Reliability Engineering and System Safety 134 (2015) 208–217

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Development of a cyber security risk model using Bayesian networks

Jinsoo Shin [a], Hanseong Son [b,*], Rahman Khalil ur [a], Gyunyoung Heo [a]

[a] Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 446-701, Republic of Korea
[b] Joongbu University, 201 Daehak-ro, Chubu-Myeon, Geumsan-gun, Chungnam 312-702, Republic of Korea

ARTICLE INFO

Article history:
Received 13 September 2013
Received in revised form
2 October 2014
Accepted 8 October 2014
Available online 28 October 2014

Keywords:
Cyber security
Activity-quality
Architecture analysis
Bayesian network
Reactor protection system
Research reactor

ABSTRACT

Cyber security is an emerging safety issue in the nuclear industry, especially in the instrumentation and control (I&C) field. To address the cyber security issue systematically, a model that can be used for cyber security evaluation is required. In this work, a cyber security risk model based on a Bayesian network is suggested for evaluating cyber security for nuclear facilities in an integrated manner. The suggested model enables the evaluation of both the procedural and technical aspects of cyber security, which are related to compliance with regulatory guides and system architectures, respectively. The activity-quality analysis model was developed to evaluate how well people and/or organizations comply with the regulatory guidance associated with cyber security. The architecture analysis model was created to evaluate vulnerabilities and mitigation measures with respect to their effect on cyber security. The two models are integrated into a single model, which is called the cyber security risk model, so that cyber security can be evaluated from procedural and technical viewpoints at the same time. The model was applied to evaluate the cyber security risk of the reactor protection system (RPS) of a research reactor and to demonstrate its usefulness and feasibility.

1. Introduction

Recently, cyber-attacks have been emphasized as one of the issues caused by the digitalization of instrumentation and control (I&C) systems and the extensive use of networks in industrial control systems [1]. Cyber security refers to the prevention and mitigation of the cyber terror probability beforehand and the appropriate response if a cyber-attack occurs. Nuclear facilities have serious concerns regarding cyber-attacks because of the vast and long-term effects of dangerous radioactive materials when an accident occurs [2]. For example, a nuclear facility in Iran experienced a cyber-attack, namely, “Stuxnet”, in 2010 [3–5]. In dealing with this emerging safety issue, the US NRC reports reinforce regulation guides, such as 10 CFR 73.54, Regulatory Guide (RG) 1.152 Version 2 and 3, and RG 5.71 [6–9]. The Institute of Electrical and Electronics Engineers (IEEE) issued IEEE Std. 7-4.3.2-2010, which addresses RG 1.152 Version 2 in view of cyber security [10]. The International Atomic Energy Agency (IAEA) published a technical guidance document for computer security at nuclear facilities under IAEA Nuclear Security Series No. 17 [11]. The Korea Institute of Nuclear Safety, a regulatory body of Korea, published RG 8.22 for controlling cyber security at nuclear facilities in Korea in 2011 [12]. A cyber security demonstration at ShinHanul units 1 and 2 and ShinGori units 3 and 4 was conducted, representing the first trial in Korea. There have also been various studies on how to apply relevant regulatory guides and standards for cyber security assurance at actual nuclear facilities [13,14]. The National Security Research Institute and the Korea Atomic Energy Research Institute are developing a cyber security evaluation system for nuclear power plants (NPP) [15].

One important focus of the evaluation of cyber security is to verify that the regulatory guides and the standards for cyber security are sufficiently complied with by the developers and/or the operators of a nuclear facility. Another focus is to evaluate the effects of system-specific vulnerabilities and the mitigation measures against them on cyber security. The first focus is related to the procedural aspects of cyber security, and the second focus is related to the technical aspects. In addition, while the first focus mainly involves qualitative evaluations, the second focus involves quantitative and qualitative evaluations. Thus, there has been a tendency so far for these two foci to be taken into account separately. However, cyber security should be evaluated in an integrated manner so that the different aspects can be incorporated together for evaluation [16]. The procedural and technical aspects have a substantial relationship with each other because the quality of the procedural aspect affects the completeness of the technical aspect. For example, a cyber security program includes a mitigation measure against the vulnerability during cyber-attack, which is more complete when systematically

* Corresponding author. Tel.: +82 41 750 6252.
E-mail addresses: bigjoyman@khu.ac.kr (J. Shin), hsson@joongbu.ac.kr (H. Son), khalil523@khu.ac.kr (R. Khalil ur), gheo@khu.ac.kr (G. Heo).

http://dx.doi.org/10.1016/j.ress.2014.10.006
0951-8320/© 2014 Elsevier Ltd. All rights reserved.

checking the procedural aspect versus not considering it. A systematic model that can be used for cyber security evaluation is useful for addressing this issue. This work suggests a cyber security risk model to evaluate cyber security for nuclear facilities in an integrated manner. The suggested model enables the evaluation of both the procedural and technical aspects of cyber security.

To develop the cyber security risk model, an activity-quality analysis model was developed first to evaluate how sufficiently people and/or organizations comply with the regulatory guides for cyber security. The architecture analysis model was created second to evaluate the vulnerabilities and mitigation measures with respect to their effects on cyber security. Then, the two models were integrated into a single model, which is called the cyber security risk model, so that cyber security could be evaluated from the procedural and technical viewpoints at the same time. The Bayesian network (BN) facilitated the integration of the two models. In addition to the integration, the BN makes it possible to perform various analyses that provide useful and integral perspectives on cyber security. For example, the reasoning of cyber-attack sources can be achieved through the back propagation capability of the BN. The model is applied to evaluate the cyber security risk of a research reactor and demonstrate its usefulness. In spite of their inherent safety, research reactors may be more vulnerable from the viewpoint of cyber security because of frequent operator access. Particularly, the demonstration was performed for the reactor protection system (RPS), which is a crucial I&C system for nuclear safety.

