MODEL BASED CYBER SECURITY ANALYSIS FOR RESEARCH REACTOR PROTECTION SYSTEM

JINSOO SHIN, RAHMAN KHALIL UR, GYUNYOUNG HEO
Kyung Hee University, Seogyeong-daero, Giheung-gu, Gyeonggi-do, 446-701, Republic of Korea

HANSEONG SON
Joongbu University, 201 Daehak-ro, Chubu-Myeon, Geumsan-gun, Chungnam, 312-702, Republic of Korea

* Corresponding author: hsson@joongbu.ac.kr

ABSTRACT

The instrumentation and control systems in nuclear facilities have changed from analog to digital system due to obsolescence and other reasons. The digitization has introduced the cyber security issue and the several cyber-attacks penetrating vulnerabilities of digital systems have been reported. In order to prepare security program against cyber-attack, the related organizations and regulatory authorities have published guidelines, but a model to evaluate cyber security systematically is required for the effective and efficient analysis. In this work, the cyber security risk analysis model is suggested for research reactors using Bayesian network. This model enables the level of cyber security to be quantitatively evaluated in terms of administrative and technical aspects. We focused on the evaluation of the reactor protection system for a demonstrative purpose.

1. Introduction

According to a IAEA report of August 2013, the number of nuclear reactors in world are 434, among which 195 (44.9%) units were built in last 30 years and 319 (73.5%) are constructed during last 25 years [1]. Due to time lag, a construction of new nuclear reactor would require digital system and change of obsolescence systems is necessary. In such a process, instrumentation and control system of nuclear research reactor is changed from analog to digital system, as well as other nuclear facilities due to halt or lack of replace equipment and degradation of performance capacity, reliability, and efficiency related using analog obsolescence equipment. The digitization of system has characteristic of digital equipment, the cyber security is highlighted as new type of threat to nuclear facilities. Several cases that show the risk and occurrence probability of cyber-attack targeting digital system on nuclear facilities has been reported [2]. For example, the Slammer worm attacked the Davis-Besse nuclear power plant targeting a vulnerability and infected computer systems and safety parameter display system in January 2003. Plant personnel could not access the system and it was showing meltdown conditions of the plant, due to network traffic by the worm. Similarly unit 3 at the Brown Ferry nuclear power plant was a shutdown in 2006. It was manually shut down after a failure of the controllers with embedded microprocessors and Ethernet communication capabilities. It shows that critical reactor components can be disabled by a cyber-attack. In order to prepare for cyber-attack, US NRC reinforces the regulation guide such as 10 CFR 73.54, Regulatory Guide (RG) 1.152 Version 2 and 3 and RG 5.71 [3, 4, 5, 6]. IEEE (Institute of Electrical and Electronics Engineers) issued IEEE Std 7-4.3.2-2010 which is applied to the RG 1.152 Version 2 for cyber security [7]. The Korea Institute of Nuclear Safety (KINS), a regulatory body, published the RG 8.22 for controlling cyber security of nuclear facilities in Korea [8].

As the cyber security issue is being focused more and more, the necessity of a cyber security

model for evaluation and analysis of cyber security risk for nuclear facilities increases. In this work, a systematic cyber security risk analysis model is suggested for cyber security analysis for RPS of nuclear research reactor. The model can be evaluated in terms of both administrative and technical aspects, which mean the extent of compliance with regulation guides and the vulnerability of RPS architecture for cyber-attack, respectively. The model is based on the Bayesian Network (BN) [9]. The cyber security analysis against various cyber-attack scenarios can be performed by using the BN model. The analysis involves the two possible cases at RPS that are ‘involuntary insertion of reactor trip through RPS' and 'manipulation of information through RPS such as scram halt'. The reason for analyzing the RPS of research reactor is that the RPS is the system that need to perform protection and as well as safety action simultaneously unlike nuclear power plants. Representatively, a case, in which a cyber-attack is assumed to occur to each subsystem of RPS, was analyzed. Through the analysis, the critical vulnerabilities and checklists were identified.

