Applications of Bayesian Networks for Evaluating Nuclear I&C systems

Jinsoo Shin[a], Rahman Khalil Ur[a], Hanseong Son[b], and Gyunyoung Heo[a*]
[a]Kyung Hee University, 1732 Deogyeong-daero,Giheung-gu, Yongin-si, Gyeonggi-do 446-701, Korea
[b]Joongbu University, 201 Daehak-ro,Chubu-Myeon, Geumsan-gun, Chungnam, 312-702, Korea
*Corresponding Author: gheo@khu.ac.kr

Abstract: The research presented, in this article, has been performed under the Korean research reactor project, an ongoing program to develop an optimized instrumentation & control (I&C) architecture and cyber security assessment of research reactors. The optimization of instrumentation and control systems and cyber security issues have been emphasized due to competitiveness of business (i.e. cost). Furthermore, these issues became more significant with the introduction of digital I&C systems. In this article, we have presented research activities performed for I&C architecture analysis and cyber security assessment for a reactor protection system (RPS). In I&C part, the architecture formulation, reliability feature analysis, cost estimation and cost-availability optimization of I&C architectures has been presented. In cyber security part, the cyber security risk evaluation model has been developed by integrating architecture model and activity-quality evaluation model, and analysis for cyber security evaluation for I&C system is presented. A probabilistic Bayesian network approach has been applied for I&C and cyber security analysis.

Keywords: Instrumentation and Control, Cyber Security, Reactor Protection System, Bayesian Network

1. INTRODUCTION

The various programs related to research reactor study such as instrumentation and control (I&C), cyber security, human factor engineering etc. are ongoing research activities in South Korea under Advanced Research Center for Nuclear Excellence (ARCNEX) project. Research activities and outcome related to I&C and cyber security are described in this article. Rahman and his co-authors [1] explained in one study that I&C architecture of nuclear power plants has been established to certain level, yet these are design dependent and not standardized for all industry. They also highlighted need for research to find suitable architecture for research reactor. The advent of digital technology in I&C has introduced novel kind of problems such as threat to cyber security, highlighted common cause failure (CCF) and software processing unit [2] failure and a comprehensive research is required to verify and get confidence on use of digital technology [3]. The optimization of I&C system architecture with respect to cost and its availability [4] and its resistibility to cyber-attack is also one of the basis of this research. Bayesian network has been selected for analysis in this study because this approach is suitable to model complex dependencies among components and has potential to count for uncertainties in failure data and modeling. Since I&C architecture has complex relation, so BN model has been developed for sensitivity, availability analysis and large uncertainties, due sparse failure data, has been handled effectively in BN model for cyber security evaluation.
In this article, we are presenting reliability and importance analysis of I&C components and modules of reactor protection system (RPS) I&C architecture configurations. Sensitivity study is important to get the insight of risk contribution from each component in a complex system. In this regard, many methodologies such as fault tree analysis, BN etc. have been implemented to find the sensitivity of software and software induced common cause failures to RPS using fault tree technique [5-7]. Four configurations of a single channel of RPS are formulated in the current article and BN models were developed to get the unavailability and I&C component sensitivity analysis. This study is performed for the standardization of an optimized I&C architecture for low & medium power research reactors. In this study, we also suggested the cyber security risk model to analyze the cyber-attack risk. The model utilizing the benefit of BN can analyze the risk that cyber-attack occurs at RPS. It can be utilized for the quantitative analysis by the proposed measure, cyber security risk as well as for various qualitative analyses[8-9]. Cyber security risk model is composed of the activity-quality analysis model

and the architecture analysis model. The activity-quality analysis model was proposed to check how people and/or organization comply with the cyber security regulatory guide. It helps to analyze the relationships of the activity-quality checklists and their influences to cyber security. The architecture analysis model was also developed, particularly for the RPS of a research reactor as an illustrative purpose. For the definition of the critical cyber-attack scenarios on research reactors, the vulnerabilities and mitigation measures were analyzed. Then, the two models were integrated to cyber security risk model by using BN. A few kinds of analysis with respect of cyber security were performed by using the cyber security risk model.
The objective of this research, in this article, is to identify a configuration of architecture which gives highest availability with maintaining low cost of manufacturing and low cyber risk. In this regard, four configurations of a single channel of RPS are formulated in the current article and BN models were developed to get the unavailability and I&C component sensitivity analysis. The cyber security risk of RPS has been evaluated by proposing a model based on considerations of vulnerability and the activity-quality checklist. The analysis of the vulnerability and the activity-quality checklist was performed with the assumption that a cyber-attack occurs to a maintenance and test processor in the RPS with BN models. These study are performed for the standardization of an optimized I&C architecture for low & medium power research reactors and the suggestion of cyber security risk evaluation model of I&C architecture with BN.