Section 2 describes the cyber security risk analysis model developed in this work. After introducing the basic concepts of the BN briefly, the activity-quality analysis model, architecture analysis model, and integrated cyber security risk analysis model are described. The analysis results for the RPS of a research reactor using the integrated model are provided in Section 3. Section 4 concludes this article.

2. Cyber security risk analysis model

2.1. Basic concepts

2.1.1. Activity-quality

The term ‘activity-quality’ describes how people and/or organizations 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 [6–9,12], and their relevant standards. We assume that when cyber security activities are performed well according to the regulatory guides that the activity-quality is good and the risk is low. In this work, the activity-quality is evaluated based on RG 5.71.

The cyber security regulatory guides require that the functionality of the reactor I&C systems be assured by following guidelines regarding confidentiality, integrity, and ensuring the availability of data against cyber threats. The confidentiality means that the resource information for the protection system should not be exposed to an unauthorized subject, and the integrity is the concept of ensuring that the hardware and software information that comprise the system to be protected is complete, accurate, and correct. The availability is the concept of the guarantee that legitimate users can use the information and perform the function at any time. To perform cyber security activities with the concepts described above, the regulatory guide proposes an analysis of the vulnerability regarding the object and a deduction of the cyber threats due to the vulnerability. To prevent and/or mitigate cyber threats, the regulatory guide proposes cyber security evaluation as follows:

- Appropriateness of the assessment for the cyber security policy and plan.
- Evaluation for the cyber security organization and system.
- Appropriateness of the assessment for the cyber security level.
- Appropriateness of the assessment for the access and control technique included in intrusion detection and prevention.
- Appropriateness of the assessment for the password management technique.
- Connection evaluation of the network and/or equipment.
- Appropriateness of the assessment for the recording, storage, and preservation of information.
- Integrity assessment of the software.
- Appropriateness of the assessment for the management technique for a commercial product.
- Appropriateness of the assessment for physical access.
- Reflect the result of the periodic analysis and/or evaluation and the assessment of a cyber security audit.

The activity-quality analysis model, which is described in Section 2.2.1, incorporates all the proposals of the regulatory guide mentioned above.

2.1.2. Typical architecture of the RPS

The RPS is a safety-grade I&C system that performs a reactor trip by making a trip signal and by inserting control rods into a reactor core for the protection of the nuclear reactor when anticipated operational occurrences (AOO) occur. It monitors various parameters for the informed reactor state, such as power, temperature, pressure, and coolant flow to trip when a reactor reaches an abnormal state.

The RPS architecture is generally composed of a bistable processor (BP), coincidence processor (CP), interface and test processor (ITP), and maintenance and test processor (MTP) in a single channel [17,18]. The BP transfers the trip signal to the CP when the input data parameter(s) exceeds the standard trip set point. The CP receives the trip signal from the BP using logic such as 2-out-of-4 or 2-out-of-3 to make a trip-initiation signal. The function of the ITP is to test whether the signal state from the BP is fine and to monitor each RPS state. In addition, the ITP delivers these results and values to the MTP and post-accident monitoring system (PAMS). The MTP provides the display and control needed to support RPS operation. It is used during RPS maintenance and transfers information to the main control room (MCR) through the information processing system (IPS).

2.1.3. Bayesian network and cyber security evaluation index

The compliance with the cyber security guide is inherently qualitative, and thus it is difficult to represent the relevant quality quantitatively. The BN is often used to overcome this difficulty by converting the qualitative value to the quantitative value [19,20]. The BN is a directed acyclic graph of an arc that represents the dependencies between the nodes and variables using Bayes' theorem [21]. Bayes' theorem is represented in Eq. (1):

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

where $P(x)$ is the probability distribution of variable x at the entire population, $P(C)$ is the prior probability that some sample belongs to a class, $P(x|C)$ is the conditional probability for obtaining the value of variable x, and $P(C|x)$ is the posterior probability that the value of variable x belongs to a class in a given situation. Newly learned information about the conditional probability can improve the probability by calculating the relationship between the posterior and prior probability. The BN is composed of a node, arc and node probability table (NPT). The node and arc are a variable and the cause-and-effect relationship, respectively. The nodes have two types: parent and child. The child node has the cause element, and the parent node has a result element of the child nodes. The NPT is the probability table that summarizes the occurrence probability between the causal relationship nodes. Because the NPT values can be used as observable quantities, latent variables, unknown parameters, or hypotheses, they are useful for changing from the qualitative problems to the quantitative problems.