2. Model and analysis

2.1 Cyber security risk model

This work suggests the cyber security risk model to evaluate the cyber security in terms of both administrative and technical aspects using the BN [10]. The cyber security risk model is made up of the activity-quality analysis model and the RPS architecture analysis model. The activity-quality analysis model analyzes how people and/or organization comply with the cyber security regulatory guides such as RG 5.71, RG 1.152, 10 CFR Part 73.54 and KINS/RG 08.22. When the cyber security activity is performed well according to the regulatory guides, the activity-quality becomes good and the cyber security risk becomes low. The checklist is made based on the regulatory guides to evaluate each activity-quality element and it is translated straightforwardly into the nodes of BN. The RPS architecture analysis model is developed for analysis in term of technical aspect. We assumed the ‘insertion of reactor trip through RPS’ and the ‘scram halt through RPS’ to determine the final cyber threat influencing RPS. After final cyber threat at RPS is determined, we designate 5 vulnerabilities (i.e., Denial of Service attack (DoS) occurrences and malware carrying out on systems network during maintenance works (V1), System shut-down by contagion of malware from maintenance works (V2), Data alteration by contagion of malware from maintenance works (V3), DoS occurrences and malware carrying out on other systems by vulnerabilities existing in the system (V4), Data alteration by using recognized vulnerabilities of standard communication protocols (V5)) and 6 mitigation measures (i.e., Establishment of managing infection detection systems for external storage media like USB or PC used for PLC maintenance works(M1), Establishment of security system such as firewalls / Intrusion detection system (IDS) / intrusion prevention system (IPS)(M2), Check for running services(M3), Network monitoring(M4), Establishment of device validation policies(M5), Vulnerability patches(M6)). Reflecting the definition of vulnerability and mitigation measure for cyber security of RPS, the RPS architecture analysis model is developed with the consideration of the RPS architecture, which are Bi-stable processor (BP), Coincidence Processor (CP), Information and Test Processor (ITP), Maintenance & Test Processor (MTP) and Intra-Channel. The cyber security risk model has been created by integrating the activity-quality analysis model and the architecture analysis model, both of which are developed based on the BN. The analysis in terms of administrative and technical aspects is represented by node of BN for modeling. The cyber security evaluation index, which values each node of BN, is used for the evaluation of cyber security. With the integrated model, various cyber security risk analyses can be

performed. The structure of the cyber security risk model for RPS of a research reactor is shown in Fig. 1.

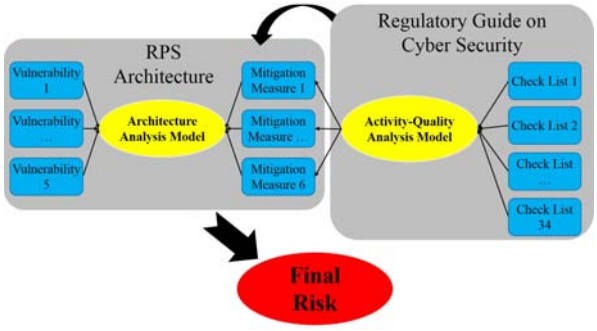

Fig 1. The structure of the cyber security risk model with the activity-quality model and the architecture analysis model

The mitigation measure to prevent and mitigate cyber-attack is closely related to the cyber security activity-quality. Thus the activity-quality analysis model is linked with the mitigation measure nodes of the RPS architecture analysis model to develop the cyber security risk model (as shown in Fig. 2). Just before the linkage, according to the extent of influence and particularity for mitigation measure, the activity-quality checklists are grouped into the specific checklist group and the general checklist group. By using this model, we can analyze 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 situations.

