Cyber Security Risk Analysis Model Composed with Activity-quality and Architecture Model

Jinsoo Shin[1], Hanseong Son[2], Gyunyoung Heo[1]
[1]Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 446-701, Korea
[2]Joongbu University, 201 Daehak-ro,Chubu-Myeon, Geumsan-gun, Chungnam, 312-702, Korea
hsson@joongbu.ac.kr

Abstract - Extensive use of digital systems and networks is causing the problem of the cyber security to safety related industries like research reactors. The aim of cyber security study, in this article, is to develop a cyber-security risk analysis model based on activity-quality & Instrumentation & Control (I&C) architecture for the safety of nuclear industry. Activity-quality is a qualitative number showing the extent to which systems or plant personnel are following the regulatory guidelines, for instance very well, well, good bad etc. Architecture assessment is performed in terms of vulnerability and mitigation measures against the cyber-attack. The activity-quality analysis model and the architecture analysis model are integrated in the cyber security risk model using Bayesian Network (BN). This model can helps us to identify key elements based on their final cyber security risk .

Index Terms – Cyber Security, Activity-Quality, Architecture, Digital Systems and Networks, Bayesian Network

1. Introduction

Recently, cyber security has been highlighted as one of the issues due to the extensive use of digital systems and networks in industrial control systems [1]. Research on cyber security of commercial power plants has also been actively promoted, on contrary to that research reactor still needs to do a lot. The Industrial Control Systems Cyber Emergency Response Team (ICS-SCRT) of the Department of Homeland Security (DHS) in America announced that the weak point of control system is increasing rapidly since 2010 year. Actually, the nuclear facility in Iran was attacked the cyber-attack to nuclear facilities like “stuxnet” [2]. The cyber security means preventing and mitigating the cyber terror probability ahead of time, and responding appropriately when the event of cyber-attack is happen.

However, research on cyber security is at its early stage in nuclear industry. The Korea Institute of Nuclear Safety (KINS) as a regulatory agency declares the R.G 8.22 for applying cyber security regulation in Korea in 2011. In Korean nuclear power industry, ShinUljin unit 1&2 and ShinGori unit 3&4 are demonstrating the cyber security for the first time. The National Security Research Institute and the Korea Atomic Energy Research Institute are developing the nuclear power plant cyber security evaluation system.

We study cyber security risk analysis model for instrumentation and control (I&C) systems of reactor protection system (RPS) for research reactor using BN. Analysis models are constructed for 1) cyber security activity-quality by evaluating whether the regulatory guide is followed sufficiently and 2) I&C architecture to evaluate the structural vulnerability to cyber-attacks. 3) These two models are integrated as one model using BN [3]. Then, using a new measure called Cyber Security Risk, 4) we can analyze both the activity-quality and the architecture in terms of cyber security.

2. Methods and Result

A. Basic Concept

1) Bayesian Networks: BN is directed acyclic graph (DAG) of arc to represent the dependencies between nodes and variables using Bayes' theorem. The Bayes' theorem is following as (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 new information on the conditional probability, it can achieve the improvement of the probability by calculating the relationship between the posterior and prior probability. Fig. 1 shows this mechanism schematically.

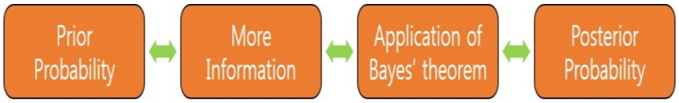

Fig. 1. The schematic cause-and-effect relationship of Bayes' theorem

BN is composed of node, arc and node probability table (NPT). The node means a variable. The arc means the cause-and-effect relationship. NPT means the probability table that summarizes the occur probability between the causal relationship nodes. Because NPT value is used as observable quantities, latent variables, unknown parameters, or hypotheses, it is useful for changing from the qualitative problems to quantitative ones. In this study, in order to evaluate the qualitative value, the evaluation degree of each node is divided by 5 levels such as very low, low, normal, good, and very good. And when each node is evaluated, the weight value can be input to each node according to its qualitative data.

TABLE I Example of the activity-quality checklist

classification	Evaluation item
Definition	How critical digital assets (CDAs) that are within the scope of the rule (RG. 5.71) are identified?
Defense -in- Depth	Are CDAs associated with safety allocated to Level 4 and protected from all lower levels?
	Are the data flows allowed only one-way from Level 4 to Level 3 and from Level 3 to Level 2?
	Do the data only flow from one level to other levels through a device or devices that enforce security policy between each level?
System Protection	Does the licensee protect systems and networks from cyber-attacks about adversely impact to data or software?
	Does the licensee protect systems and networks from cyber-attacks about deny access to or adversely impact to system, services, or data?
	Does the licensee protect systems and networks from cyber-attacks about adversely impact to system, network, and associated equipment?
Operation	Are all nuclear power plant employees subject to background and criminal history checks before they are granted access to the plant?
	Must new nuclear plant employees or contractor employees pass several tests and background checks before they are allowed unescorted access to protected areas?
	How does the licensee maintain its cyber security program?