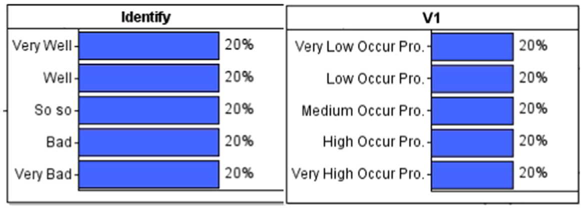
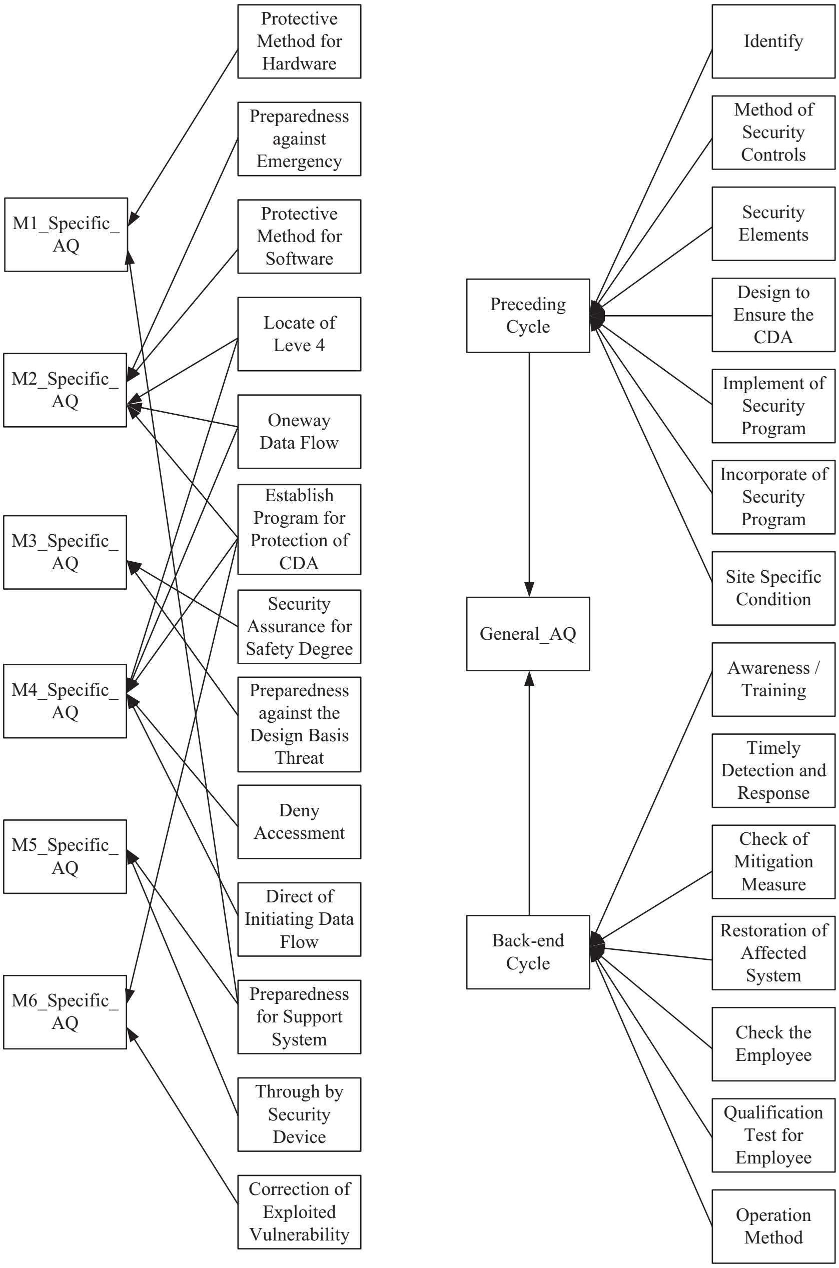


Fig. 1. The node example of activity-quality checklist and architecture vulnerability.

The cyber security risk index (CSRI) is the probability of cyber-attack occurrence or the completeness of the mitigation measure and/or the extent of activity-quality. No CSRI index has the value of ‘0’ or ‘100’. In this work, to evaluate the qualitative value, the evaluation degree of each node is divided into 5 levels, including very low, low, normal, good, and very good. Each CSRI index is converted into a five-stage metric. When each node is evaluated, the weight value can be input into each node according to its qualitative data as follows [22]:

- The numeric values of the activity-quality checklist node at each stage (as shown on the left side of Fig. 1) are ‘Very Well=0.9’, ‘Well=0.7’, ‘So So=0.5’, ‘Bad=0.3’, and ‘Very Bad=0.1’.
- In the same way, the numeric values of the architecture vulnerability (as shown on the right side of Fig. 2) are ‘Very Low Attack Occurrence Probability=0.9’, ‘Low Attack


Protective Method for Hardware
Preparedness against Emergency
Protective Method for Software
Locate of Leve 4
Oneway Data Flow
Establish Program for Protection of CDA
Security Assurance for Safety Degree
Preparedness against the Design Basis Threat
Deny Accessment
Direct of Initiating Data Flow
Preparedness for Support System
Through by Security Device
Correction of Exploited Vulnerability
M1_Specific_ AQ
M2_Specific_ AQ
M3_Specific_ AQ
M4_Specific_ AQ
M5_Specific_ AQ
M6_Specific_ AQ
Identify
Method of Security Controls
Security Elements
Design to Ensure the CDA
Implement of Security Program
Incorporate of Security Program
Site Specific Condition
Awareness / Training
Timely Detection and Response
Check of Mitigation Measure
Restoration of Affected System
Check the Employee
Qualification Test for Employee
Operation Method
Preceding Cycle
General_AQ
Back-end Cycle

The Specific Activity-Quality Checklists The General Activity-Quality Checklists

Fig. 2. The activity-quality analysis model using the BN.

Occurrence Probability=0.7’, ‘Medium Attack Occurrence Probability=0.5’, ‘High Attack Occurrence Probability=0.3’, and ‘Very High Attack Occurrence Probability=0.1’.