2. BAYESIAN NETWORK ANALYSIS

The BN is a directed acyclic graph of arc to represent the dependencies between nodes and variables using Bayes' theorem [10]. The Bayes' theorem is represented as the equation (1)

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

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. BN 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 BN 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 modelling and less impact of large uncertainties.

The BN has been selected for reliability analysis because this approach works better than Fault Tree Analysis (FTA) for two reasons. For last few decades, BN models have been applied to dependability analyses, such as Boudali and Dugan [11] transformed Dynamic Fault Tree (DFT) to BN for probabilistic analysis and Torres-Toledano and Succar [12] developed BN models for reliability analysis of complex systems based on Reliability Block Diagram (RBD). But these techniques require the development of dynamic fault tree or identification of path sets of system as a pre-request. Identification of path sets becomes difficult in case of complex system and it can produce misleading results because of incorrect or insufficient identification of path sets. The development of BN by mapping Reliability Block Diagram with General Gates (RBDGG) such as 'AND', 'OR' and 'K out of

N (KooN)' has been realized by Kim [13] in 2011. RBDGG is an extended form of RBD. The construction of BN model is easier than developing a fault tree and BN yields exact results because its analysis is based on conditional probabilities. In this article, we are more interested in reliability features of system and importance of components in terms of risk contribution not in detail failure mechanism of system. Here mapping of RBDGG to BN modeling technique has been adopted for desire analysis, in which all the logic and function has been kept preserved for each node. Therefore, it is beneficial to use BN, which will reduce the effort and give the reliable numbers for analysis.
It is also used to develop the cyber security risk model for I&C system for overcoming lack of information when analyzing and modelling about cyber security against cyber-attack by using the benefit of BN. The BN is often used in order to overcome this difficulty by the conversion from the qualitative value to quantitative value [14]. The model with BN 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 BN model.

3. BN FOR I&C ARCHITECTURE FEATURES

I&C architecture of RPS is selected for analysis in this study and four (4) single channel architecture configurations has been developed. For realization, reliability block diagram (RBD) of architecture configuration-I and BN models as provided in Figure 1. For comparison purpose, a baseline composition of configuration-I, given in (a) part of Figure 1, consists of a single bi-stable processor (BP) BP_A and single coincidence processor (CP) CP_A and circuit breakers to trip with 2/3 logic. This configuration is typical and basic for a channel and has no inter-channel redundancy. Inter-channel redundancy means redundant modules within a channel whereas intra-channel redundancy is based on number of channels. In architecture configuration-II, redundancy is added in BP to evaluate the impact on single channel. In order to observe the sensitivity of CP module on single channel failure, CP is added in the channel for case of configuration-III. This configuration consists of a bi-stable processor BP_A, redundant pair of CP processors CP_A1 & CP_A2 and circuit breakers to trip with 2/3 logic. Configuration IV consists of inter-channel redundancy of BP & CP modules i.e. two modules of each. The differences among configurations are delineated in Table 1.
The RBD of proposed I&C architecture configurations was converted to BN models preserving all the functions and logics of system. BN models, as shown in (b) and (c) of Figure 1, show the propagation of failure from transmitter & Sensor to circuit breaker actuation. Two failure states for each component are considered in this study, which are 0 and 1. State 0 represents the failure state and 1 represents the perfect is representing a node and NPT is prepared for every node based on operational logic and failure data [11-14].

Table 1: I&C architecture configurations composition[†]

Component/Module	Architecture Configuration			
	I	II	III	IV
Bi-stable Processor	1	2	1	2
Coincidence Processor	1	1	2	2
Digital Output	1	1	1	2

[†] All the other components/modules in the architecture are kept the same, as shown in Figure 1 (a).