2) *Activity-Quality*: The term of activity-quality means how people and/or organization comply with the cyber security regulatory guide such as RG.5.71, RG.1.152, 10 CFR Part 73.54 and KINS/RG_08.22 [4][5][6]. That is, the good quality of the activity means that the cyber security activity is performed well according to the detailed description of regulatory guide.

3) *Architecture:* In this paper, the architecture of the nuclear RPS is analysed because it is a critical system with respect to risk and safety of nuclear reactor.

B. Cyber Security Risk Model

1) Cyber Security Activity-Quality Analysis Model

Cyber security activity-quality is modeled by making the checklist of whether or not the cyber security regulatory guide is carried out well. Therefore, the analysis model is created by making activity-quality checklists based on RG-5.71 [6], additionally adding the KINS/RG-N08.22, and using cyber lifecycle.

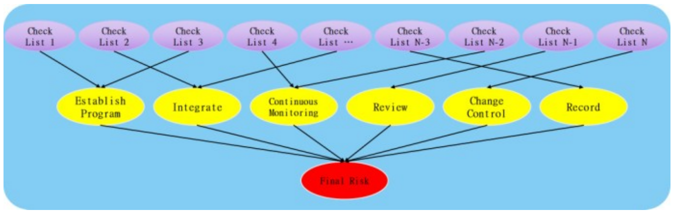

Fig. 2. Schematic diagram of the cyber security activity-quality analytical model using the BN

The cyber security lifecycle means the whole cycle of cyber security during cyber security activity. By reflecting the quality checklist activities of the cyber life cycle, it is possible to systematically analyze the quality of activity. It enables to analyze systematically by applying the activity-quality checklists to the lifecycle. Checklist is derived by analyzing the regulatory guide, and then picked out total of 34 items except the duplicate items such as Table 1. These checklists are matched with lifecycle and analyzed the correlation of related item each other and arranged the relationships Fig. 2.

The each checklist has to reflect the cyber security risks, and the final analysis has to comply with the cyber life cycle. These are evaluated and evaluation of each life cycle is comprehensive. Each checklist has to reflect the cyber security lifecycle by analysis and evaluation. And then, each lifecycle reflects the final cyber security risk.

2*) Cyber Security Architecture Analysis Model*

The cyber security architecture analysis model is constructed for the research reactor RPS architecture due it is closely relative to the reactor safety by evaluation of structural vulnerability for cyber-attack.

After the evaluation of cyber security risk of RPS I&C system for nuclear power plant is construed [7], for reflecting the architectural risk of cyber-attack for RPS I&C system, Architectural risk for RPS I&C system of research reactor is analysed. After confirming the structure of the RPS, the architecture analysis model is composed with vulnerability and mitigation measure parts for reflection of extent about vulnerability of architecture and mitigation about penetration. The list of vulnerability are 1) DoS attacks and malware execution on systems network during maintenance works, 2) shut-down of system by malware infected during maintenance works, 3) data modification by malware infected by maintenance works, 4) seizure of system authority due to vulnerabilities residing in the OS, 5) Dos attacks and malware execution on other systems by vulnerabilities residing in the system, 6) eavesdropping, data forgery, and attacks by malware and 7) data modification by suing known vulnerabilities of standard communication protocols. And the list of mitigation measures are 1) establishment of managing infection detection systems for PC, USB, and external storage media used for PLC maintenance works, 2) establishment of device authentication policies, 3) monitoring of running services, 4) network monitoring, 5) firewalls / Instruction detection system (IPS) / instruction prevention system (IDS), 6) data encryption and 7) Vulnerability patches. Evaluations for these architecture vulnerability and mitigation measure influence on final cyber security risk.

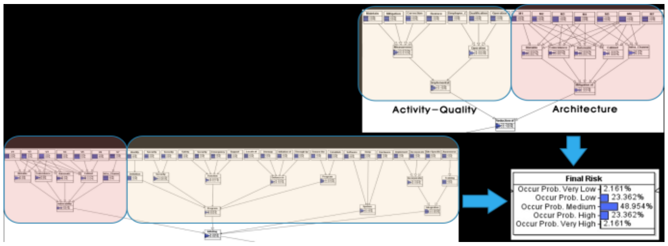

Fig. 3. The cyber security integration model composed with activity-quality and architecture analysis model

3) *Integrated Cyber Security Risk Model*

By integrating, based on BN [8], the activity-quality analysis model and the architecture analysis model, a measure "Cyber Security Risk" has been created. With the integrated model, the comprehensive analysis of cyber security risk can be performed. The integrated cyber security risk model for RPS of a research reactor is depicted in Fig. 3. By using this model, we can analyse the interaction among the checklists and find out the critical element in the event of a threat. In addition, this model is expected to be used to develop the simulated penetration test scenarios according to situation.

C. *Analysis Results Using the Model*

We have analyzed the cyber security risk using the integrated model that includes the activity-quality analysis model and the architecture analysis model. Firstly, we have analyzed the impact of each activity-quality on the overall cyber security risk. The analysis results have been compared with the intuitive judgments to be found out that they are conformed. Fig. 4 shows two examples of the analysis results. Although some checklists were evaluated very low from this analysis, these lists proved to be not important to the final cyber security risk because other checklists reduce the influence by affecting each other. These lists with the little influence can be properly dealt with to reduce the engineering cost of complying with the required regulatory guidelines. For example, all the regulatory guide items are not necessarily applied to research reactors because they are less risk sensitive than commercial nuclear power plants.