The CSRI index of a single node is calculated by multiplying the numeric values of each stage and the weight of each stage evaluation as shown in Eq. (2):

$$\mathrm{CSRI} = \sum_{s=1}^{5} 10(2s-1) \times w_s \tag{2}$$

such that weights w_s of stages ‘s’ are:

$$\sum_{s=1}^{5} w_s = 1 \tag{3}$$

where s is a numeric value of the activity-quality checklist node or architecture vulnerability at each stage. These values are presented in Table 1. w_s is the weight of the ‘s’ stage, which denotes the share of a single node. The value of w_s for a single node is 1 aggregating each weight of stages 1 to 5.

For example, evaluating the left node score of Fig. 1 is ‘$\mathrm{CSRI}_{(\mathrm{Identify})}=10 \quad (2\times1-1)\times0.2+10 \quad (2\times2-1)\times0.2+10 \quad (2\times3-1)\times0.2+10 \quad (2\times4-1)\times0.2+10 \quad (2\times5-1)\times0.2=50$’. If the activity-quality is evaluated as ‘very well’, it has a maximum of 90 points, while it has a minimum of 10 points if the activity-quality is evaluated as ‘very bad’. The security check can be verified based on the CSRI index, which has a range between the lower and upper values of 10 and 90, respectively. However, in terms of the architecture vulnerability for cyber security, the score for the architecture vulnerability node has a minimum of 10 points when the cyber-attack probability is the highest.

2.2. *Cyber security risk model*

2.2.1. *Activity-quality analysis model*

Based on RG 5.71 [9] with additional aid from KINS/RG-N 08.22 [12], checklists were developed for verifying whether the cyber security regulatory guide is compiled well. The checklists are derived by analyzing the regulatory guides for a total of 34 items. These checklists can be allocated to each phase of the cyber security lifecycle, which comprises the whole cycle of cyber security activity, including ‘establish program’, ‘integrate’, ‘continuous monitoring’, ‘review’, ‘change control’ and ‘record’. It is possible to systematically evaluate the overall activity-quality without the omitted portion by evaluating the checklist according to the cyber security lifecycle. For example, ‘How well do the identified critical digital assets (CDAs) follow the regulation?’ is allocated to the ‘establish program’ phase in the cyber security lifecycle. This is because the subject of the application for cyber security must be defined at an early stage such as the ‘establish program’ stage for the development of the cyber security program. The checklist that evaluates ‘How does the licensee maintain its cyber security program?’ is assigned to the ‘continuous monitoring’ phase. To check the strength of the cyber security program, it is continuously monitored to confirm the provision of information to the operator regarding how well the cyber security program is performed. It can be assessed that the monitoring of the cyber security program is meaningless if it does not work for various reasons. After the checklists are systematized as mentioned above, the checklists are transformed into a BN model by assigning each checklist to a child node and performing an overall evaluation of the activity-quality to the parent node. The intermediate parent nodes between the child nodes and the final parent node are made by grouping them with relevant child nodes for a rapid calculation. If one parent node is linked with many child nodes, the calculation of the BN becomes very slow, and thus, the intermediate node is introduced to solve this problem. A grouping example is as follows: The checklist item “Does the data only flow from one level to other levels through a device or devices that enforce the security policy between each level?” confirms the presence or absence of a safety device between the safety levels based on the security defensive architecture. The checklist item “Are the data flows allowed for only one-way from Level 4 to Level 3 and from Level 3 to Level 2?” verifies the one-way data flow across the safety importance levels. The checklist item “Are CDAs associated with safety allocated to Level 4 and protected from all lower levels?” checks whether the CDAs related closely with the safety level are set on the safety level and are protected against cyber-attack. These can be grouped into the intermediate parent node for “defense-in-depth”. The steps for the lifecycle and the classification of checklists for activity-quality are shown in Table 2.

Table 1
Numeric value of stage for architecture model and activity-quality model.

Architecture Model		**Activity-quality model**	
Numeric value of stage	Mean (Attack Occurrence)	Numeric value of stage	Mean (Compliance)
5	Very Low	5	Very Well
4	Low	4	Well
3	Medium	3	So so
2	High	2	Bad
1	Very High	1	Very Bad

The final risk of the activity-quality can be modeled as the accumulated risks from each checklist using the BN. Fig. 2 shows an example of the activity-quality analysis model. The activity-quality analysis model, which is developed by using the BN, is a reflection of the evaluation based on the checklists for the activity-quality.

Considering the relationship with the architecture analysis model described in Section 2.2.2, the checklists are classified into specific activity-quality checklists and general activity-quality checklists according to their influences on the mitigation measures, which are important factors of the architecture analysis model. The checklists involved with the specific activity-quality checklist are grouped, and they affect the mitigation measures substantially. It should be noted that each checklist only affects the corresponding mitigation measure. The checklists included in the general activity-quality checklist are those that do not affect any of the mitigation measures. These general checklists are grouped again into the preceding cycle checklists, and the back-end cycle checklists are grouped in accordance with the cyber security lifecycle. Reflecting these groupings straightforwardly, the BN model is developed to collect (to obtain an update of) the cyber security risk.