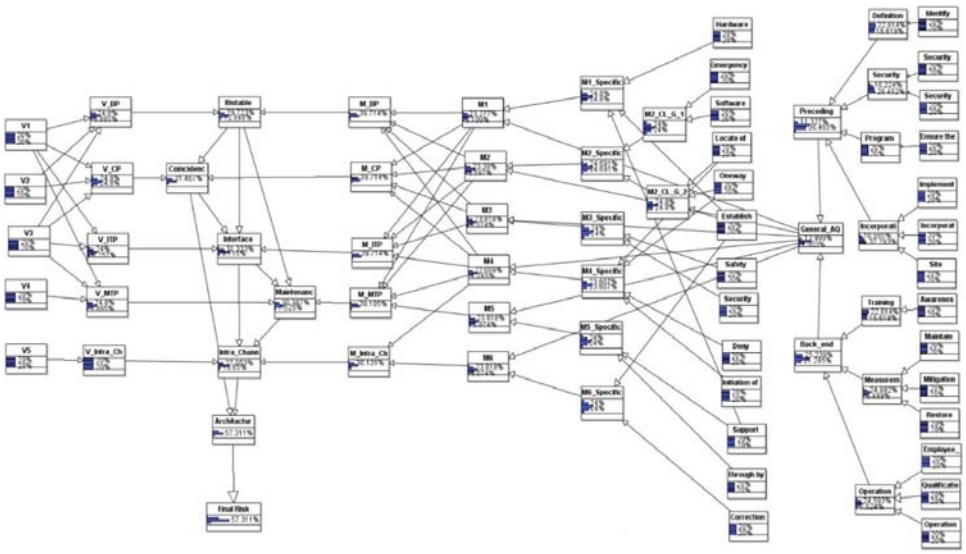

Fig 2. The Cyber Security Risk Model using BN

2.2 Analysis results

We have analyzed the cyber security risk for RPS of a research reactor using the cyber security risk model that combines the activity-quality analysis model and the architecture analysis model. All the scenarios are not covered but rather a case that is for the analysis of the vulnerability and the activity-quality checklist when a cyber-attack occurs to each subsystem of RPS is described in this article. The purpose of this analysis is to acquire information on which vulnerabilities and activity-quality checklists should be prioritized in the design, development, testing and maintenance in view of cyber security when the each

subsystem of the RPS is assumed to get a cyber-attack. Assuming that any preliminary evaluation is not performed, 50 points are assigned to the score of each node, which represents activity-quality checklist and vulnerability. Normally, the numeric value of each node at activity-quality checklist and architecture vulnerability means that 90 point is 'High-High quality' or 'Low-Low occurrence probability', 70 point is 'High quality' or 'Low occurrence probability', 50 point is 'Normal quality' or 'Normal occurrence probability', 30 point is 'Low quality' or 'High occurrence probability', 10 point is 'Low-Low quality' or 'High-High occurrence probability'. Then the high points like 70 points are assigned to each subsystem of RPS as hard evidence, which means that the probability of cyber-attack at subsystem is assumed low. After this, 10 points are assigned to the each subsystem node as hard evidence, which assumes the each subsystem was attacked. The vulnerability, the mitigation measure and each checklist are analyzed according to the occurrence of cyber-attack on each subsystem based on the simulation results.

Table 1 shows the changes of the vulnerability score according to the occurrence of cyber-attack on each subsystem. Before the cyber-attack occurrence to each subsystem, the score of each subsystem is 50 points. However, the score of vulnerabilities is changed after each subsystem is attacked. This is simulated by inputting the hard evidence (i.e. 10 points) on the node as a situation of cyber-attack occurrence on subsystem. By confirming the gap (in Tab. 1), which is the difference between before and after cyber-attack occurrence, we can know that, while the probabilities of vulnerability related to the attacked subsystems have increased, the probabilities related to the other subsystems, which are not attacked, have decreased. For example, when BP is attacked, the order of response against cyber-attack can be determined efficiently such that V2 have to be checked firstly, and then V1 / V3, V4 and V5 can be checked in this order.