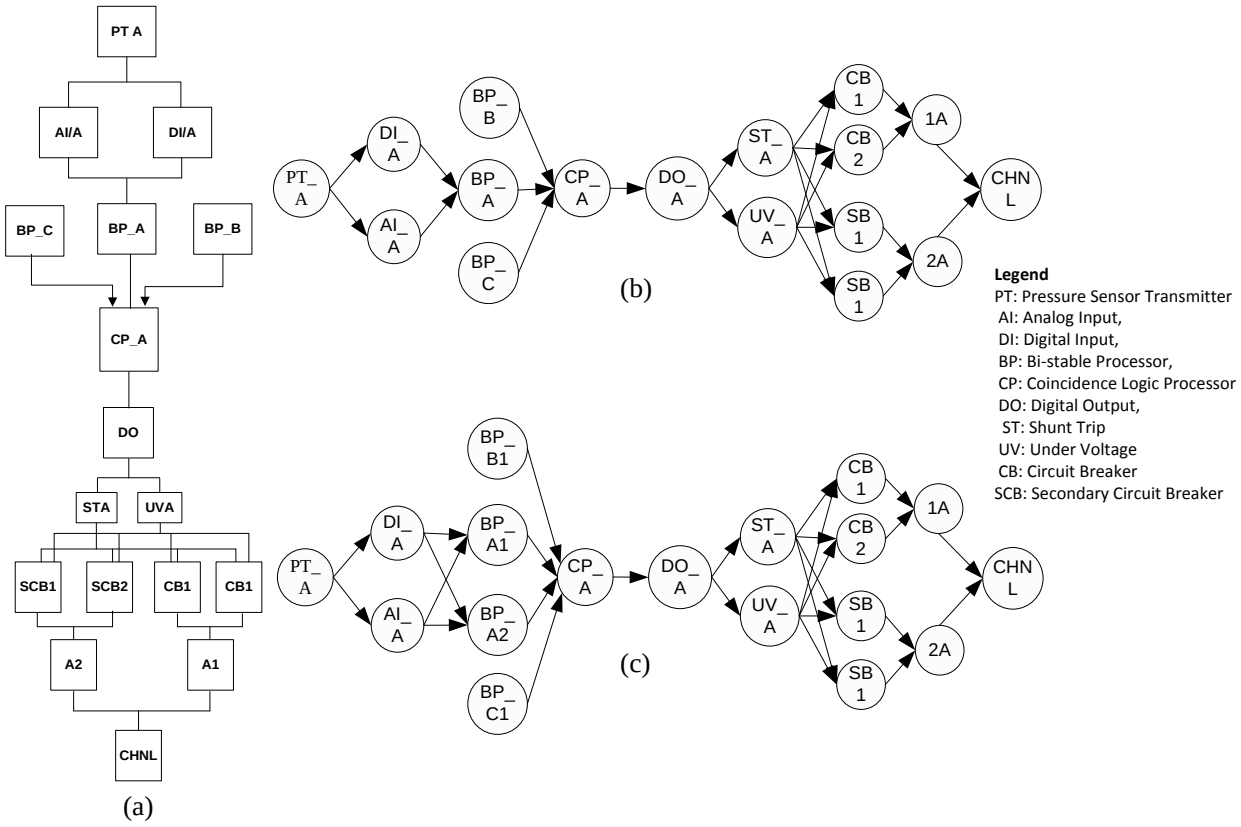

Figure 1: I&C Architecture (a) RBD of configuration-I (b) BN model of configuration-I (c) BN model of configuration-II

3.1. Architecture Availability

Reliability feature analysis of architecture configurations, such as availability, unavailability, has been performed using BN. The channel (CHNL) in BN model gives the output features for states 0 (failure) and 1 (perfect) for single channel. The results for four configurations are presented in Table 2. $P(x=0|\lambda)$ gives probability of failure state whereas $P(x=1|\lambda)$ yields probability of success for single channel. These parameters are also termed as unavailability and availability of I&C architecture.