2.2.2. *Architecture analysis model*

In this work, the architecture analysis model is constructed for a research reactor RPS. Although the model is system specific, it offers a general perspective for the construction of the architecture analysis model for any system. The analysis model for the RPS architecture of a research reactor was divided into vulnerability and mitigation measure parts to allow consideration of the extent to which the architecture is vulnerable and how much mitigation is effective. The vulnerability analysis of the RPS for a NPP was performed [15]. However, the results of the analysis cannot be used to construct the architecture analysis model for the RPS of a research reactor because of the differences between the RPS architectures. Thus, the vulnerability analysis for a research reactor RPS was performed in this work. The characteristics of the RPS

Table 2
Example of the activity-quality checklist.

Lifecycle	Classification	Evaluation items
Establish Cyber Security Program	Definition	How well critical digital assets (CDAs) 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?
		Does the data only flow from one level to other levels through a device or devices that enforce security policy between each level?
Integrate	System protection	Does the licensee protect systems and networks from the cyber-attacks damage data or software?
		Does the licensee protect systems and networks from the cyber-attacks which deny access or damage to system, services, or data?
		Does the licensee protect systems and networks from the cyber-attacks damage system, network, and associated equipment?
Monitoring	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?

architecture of the NPP and research reactor is as follows:

(a) The NPP RPS has 4 channels, while the research reactor RPS has 3 channels;
(b) The BP set points can be changed depending upon the situation in the case of a NPP, while this is not possible for a research reactor
(c) The research reactor RPS has a one-way flow of information in the network, whereas the NPP RPS also has reverse information buses;
(d) The NPP RPS has 2-out-of-4 coincidence logic, and the research reactor RPS has 2-out-of-3 coincidence logic.

The RPS architecture of a research reactor may be simplified with respect to the interfaces and operation, as shown in Fig. 3.

There are 5 vulnerabilities and 6 mitigation measures, which are selected for the cyber security analysis of two cases. The two cases are ‘insertion of reactor trip through RPS’ and the ‘scram halt through RPS’. The list of vulnerabilities is described in detail as follows [23,24]:

(1) Denial of Service (DoS) attacks and the introduction of malware to system networks during maintenance work (V1),
(2) System shut-down by contagion of malware during maintenance work (V2),
(3) Data alteration by contagion of malware during maintenance work (V3),
(4) DoS occurrences and malware spread to other systems because of vulnerabilities existing in the system (V4),
(5) Data alteration using recognized vulnerabilities from standard communication protocols (V5).

The list of mitigation measures applicable to counter the aforementioned vulnerabilities are explained below:

1) Establishment of infection detection systems for external storage media, such as USBs or PCs, for PLC maintenance work,
2) Establishment of a security system, including firewalls, intrusion detection systems and/or intrusion prevention systems,
3) Check for running services,
4) Network monitoring,
5) Establishment of device validation policies,
6) Vulnerability patches.

The analysis result of the vulnerability and mitigation measure of a research reactor is described in Table 3. The evaluations for these vulnerabilities and mitigation measures are reflected in the architecture analysis model.

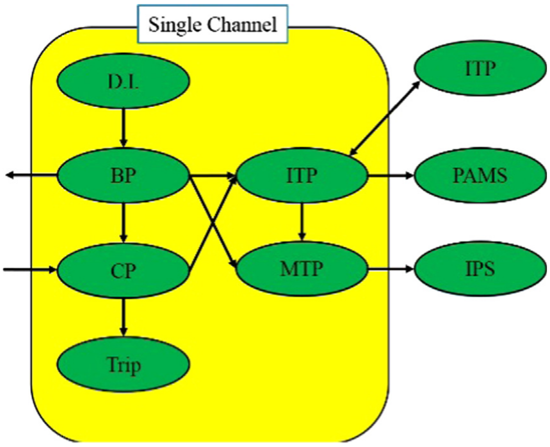


Fig. 3. The architecture of single RPS channel of a research reactor.

The architecture analysis model was constructed by using the BN and by considering the RPS architecture of a research reactor (shown in Fig. 3) and the vulnerability and mitigation measure analysis result, as shown in Fig. 4. The relative occurrence probability of the vulnerability for each RPS component is provided in the NPT. The reduction probability of the vulnerability on each component is provided for mitigation measures through the NPT. Mitigation measures reduce the vulnerability probability by applying the concept of diversity at the plant and system levels. Each level of mitigation has a different effect on reducing vulnerability. It is assumed that one mitigation measure can reduce the vulnerability by a large amount, and additional mitigation measures may reduce vulnerability to much extend.

The characteristics of this BN model are as follows: First, it reflects the analysis result of the vulnerability and mitigation measures of a research reactor RPS architecture. Second, it reflects the correlation of the components on the RPS architecture. Finally, it emphasizes the relationship among the components, vulnerability, and mitigation measures.

2.2.3. *Cyber security risk model*

The cyber security risk model, which produces a measure denoted as “Cyber Security Risk”, was created by integrating the activity-quality analysis model and the architecture analysis model, both of which are developed based on the BN. With the integrated model, the cyber security risk analysis can be

Table 3
The cyber security analysis of research reactor RPS architecture.