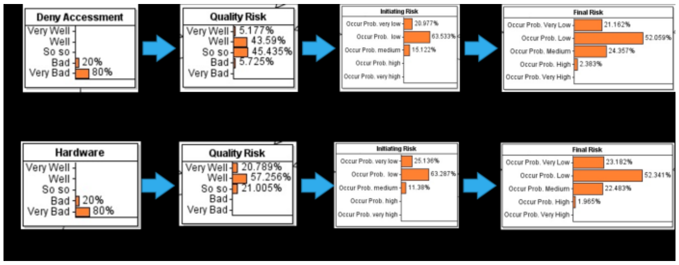

Fig. 4. The influence analysis of overall cyber security risk for each activity-quality

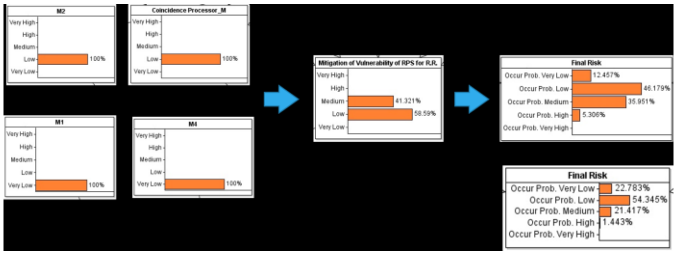

Fig. 5. The influence analysis of architecture vulnerability on the overall cyber security risk of RPS of research reactor

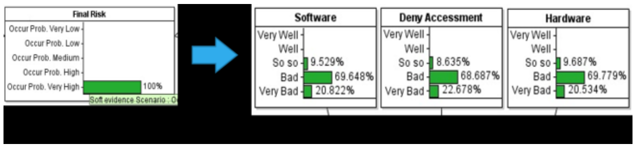

Fig. 6. The analysis for deduction of priority checklist when cyber-attack is occur

Secondly, an analysis of the effect of the architecture vulnerability on the cyber security risk is carried out by changing the extent of the vulnerability for the situation in which a cyber-attack to the architecture occurs. Fig. 5 shows an example of the analysis results. The integrated model can be utilized to create a simulated penetration test scenario. This is because the cyber-attack success probability changes according to the each vulnerability.

Lastly, by giving 100% final risk to the corresponding node assuming the occurrence of cyber-attack, we have analyzed the difference of the effect of each checklist on the final risk. This is performed owing to the reverse BN calculation shown in Fig. 6. From the analysis results, it is revealed that the check elements with high priority can be obtained by confirming which node is affected most severely by the highest risk node with the reverse BN calculation.

3. Conclusion

Analysis of the key elements of cyber security was possible through the activity-quality and architecture analysis model of cyber security. 1) It is possible to analyze the extent of the effect of each checklist on final risk by evaluating input score for each checklist node. In this way, 2) we can identify an important checklist. Further, if the cyber-attack occurs, 3) it is possible to provide evidence that is able to determine the key element corresponding to each situation via a reverse calculation of BN. Finally, 4) utilization of the integrated model is possible to create a simulated penetration test scenario according to each situation.

In the future research, the values of the NPT that represent the correlation between the lists will be improved by expert opinions. Using this model, further analysis for cyber security risk will be performed for more cases.

Acknowledgment

This work was supported by Advanced Research Center for Nuclear Excellence (ARCNEX) program funded by the

Ministry of Education, Science and Technology (Grant Number: 2011-0031773).

References

[1] B. Gan, J. H. Brendlen, “Nuclear power plant digital instrumentation and control modifications,” Nuclear Science Symp. And Medical Imaging Conf., IEEE Conference Record, Vol. 2, Oct. 25-31, 1992.

[2] Sean Collins and Stephen McCombie, “Stuxnet: the emergence of a new cyber weapon and its implications”, Journal of Policing, Intelligence and Counter Terrorism, Vol. 7, No. 1, p. 80-92, April, 2012.

[3] Heckerman, D. “A tutorial on learning with Bayesian networks, Microsoft Research report MSR-TR-95-06,1995

[4] Regulatory Guide 1.152 revision 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, January 2006.

[5] 10 CFR Part 73.54, Protection of Digital Computer and Communication systems and Networks, U.S. Nuclear Regulatory Commission, Washington, D.C., 2009.

[6] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.

[7] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, and Dong-Young Lee, “A cyber security risk assessment for the design of I&C Systems in nuclear power plants”, Nuclear Engineering and Technology, Vol. 44, No. 8, pp. 919-928, 2012.

[8] T.L. Chu, M. Yue, A. Varuttamaseni, M.C. Kim, H.S. Eom, H.S. Son and A. Azarm, Applying Bayesian belief network method to quantifying software failure probability of a protection system, NPIC&HMIT 2012, San Diego, CA, July 22-26, 2012.