Table 2: Reliability Analysis of I&C architecture configurations [4]

Configuration	CHNL	Unavailability ($P(x=0|\lambda)$)	Availability ($P(x=1|\lambda)$)
I	(1BP, 1CP)	1.9751E-4	9.998E-01
II	(2BP, 1CP)	3.1525E-4	9.9968E-01
III	(1BP, 2CP)	3.9701E-5	9.9996E-01
IV	(2BP, 2CP, 2DO)	3.1596E-7	0.9999996

3.2. Sensitivity Aspects

The mangers, designers and operators have been keen to recognize importance of equipment, components or system failures on the overall performance of the unit. This is valid for research reactors too. It is very important to know the fact that how much risk will increase/decrease if the failure of component happens frequently or it never fails. The indicator showing the decrease in risk is

called Risk Reduction Worth (RRW). The higher the RRW measure, the more sensitive would be the component to risk. It can be calculated by, equation 1 [1, 6], taking the ratio of the failure probability of system with λ for ith component set equal to 0 to channel total failure probability (unavailability). RRW results for four configurations are presented in Table 3.

$$RRW_i = \frac{Q_{CHNL}(\lambda)}{(Q_{CHNL}(\lambda = 0))_i} \quad (2)$$

Whereas index 'i' represents the components/modules in the architecture.
QRPS (λ) is the system unavailability and would be equivalent to P(x=0|λ) in this article. While QRPS (λ=0) shows the system unavailability if ith component never fails (λ equal to 0). In this article, it would be equivalent to P(x=0|λ=0).

Table 3: Sensitivity Results of I&C architecture configurations [6]

Component/Module	RRW			
	Configuration I	Configuration II	Configuration III	Configuration IV
PT	1.000608	1.589843	1	1.000507
DI	1	1.000476	1	1
AI	1	1.000476	1	1
BP	1.002538	1.002385	1.000025	1.000317
CP	4.871858	1.991472	1.00063	1.108632
DO	1.249115	1.14279	131.256	1.025212
ST	1.00076	0.470909	1.003742	1.875022
UV	1.00076	0.470909	1.003742	1.875022
CB	1.000304	0.470853	1.00164	1.257652
SCB	1.000304	0.470853	1.00164	1.257702

3.3. Cost Estimation

It is necessary to mention that information related to cost of safety grade instruments is proprietary and is available for academic researches. Therefore, cost of architecture has been estimated based on certain assumptions. The cost can be discretized into the unit cost for each component and number of components. Cost estimation formula has been proposed in the form of equation (3) [4]. The equation (2) gives cost as the multiple of X and multiple is product of number of components and its unit cost, where X is an arbitrary unit.

$$U_j = \sum_i u_i.n_i.X \quad (3)$$

Whereas U_j is the cost of jth architecture and j varies from 1 to 4. The parameters u_i and ni are component unit cost and number of ith component & modules in jth architecture. The components/modules are pressure/level transmitter (PT), analog input (AI), digital input (DI), bi-stable processor (PB), coincidence processor (CP), digital output (DO), shunt circuit (ST), under voltage circuitry (UV). The costs of architecture configurations I, II, III and IV has been estimated 8.5X, 10X, 10X and 12.5X respectively.
In order to observe variation of cast with respect to architecture availability & unavailability, it is plotted in Figure 2. The unavailability of system decreases from 1.9751E-4 to 3.1596E-7 for architecture I to architecture IV and availability increases from 9.998E-01 to 0.9999996 (nearly 1). The physical significance can be realized in terms of cost saving. If we consider an arbitrary unit as 100 US dollar, then cost increases by (4X) or 400USD.
A reliability index (RI) has been proposed for I&C study under this project, based on the equation (4). This index calculates the increase of availability per unit of cost. The architecture availability increases at the rate of 4.99E-05 per X unit of cost.