	BP	CP	ITP	MTP	Intra-channel network
Network input	D.I./ITP	BP/intra-channel	BP/CP/intra-channel	BP/ITP	BP/ITP/MTP
Network output	CP/ITP/MTP intra-channel network	ITP/initiation logic	BP/PAMS/MTP/intra-channel network	IPS	CP
Blocking of data traffic by the security level difference	Data receipt form intra-channel network	Data receipt form intra-channel network	Data receipt from intra-channel network	–	Data transmission to BP, CP, ITP, MTP
Access by maintenance	Yes	Yes	Yes	Yes	–
Vulnerabilities	V1, V2, V3	V1, V2, V3	V1, V3	V1, V3, V4	V5
Impact to	CP/ITP/intra-channel network	ITP/initiation logic	PAMS/MTP	IPS	BP/CP/ITP/MTP
Possible mitigation measures	M1, M2, M3, M4	M1, M2, M3, M4	M1, M2, M3, M4	M1, M2, M4, M5	M4, M6

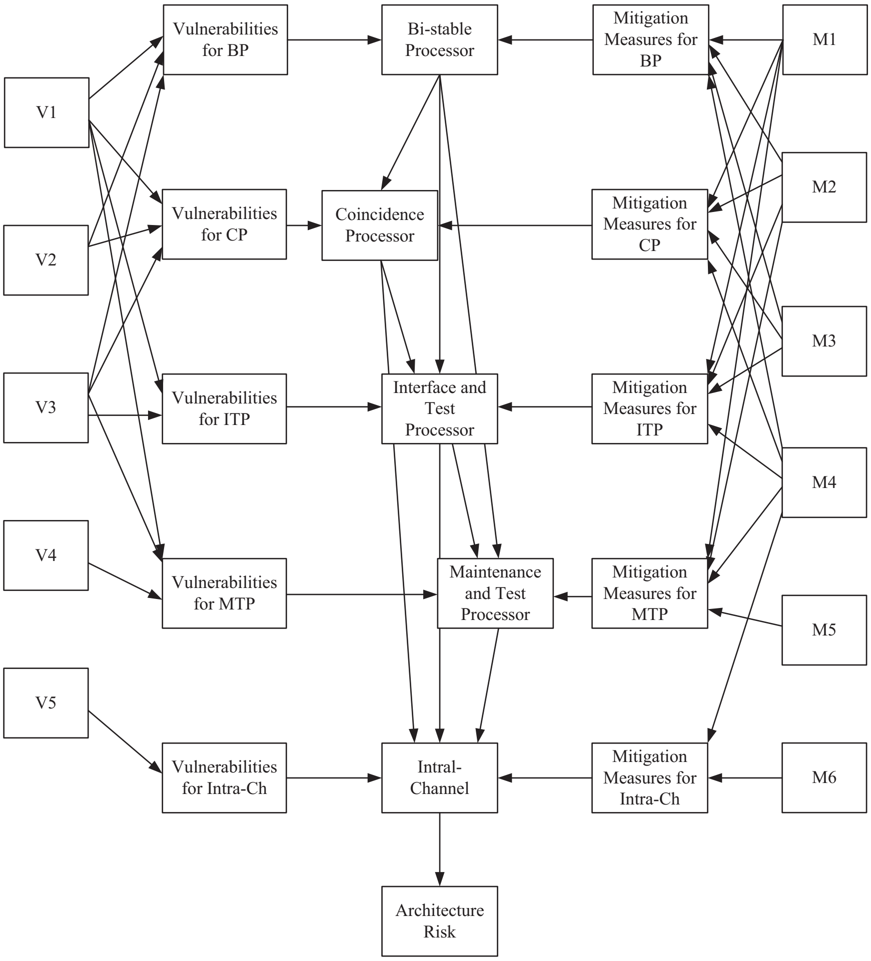

Vulnerabilities for BP
Bi-stable Processor
Mitigation Measures for BP
M1
V1
Vulnerabilities for CP
Coincidence Processor
Mitigation Measures for CP
M2
V2
M3
V3
Vulnerabilities for ITP
Interface and Test Processor
Mitigation Measures for ITP
M4
V4
Vulnerabilities for MTP
Maintenance and Test Processor
Mitigation Measures for MTP
M5
V5
Vulnerabilities for Intra-Ch
Intral-Channel
Mitigation Measures for Intra-Ch
M6
Architecture Risk

Fig. 4. The architecture analysis model for RPS of a research reactor.

performed [25–27]. The cyber security risk model for the RPS of a research reactor is depicted in Fig. 5.

BN has the ability to perform a Bayesian update based on NPT inputs which can be provided by using either system of equations or input data in terms of probability [17,28]. In this work, a representative calculation method is 'WMean', which is one of the truncated normal distribution (TNormal) calculations for calculating the child node value from the parent nodes as shown in Eq. (4):

$$p(Y|X) = \text{TNormal}\left(\frac{\sum_{i=1}^{n} w_i X_i}{\sum_{i=1}^{n} w_i}, \frac{1}{\sum_{i=1}^{n} w_i}, 0, 1\right) \quad (4)$$

where X is the parent node, Y is the child node and has range of [0,1], n is the number of parent nodes and w_i is the weight value of X_i for explaining Y. Each mitigation measure group for each RPS component (M_BP, M_CP, M_ITP, M_MTP, M_Intra Channel), which is a child node in the RPS architecture model and is affected by the parent node similar to each mitigation measure (M1, M2, M3, M4, M5, M6), can be used by the *MIXMINMAX* function from the BN because it reduces cyber-attacks at a greater rate of occurrence versus vulnerability [29]. The equation for the *MIXMINMAX* function is Eq. (5):

$$MIXMINMAX = \frac{w_{min}MIN(X, Y, Z, \ldots) + w_{max}MAX(X, Y, Z, \ldots)}{w_{min} + w_{max}} \quad (5)$$

