Transactions of the Korean Nuclear Society Spring Meeting
Gwangju, Korea, May 30-31, 2013

Cyber Security Risk Analysis Model of I&C System Using Bayesian Network

Jinsoo Shin [a], Hanseong Son [b*], Gyunyoung Heo [a], Jaekwan Park [c]
[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*
[c]*Korea Atomic Energy Research Institute, Daedeok-daero 999-111, Yuseong-gu, Daejeon, Korea*
[*]*Corresponding author: hsson@joongbu.ac.kr*

1. Introduction

Nowadays, cyber security is issued due to digitalization of instrumentation and control (I&C) system [1]. The Industrial Control Systems Cyber Emergency Response Team (ICS-SCRT) of the Department of Homeland Security (DHS) in America announces that the weak point of control system is increasing rapidly since 2010 year. Actually, Iran is attacked the cyber-attack to nuclear facilities like “stuxnet” [2]. Or Iran attacked? 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 Korean nuclear industry. The Korea Institute of Nuclear Safety (KINS) as a regulatory agency declares the R.G 8.22 for applying cyber security in Korea in 2011. In nuclear power industrial, ShinUljin 1, 2 unit and Shingori 3, 4 unit are demonstrating the cyber security for the first time. And in terms of research, the National Security Research Institute and the Korea Atomic Energy Research Institute are developing the nuclear power plant cyber security system in Korean. Currently, these cyber securities like regulation, demonstration and research are focused on nuclear power plant. However, cyber security is also important for the nuclear research reactor like a HANARO which is in Daejeon, primarily due to its characteristic as research reactor since since people access more than power plant.

2. Methods and Results

Therefore, we study cyber security risk analysis model of I&C of reactor protective system (RPS) for research reactor using Bayesian network. The study method is described as in the following. Analysis models are constructed for 1) cyber security activity-quality by evaluating whether the regulatory guide is carried out and 2) I&C Architecture to evaluate the structural vulnerability to cyber security. 3) These two models are integrated as one model using Bayesian network (BN) [3]. Then, using the new index like the Cyber Security Risk, 4) we can compare and analysis both activity-quality and architecture for cyber security.

2.1 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 [4], additionally adding the KINS/RG-N08.22, and using cyber lifecycle.

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. These checklists are matched with lifecycle and analyzed the correlation of related item each other and arranged the relationships. [Fig. 1] 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.

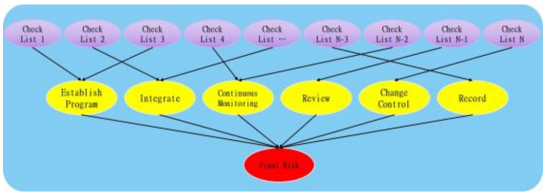

Fig. 1. Schematic diagram of the cyber security activity-quality analytical model using the Bayesian Network.

2.2 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 [5], for reflecting the architectural risk of cyber-attack for RPS I&C system, Architectural risk for RPS I&C

system of research reactor is analyzed. 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. Evaluations for these that architecture vulnerability and mitigation measure influence on final cyber security risk.

2.3 Cyber Security Integration Risk Model

By extending integrated based on BN, the activity-quality analysis and architecture analysis model, an index of "Cyber Security Risk" has been created. Therefore, it is possible to comprehend the comparative analysis of cyber security.

The Cyber security integration model that integrates the activity-quality of cyber security and architecture of RPS for research reactor analysis model seem to be following Fig. 2. By using this model, we can analyze the interaction of each checklist and determine the critical check element in the event of a threat. In addition, it is expected to be possible to utilize the simulated penetration test scenarios that are created according to each situation.

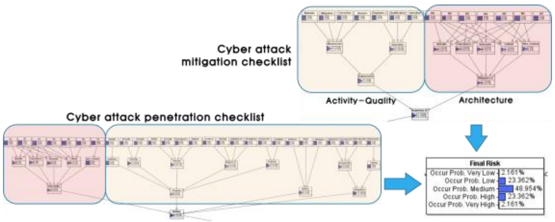

Fig. 2. The cyber security integration model composed with activity-quality and architecture analysis model.

2.4 Analysis using cyber security risk analysis model

We have performed the preliminary validation using an integrated model of the activity-quality and architecture of cyber security. First of all, we have compared the similarity with the intuitive judgment by analyzing the impact on the overall cyber security due to checklists of each activity-quality and the important information that a major impact on the risk of cyber security. Secondly, a comparison of the effect on the risk of cyber security is carried out by changing the extent of the vulnerability for the situation in which the problem about vulnerability of architecture occurs. Lastly, when it has given as 100% final risk assuming the occurrence of cyber-attack, we have analyzed to compare the degree of risk of the checklist, which is calculated by reverse BN calculation.

3. Conclusions

Analysis of the key elements of cyber security is possible to study through the activity-quality and architecture analysis model of cyber security. 1) It is possible to analyze the extent reflected final risk by evaluating input score for each checklist. In this way, 2) you can see an important checklist. Further, if the cyber-attack occurs, 3) it is possible to provide an evidentiary material that is able to determine the key check element corresponding to each situation via a reverse calculation of BN. Finally, 4) Utilization is possible to create a simulated penetration test scenario according to each situation.

Analysis of the key elements of cyber security is possible to study through the activity-quality and architecture analysis model of cyber security. 1) It is possible to analyze the extent reflected in the final risk by evaluating input score for each checklist, in this way, 2) you can see an important checklist. Furthermore, if the cyber-attack occurs, 3) it is possible to provide an evidentiary material that enables to determine the key check element corresponding to each situation via a reverse calculation of BN. Finally, 4) Utilization is possible to create a simulated penetration test scenario according to each situation.

In the future, the value of the node probability table that entered the correlation between the lists will be improved through the advice to meet experts. And using this model, further analysis will be derived and analyzed regarding to the more cases about cyber security.

ACKNOWLEDGEMENT

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] 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

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

[5] 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