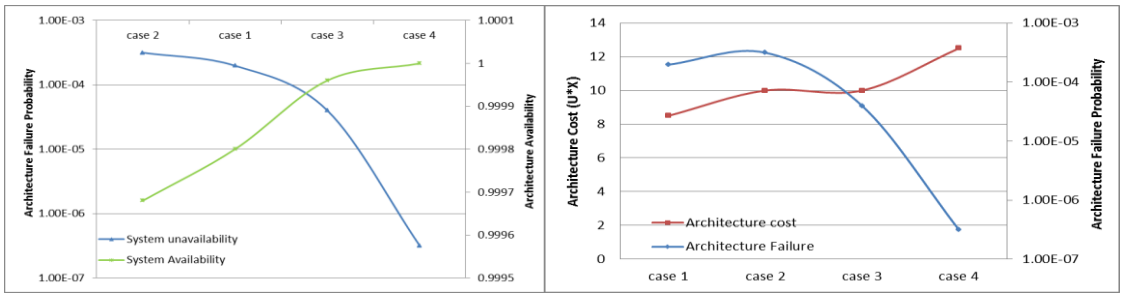

Figure 2: Variation of reliability features and cost for I&C architectures

$$RI = \frac{P_n(X=1\|\lambda) - P_1(X=1\|\lambda)}{U_n - U_1} \qquad (4)$$

4. BN FOR CYBER SECURITY RISK MODEL

The cyber security risk model for evaluation of cyber-attack risk was developed based on regulatory guide 5.71 [19] to perform cyber security analysis for I&C systems of nuclear facilities. The model is consist of two parts which are called activity-quality analysis model and architecture analysis model. The activity-quality analysis model is made for qualitative analysis such as whether or not the personal and/or organization carry out the cyber security regulatory guide well. The architecture analysis model has been developed for quantitative analysis such as structural vulnerability of I&C system for cyber-attack. Since the activity-quality analysis model affects the architecture analysis model, two model is integrated into the cyber security risk model by using BN for transformation from qualitative value of the activity-quality model to quantitative value. The cyber security risk model has performed the analysis about case studies with assumption that a cyber-attack occurs to RPS.

4.1. Application of BN for Cyber Security Risk Model

The cyber security risk model was developed with BN to utilize the benefit of it such as converting from the qualitative value to the quantitative value and calculation for back propagation by using Bayes theorem. The model is consist of activity-quality analysis model and architecture analysis model because both the management aspects and the system architecture aspect are important in terms of cyber security.

The activity-quality analysis model was developed based on regulatory guide 5.71 and using cyber lifecycle to check how personal and/or organization comply with the cyber security regulatory guide. We make 27 checklists (ex, one-way data flow, security assurance for safety degree), which is specified by cyber security regulatory guide, and represent as nodes with BN. The model helps to analyze the relationships of each nodes and their influences to cyber security and affect mitigation measure on architecture analysis model.

The architecture analysis model was constructed for RPS with two assuming situations that one is fail to trip timely due to cyber-attack and the other is reactor trip due to maliciously insertion of control rod. It offers a general perspective for the construction of the architecture analysis model for any I&C system. In order to develop the architecture analysis model for RPS, we study the network and structure about each subsystems of RPS such as BP, CP, Interface and Test Processor (ITP), Maintenance and Test Processor (MTP), and Intra-Channel. The model is composed with vulnerability and mitigation measure parts for reflection of extent of vulnerability of architecture and mitigation against penetration [??]. The vulnerabilities and mitigation measures are analyzed for RPS architecture by using this model. The lists of vulnerability are 1) Denial of service (DoS) attacks and malware execution on systems network during maintenance works (V1), 2) system shut-down by contagion of malware from maintenance works (V2), 3) data alteration by contagion of malware from maintenance works (V3), 4) Dos occurrences and malware carrying out on other systems by vulnerabilities existing in the system (V4), and 5) data alteration by using recognized vulnerabilities of standard communication protocols (V5). The lists of mitigation measure are 1) Establishment of managing

infection detection systems for external storage media like USB or PC used for PLC maintenance works (M1), 2) Establishment of security system such as firewalls / Intrusion detection system / intrusion prevention system (M2), 3) Check for running services (M3), 4) Network monitoring (M4), 5) Establishment of device validation policies (M5), and 6) Vulnerability patches (M6). The architecture analysis model with BN is developed by using these analysis results which are system network for RPS and vulnerability and mitigation measure against cyber-attack.

The activity-quality analysis model for administrative aspects evaluation is linked to architecture analysis model for evaluation of architectural system aspects for development integrated cyber security risk model. The integrated model as cyber security risk model make it possible to evaluate and analyze the final risk in view of cyber security for I&C system. Figure 3 shows the cyber security risk model for RPS with BN.