where w_{min}, $w_{max} > 0$. The ratio of w_{max} to w_{min} is in proportion to 'w_{min}:w_{min}=5:2' and presents that each mitigation measure is stronger than the vulnerability of cyber security. *MIN(X, Y, Z, …)* and *MAX(X, Y, Z, …)* are determined by Eqs. (6) and (7):

$$WMIN = \underset{\forall i=1,\ldots,n}{MIN}\left[\frac{w_iX_i+\sum_{i\neq j}^{n}X_j}{w_i+(n-1)}\right] \tag*{6)}$$

$$WMAX = \underset{\forall i=1,\ldots,n}{MAX}\left[\frac{w_iX_i+\sum_{i\neq j}^{n}X_j}{w_i+(n-1)}\right] \tag{7}$$

where the weight factor w_i in Eqs. (6) and (7) is always $w_i \geq 0$. The *WMIN* and *WMAX* functions can be viewed as a generalized version of the normal *MIN* and *MAX* functions. The mitigation measure is represented by entering different values appropriately with weight factors w_{min} and w_{max}, without being biased on *WMIN* and *WMAX* when using the *MIXMINMAX* method.

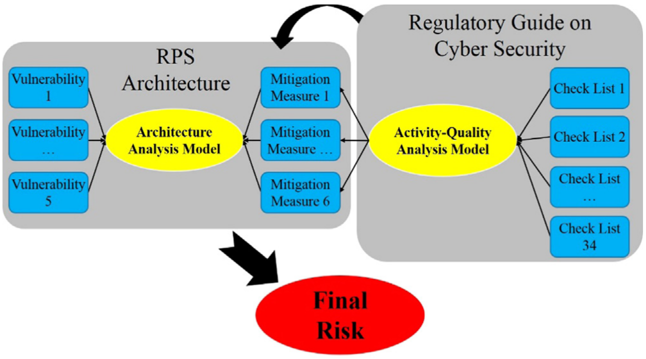


Fig. 5. The cyber security risk model composed with the activity-quality model and the architecture analysis model.

The mitigation measure to prevent and mitigate cyber-attack involves the cyber security activity-quality. The activity-quality analysis model, which evaluates how well people and/or organizations comply with the cyber security regulatory guide, is linked with the mitigation measures of the RPS architecture analysis model to develop the cyber security risk model using the BN. According to the extent of influence and particularity for mitigation measures, the activity-quality checklists are separated into a specific checklist group and general checklist group to reflect the items effectively.

The modeling was performed with the AgenaRisk Pro Version 6.0 module (as shown in Fig. 6). By using this model, we can analyze the interactions among the checklists and identify the critical element in the event of a threat. In addition, this model will be used to develop simulated penetration test scenarios according to various situations.

3. Results and discussions

We analyzed the cyber security risk by using the cyber security risk model that integrates the activity-quality analysis model and the architecture analysis model. This analysis was performed with several scenarios in which it is postulated that the following cyber threats exist: the system has vulnerabilities, and the cyber security activities and countermeasures for the system are not perfect. Although the cases in this study did not fully cover whole

