proposed in this paper is as follows. When event tree analysis shows that a cyber-attack has occurred on reactor regulating system and RPS of a research reactor, scenarios in which initial event defined as design basis accident (DBA) can be developed into core damage are analyzed (see FIG.4.). Heading of the event tree that can be affected by cyber-attack on RPS is found among the analyzed scenarios. Heading that can be affected by cyber-

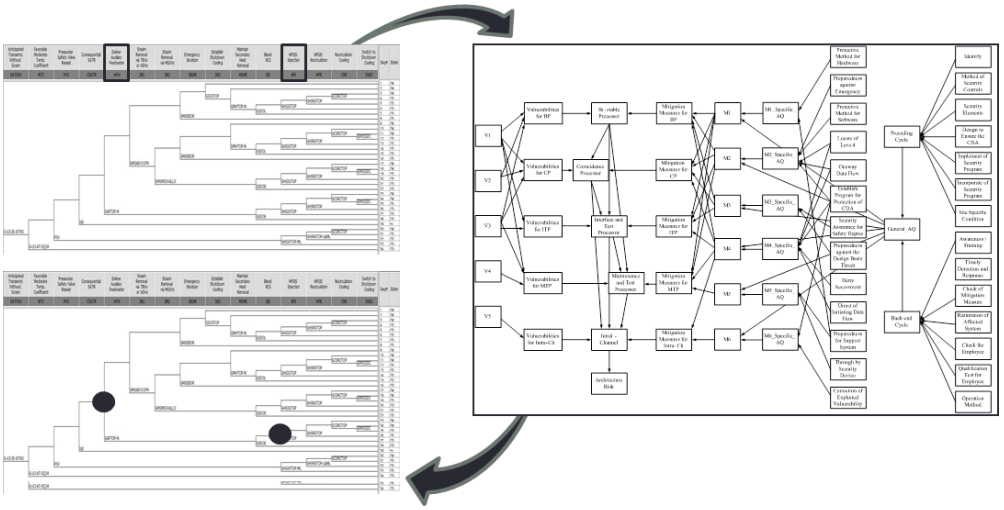

FIG. 5. BBN model and event tree analysis

attack is applied for the BBN model based on architecture of the corresponding system, as shown in FIG 5. The quantified value of cyber security risk is reflected on the event tree.

4. Conclusions

Cyber security has become one of major issues in research reactors. However, the research for cyber security evaluation has not been established yet because it is difficult to quantify and standardize all potential situations. We proposed a methodology on cyber security for digital I&C system in research reactors to prepare against cyber-attack with architectural and administrative aspects using both the event tree and BBN model. The event tree analysis can be used to analyze points of cyber-attack by analyzing which digital system can lead to dangerous situation for research reactors when a cyber-attack occur. After analyzing the event tree for cyber security, the BBN model constitute based on system architecture according to the analysis result, which allows for a more realistic analysis of the effects of cyber-attack on the system. Cyber security is characterized by difficulty of quantification and the definition of basic event, which cannot be clearly defined unlike hardware systems when performing risk assessment using fault tree analysis. The BBN model can overcome such problems with two advantages such as (1) it is easy to develop the construction of model and (2) it can overcome the lack of information when analyzing and modeling. Moreover, it can transfer qualitative data to quantitative data.

The methodology will provide the quantitative information for cyber security. It will be used to prepare the cyber security measures for research reactors against cyber-attack since it can help to find the weak points for cyber-attack among digital system which can lead a reactor to dangerous situation by virtue of event tree model and it can inform quantitative information on which points are more important to protect against cyber-attack. Furthermore, the methodology can help to reduce enormous penetration tests on nuclear facility by evaluating the vulnerability against cyber-attack and providing information that which route or point has more vulnerable than others.

Reference

[1] Collins, S., et al., "Stuxnet: the emergence of a new cyber weapon and its implications", Journal of Policing, Intelligence and Count Terrorism (2012) 80-91.

[2] Miller, B., et al., "A survey of SCADA and critical infrastructure incidents", Conference on Information Technology Education, Canada (2012) 1-6.

[3] Ch. Ali Asad, et al., "An approach for software reliability model selection", 28th Annual International Computer Software and Applications Conference (2004) 534-539.

[4] Christian Kirchsteiger, "On the use of probabilistic and deterministic methods in risk analysis", Journal of Loss Prevention in the Process Industries (1999) 399-419.

[5] Park, G.Y., et al., "Design of instrumentation and control system for research reactor", 11th International Conference on Control, Automation and System (2011) 1728-1731.

[6] Rahman, K., et al., "Comparative assessment of instrumentation and control (I&C) system architectures for research reactors", Transactions of the Korean Nuclear Society Autumn Meeting (2012) 25-26.

[7] Heyer, J. "The I&C system of the FRM-II", 6th Meeting of the International Group on Research Reactors (1998) 329-338.

[8] Lee, D., et al., "A safety assessment methodology for a digital reactor protection system", International Journal of Control, Automation, and Systems (2006) 105-112.

[9] Song, J., et al., "An analysis of technical security control requirements for digital I&C system in nuclear power plants", Nuclear Engineering and Technology (2013) 637–652.

[10] Ying, L., et al., "A survey on the quantitative evaluation methods of software reliability of digital I&C systems at NPPs", The 2013 21th International Conference on Nuclear Engineering (2013) 1-10.

[11] NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, Context-Based Software Risk Model (CSRM) Application Guide, NASA/CR-2013-218111, Washington D.C. (2013).

[12] Park, C.K., et al., Probabilistic safety assessment, Brain Korea, Seoul (2003).

[13] Heckerman. D., "A tutorial on learning with Bayesian networks. Innovations in Bayesian Networks (2008) 33-82.

[14] Chu, T.L., et al., "Applying Bayesian belief network method to quantifying software failure probability of a protection system, NPIC&HMIT (2012).

[15] Shin, J., et al., "Development of a cyber security risk model using Bayesian networks", Reliability Engineering and System Safety (2015) 208-217.

[16] Shin, J., et al., "Applications of Bayesian networks for evaluating nuclear I&C systems", Probabilistic Safety Assessment and Management PSAM 12 (2014).