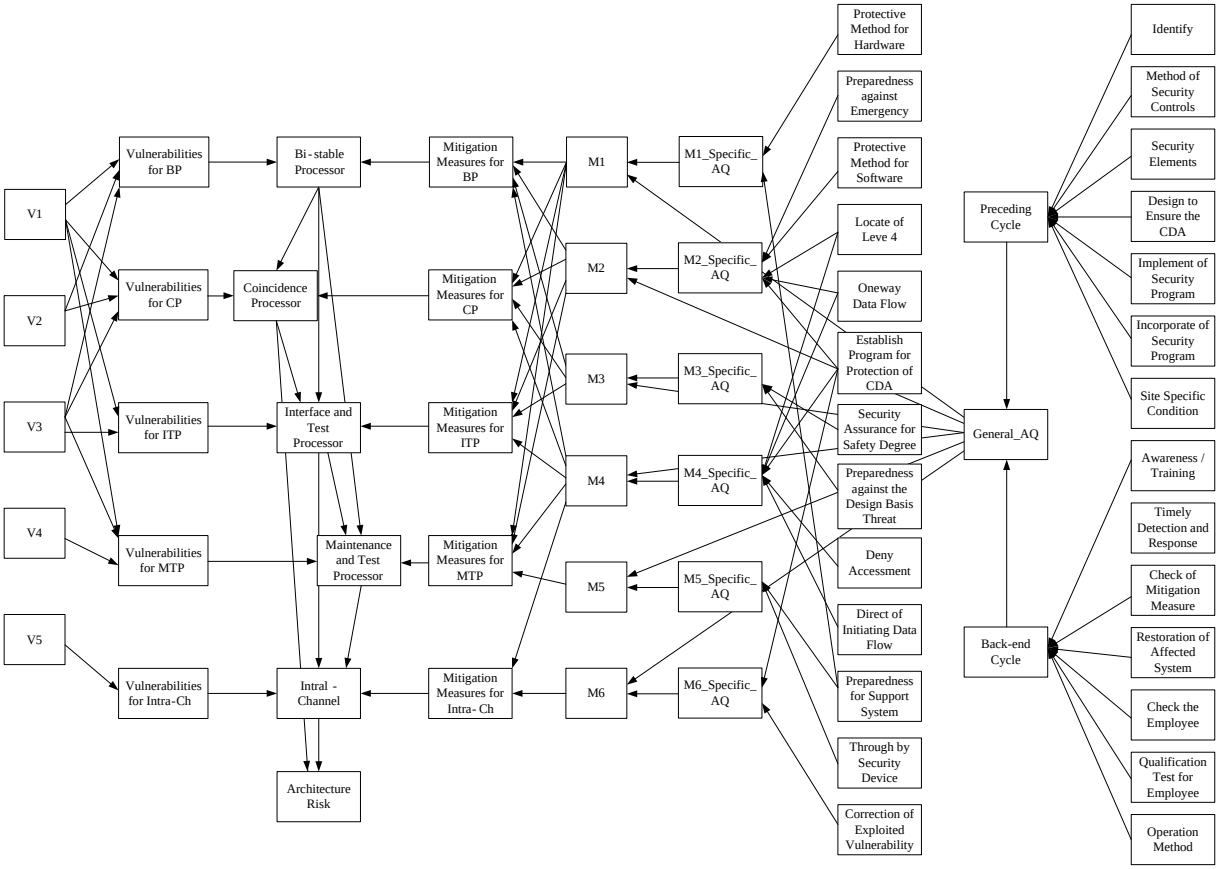

Figure 3: Cyber Security Risk Model with BN

4.2. Cyber Security Evaluation Index (CSEI)

The model used the cyber security evaluation index, called CSEI, to change from qualitative data to quantitative data for quantitative analysis. The CSEI means the extent of compliance with regulation guide or the probability of cyber-attack occurrence or the completeness of mitigation measure. It is calculated by multiplying the numeric values of each stage of node and the percentage of each stage evaluation of node as the equation. The CSEI is performed according to equation (5).

$$CSEI = \sum_{s=1}^{5} 10(2s-1) \times EP \qquad (5)$$

S is a numeric value of each stage and EP is a percentage ratio of evaluation for each stage. The numeric value for activity-quality model and architecture model are represented in Table 4.