Vulnerability / Attacked subsystem	V1	V2	V3	V4	V5
	50	50	50	50	50
BP	29.7563	14.6286	29.7563	64.4028	60.4344
(Gap)	-20.2437	-35.3714	-20.2437	14.4028	10.4344
CP	51.9449	16.499	51.9449	57.3764	67.3925
(Gap)	1.9449	-33.501	1.9449	7.3764	17.3925
ITP	27.8375	58.9753	27.8375	70.5951	81.0682
(Gap)	-22.1625	35.9753	-22.1625	20.5951	31.0682
MTP	25.4912	77.6683	25.4912	14.1514	81.9901
(Gap)	-24.5088	27.6683	-24.5088	-35.8486	31.9901
Intra-Ch	70.6413	63.3089	70.6413	54.5222	10.05
(Gap)	20.6413	13.3089	20.6413	4.5222	-39.95

Tab 1: Part of analysis result for RPS cyber security risk

The analyses of the mitigation measures and the checklists are also performed with the same scenario. From these analysis results, we can get the information that we need to perform the mitigation measures in order of priority based on the gap (difference between the probabilities of safe mitigation before and after the attack). The results show that the gap is highest for M3 (when BP under cyber-attack) and it is higher in the order of M3/M2/M1 (when CP under cyber-attack), M3/M2 (when ITP under cyber-attack), M5/M2 (when MTP under cyber-attack) and M6/M4 (when Intra-Channel under cyber-attack). Moreover, we can also get the information that helps to draw critical checklists affected from the technical aspects. For example, when ITP is attacked, the completeness of M3 is decreased. This results in that the checklists, such as the security assurance for safety degree and/or preparedness against the design basis thereat, can be determined as key checklist for the improvement of M3.

In order to maintain the functionality and safety of RPS after a cyber-attack happens, the research reactor personnel (operator or engineer) can use the information from these analyses.

In addition, this kind of analysis can be performed with various scenarios in which it is postulated that there exist cyber threats, the system has vulnerabilities, the cyber security activities and counter measures for the system are not perfect. The analysis results will provide useful information to evaluate the cyber security of a system in an integrated manner, as well as the confirmation that the model reflects the intuitions on both the activity-quality and the system architecture.

3. Conclusions

This work developed the cyber security risk analysis model, which consists of the activity-quality analysis model and the architecture analysis model to consider concurrently both administrative and technical aspects. The activity-quality analysis model can evaluate 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 is also developed to analyze the vulnerabilities and mitigation measures against cyber-attack for RPS of a research reactor. The cyber security risk model is constructed through the integration of these two analysis models and can perform the analysis for both the administrative and technical issues. It can be utilized for the quantitative analysis by the model with BN, as well as for various qualitative analyses.

In this work, the analysis of the vulnerability and the activity-quality checklist was performed with the assumption that a cyber-attack occurs to each subsystem of RPS. In this analysis, the important checklists could be identified with respect to the cyber security quality activities. Furthermore, the vulnerabilities and the mitigation measures were analyzed with a cyber-attack to RPS assumed. If a cyber-attack occurs in a system scale, it is important to have confidence on which component is the key element corresponding to the attack situation. This analysis proved that the model developed could provide this kind of information through the back propagation feature of the BN. The analysis of the RPS cyber security risk and the optimal mitigation measures regarding vulnerabilities was also performed. In other words, in order to initiate a prompt response against a cyber-attack, they can be given some assistance to determine which checklists are more important. This analysis infers that the use of the cyber security risk model makes it possible to create simulated penetration test scenarios.

4. References

[1] URL: http://www.iaea.org/PRIS/WorldStatistics/OperationalByAge.aspx

[2] KESLER, Brent. The Vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insights, Volume 10, Issue 1, p.15-25, Spring 2011.

[3] 10 CFR Part 73.54, Protection of Digital Computer and Communication systems and Networks, U.S. Nuclear Regulatory Commission, Washington, D.C., 2009.

[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] Regulatory Guide 1.152 revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission, July 2011.

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

[7] IEEE Std 7-4.3.2-2010, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE, 2 August 2010.

[8] KINS/RG-N08.22, Cyber Security for I&C System, Korea Institute of Nuclear Safety, 2009.

[9] Heckerman, D., A tutorial on learning with Bayesian networks, 2011.

[10] Shin, J.S., Son, H.S., and Heo, G.Y., Cyber Security Risk Analysis Model Composed with Activity-quality and Architecture Model, International Conference on Computer, Networks and Communication Engineering, p. 609-612, 2013.