Table 4: The numeric value of CSEI

At activity-quality checklist node		At architecture vulnerability	
Numeric value of stage	Meaning	Numeric value of Stage	Meaning
1	Very Well	1	Very Low Occur Probability
2	Well	2	Low Occur Probability
3	So so	3	Medium Occur Probability
4	Bad	4	High Occur Probability
5	Very Bad	5	Very High Occur Probability

The CSEI of each node varies from 10 to 90 points. The CSEI score of the architecture vulnerability node has the minimum 10 points when the cyber-attack probability is the highest.

4.3. Case Studies with Cyber Security Risk Model

We have performed some case studies for by using the model with BN. In this article, we introduce a results representatively. The vulnerability is analyzed by using the model when cyber-attack occurs to the MTP. The purpose of this analysis is to get information on which vulnerabilities and activity-quality checklists should be prioritized considering cyber security by using the back propagation of BN function. Assuming that any preliminary evaluation is not performed, the point of 20% is assigned to each stage of a node resulting in the average 50 points given to the node. Then the BP, CP, and ITP nodes are assigned to 70 points as hard evidences. This means that these subsystems of RPS have low possibilities to be attacked. After this, 10 points are assigned to the MTP node as hard evidence, which means the MTP was attacked. The simulation results of the model are analyzed. The result for vulnerability is shown in Table 5.

Table 5: Analysis of vulnerabilities for RPS when cyber-attack occur to MTP

Vulnerability / **Points of MTP Node**	**V1**	**V2**	**V3**	**V4**	**V5**
Points before Cyber-attack	64.98	60.16	64.98	52.50	62.39
Points after Cyber-attack	25.49	77.67	25.49	14.15	81.99
Gap between Points	-39.49	17.51	-39.49	-38.35	19.60

The second row means CSEI score for MTP before cyber-attack happening and the third row means CSEI score for MTP after cyber-attack occur to the MTP. The last low means CSEI gap between before and after cyber-attack occurrence. The negative values at last low represent the vulnerability related with MTP and the positive values represent the non-related vulnerabilities. In addition, the results can show that completeness of the mitigation measures affecting MTP have become lower in the following order: M1, M2, M4, and M5. The activity-quality checklist evaluating each mitigation measure is affected since the points of mitigation measures node are changed. The checklists that have influence of significant with MTP decrease considerably than the checklists that have influence of relatively a little.

5. SUMMARY AND CONCLUSION

BN has is some advantages such as modeling ease, suitability for modeling complex dependencies among components and potential to count for uncertainties in failure data and modeling. Since I&C architecture has complex relation, so BN model has been developed for sensitivity, availability

analysis and large uncertainties, due sparse failure data, has been handled effectively in BN model for cyber security evaluation.

The study has been performed to get the cost optimized results in terms of architecture availability and analyze the cyber-attack risk for I&C system during cyber-attack with these strength of BN. Four configurations of I&C architecture of RPS has been proposed and their BN models have been developed to get the sensitivity and availability analysis. Cost estimation model for I&C architecture has been proposed and cost-availability relation has been found out and it is defined as RI. RI provides increment in architecture availability with respect to cost, in this study this index has value of 4.99E-05 per X unit of cost. The risk due to cyber security has been evaluated for RPS in terms of administrative aspects and architectural aspects and has been measured in terms of index CSEI.

The selection of architecture has many aspects such as safety concern, designer & operator desire, availability criteria, cost etc. Based on the reliability analysis results exclusively, architecture configuration IV can be designed for the research reactor because it has a very high availability of 0.9999996. If we suppose a criteria that single channel availability of the order of 1.0E-05 would be sufficient then cost can lead towards decision of architecture. Then keep the current scenario in perspective, architecture configuration IV cane be suggested for research reactor I&C systems, because its cost varies from 10-11 X units while it has availability 0.99996 (unavailability 3.97E-05 per demand).

The cyber security risk model with BN is developed for whole RPS architecture by integration the cyber security activity-quality model and cyber security architecture model to evaluate the cyber security risk for RPS. A few analyses for RPS were performed by using the model. When cyber-attack occur to RPS, the model provides information such as the prioritized vulnerability, mitigation measure, and checklist orders with the CSEI. Theses analysis proved that the developed model could provide this kind of information through the back propagation feature of the BN. This analysis inferred that the use of cyber security risk model makes it possible to create simulated penetration test scenarios.

Acknowledgements

This work has been supported by Advanced Research Center for Nuclear Excellence (ARCNEX) project funded by the Ministry of Education, Science and Technology of Republic of Korea (Grant Number: 2013-075450).

References

[1] R. Khalil Ur, J. Shin, M. Zubair, G. Heo, and H. Son, “Sensitivity Study on Availability of I&C Components Using Bayesian Network,” Sci. Technol. Nucl. Install., vol. 2013, pp. 1–10, 2013.

[2] S. Authen and J.-E. Holmberg, “Reliability Analysis of Digital Systems in a Probabilistic Risk Analysis for Nuclear Power Plants,” Nucl. Eng. Technol., vol. 44, no. 5, pp. 471–482, Jun. 2012.

[3] R. Khalil Ur, G. Heo, and H. Son, “Architecture dependent availability analysis of RPS for Research Reactor Applications,” in Transaction of Korean Nuclear Society, 2013.

[4] R. Khalil ur, J. Shin, and G. Heo, “Study on Optimization of I & C Architecture for Research Reactors using Bayesian Networks,” in Joint IGORR 2013 and IAEA Technical Meeting, 2013.

[5] S. Kamyab, M. Nematollahi, and G. Shafiee, “Sensitivity analysis on the effect of software-induced common cause failure probability in the computer-based reactor trip system unavailability,” Ann. Nucl. Energy, vol. 57, pp. 294–303, Jul. 2013.

[6] R. Khalil Ur, M. Zubair, and G. Heo, “Reliability Analysis of Nuclear I & C Architecture using Bayesian Networks,” in 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST), IEEE, 2014.

[7] R. Khalil Ur, M. Zubair, and G. Heo, “Sensitivity Analysis of Digital I&C Modules in Protection and Safety Systems,” IOP Conf. Ser. Mater. Sci. Eng., vol. 51, Dec. 2013.

[8] J. Shin, H. Son, and G. Heo, “Cyber Security Risk Analysis Model Composed with Activity-quality and Architecture Model,” Proc. Int. Conf. Comput. Networks Commun. Eng. (ICCNCE 2013), pp. 2–5, 2013.

[9] “Development of Cyber Security Evaluation Model Using Bayesian Networks.”

[10] D. Heckerman, A Tutorial on Learning With Bayesian Networks, vol. 1995, no. November. 1996.

[11] H. Boudali and J. B. Dugan, “A discrete-time Bayesian network reliability modeling and analysis framework,” Reliab. Eng. Syst. Saf., vol. 87, no. 3, pp. 337–349, Mar. 2005.

[12] J. G. Toledano Torres and L. E. Sucar Succar, “Bayesian Networks for Reliability Analysis of Complex Systems,” Prog. Artif. Intell. — IBERAMIA 98, vol. 1484, pp. 195–206, 1998.

[13] M. C. Kim, “Reliability block diagram with general gates and its application to system reliability analysis,” Ann. Nucl. Energy, vol. 38, no. 11, pp. 2456–2461, Nov. 2011.

[14] T. L. Chu, M. Yue, and A. Varuttamaseni, “APPLYING BAYESIAN BELIEF NETWORK METHOD TO QUANTIFYING SOFTWARE FAILURE PROBABILITY OF A PROTECTION SYSTEM 1,” in NPIC&HMIT 2012, pp. 296–307.

[15] U.S National regulatory Commission, “Reliability Study: Westinghouse Reactor Protection System, 1984-1995.” NUREG/CR-5500, Vol 2, Washington, 1999.

[16] U.S National regulatory Commission, “Industry-Average Performance for Components and Initiating Events at U . S . Commercial Nuclear Power Plants.” NUREG/CR-6928, Washington, 2007.

[17] International Atomic Energy Agency (IAEA), “Generic Component Reliability Data for Research Reactor.” IAEA-TECDOC-0930, Vienna, 1997.

[18] International Atomic Energy Agency (IAEA), “Component reliability data for use in probabilistic safety assessment.” IAEA-TECDOC-478, Vienna, 1988.

[19] U.S National regulatory Commission, “Cyber Security Programs for Nuclear Facilities,” Reculatory Guide 5.71, 2010.