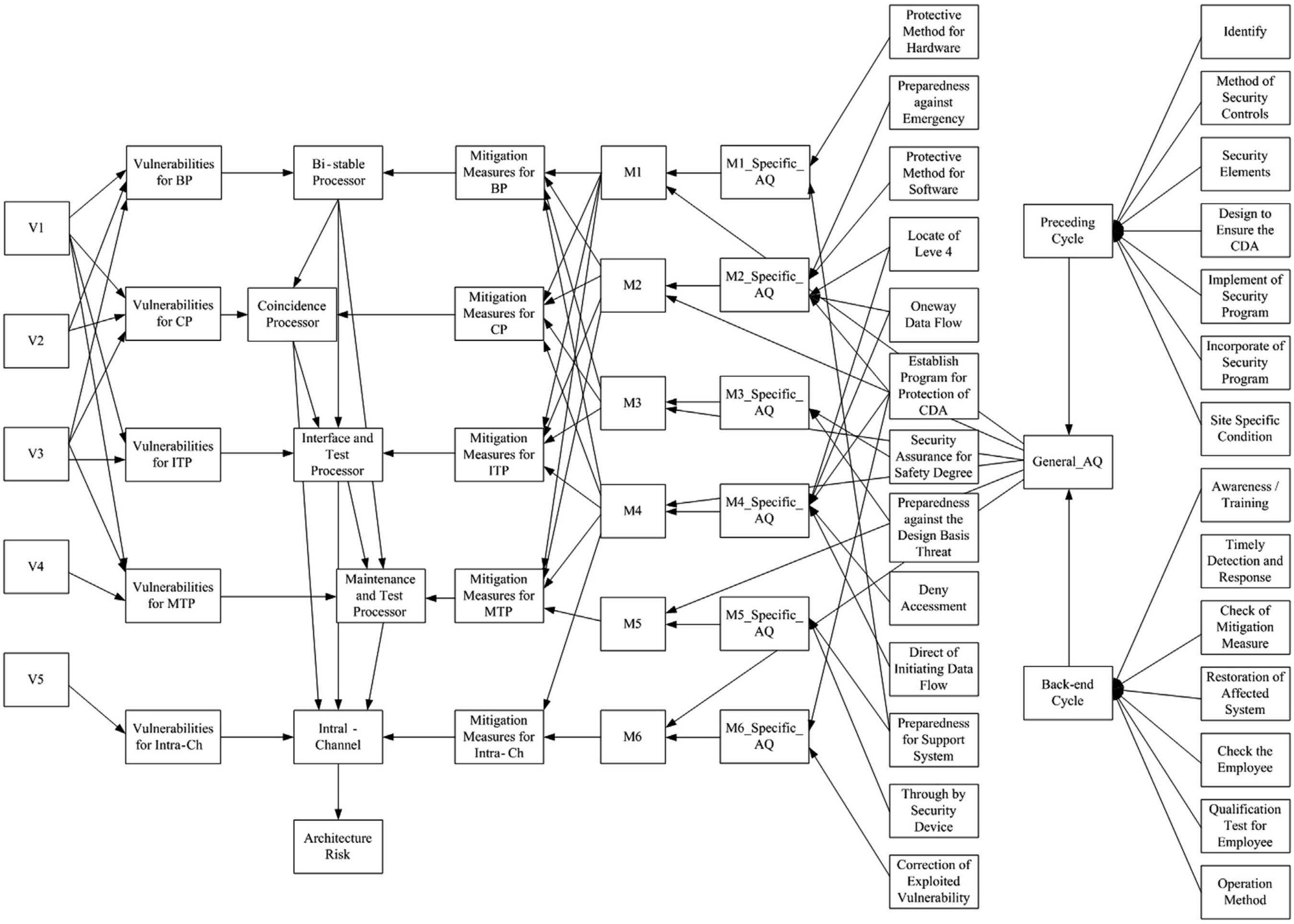

V1
V2
V3
V4
V5
Vulnerabilities for BP
Vulnerabilities for CP
Vulnerabilities for ITP
Vulnerabilities for MTP
Vulnerabilities for Intra-Ch
Bi-stable Processor
Coincidence Processor
Interface and Test Processor
Maintenance and Test Processor
Intral - Channel
Architecture Risk
Mitigation Measures for BP
Mitigation Measures for CP
Mitigation Measures for ITP
Mitigation Measures for MTP
Mitigation Measures for Intra- Ch
M1
M2
M3
M4
M5
M6
M1_Specific_ AQ
M2_Specific_ AQ
M3_Specific_ AQ
M4_Specific_ AQ
M5_Specific_ AQ
M6_Specific_ AQ
Protective Method for Hardware
Preparedness against Emergency
Protective Method for Software
Locate of Leve 4
Oneway Data Flow
Establish Program for Protection of CDA
Security Assurance for Safety Degree
Preparedness against the Design Basis Threat
Deny Accessment
Direct of Initiating Data Flow
Preparedness for Support System
Through by Security Device
Correction of Exploited Vulnerability
Preceding Cycle
General_AQ
Back-end Cycle
Identify
Method of Security Controls
Security Elements
Design to Ensure the CDA
Implement of Security Program
Incorporate of Security Program
Site Specific Condition
Awareness / Training
Timely Detection and Response
Check of Mitigation Measure
Restoration of Affected System
Check the Employee
Qualification Test for Employee
Operation Method

Fig. 6. The cyber security risk model for RPS.

scenarios, the analysis results provide useful information to evaluate the cyber security of a system in an integrated manner and confirm that the model reflects the intuition of both the activity-quality and the system architecture.

3.1. Analysis of the vulnerability and the activity-quality checklist when a cyber-attack occurs on the MTP

The purpose of this analysis is to obtain information on which vulnerabilities and activity-quality checklists should be prioritized in the design, development, testing, and maintenance in view of cyber security when a component of the RPS is assumed to receive a cyber-attack. Supposing that no preliminary evaluation is performed, the point of 20% is assigned to each stage of a node, resulting in an average of 50 points given to the node in total. Then, the high points (i.e., 70 points) are assigned to the BP, CP, and ITP nodes as hard evidence. This means that these components have a low likelihood of being attacked. After this, 10 points are assigned to the MTP node as hard evidence, which means that the MTP was attacked. The simulation results of the model are analyzed.

The vulnerability V4 decreased to 14.12 points (a 35.88-point decrease), which is the greatest decrease in this analysis, indicating that this vulnerability is the most risk significant in this scenario. The V4 node in Fig. 7 shows that the occurrence probability is very high because of the cyber-attack on the MTP. V1 and V3 also decreased to 25.58 because of the 24.42-point decrease, which indicates that they are less risky than V4 in a half level approximately. V1 and V3 are the vulnerabilities affecting other RPS components (BP, CP, and ITP) and the MTP. The degree of risk, that is, the occurrence probability, did not increase significantly compared with the case of V4, which affects the MTP alone. However, the occurrence probability of V2 was very low, as shown in Fig. 8. The value of the node increased by 22.89 points and reached 77.89 points. Because the risk of cyber-attack from other RPS components (BP, CP, and ITP) is assumed to be low, the occurrence probability of V2, which did not have a direct effect on the MTP, decreased.

The analysis results show that the completeness of the mitigation measures affecting the MTP decrease in the following order: M1, M2, M4, and M5. In addition, because the points of the mitigation measure nodes decreased, the activity-quality checklist evaluating each mitigation measure is affected. For example, the CSRI affecting M5, including 'Support System' and 'Through Device', had very low scores, 25.45 and 17.94, respectively. The checklist 'Denial of Access' decreased by 35.17 points. These checklists are the subjects to which careful attention should be given through the cyber security lifecycle. The other checklists yield a relatively small decrease of approximately 5 points and are insignificant compared to the above checklists. In this way, it is possible to identify the checklists that should be carefully addressed at the next cyber security lifecycle phase by analyzing the changes in the values of the activity-quality nodes affecting the mitigation measures.

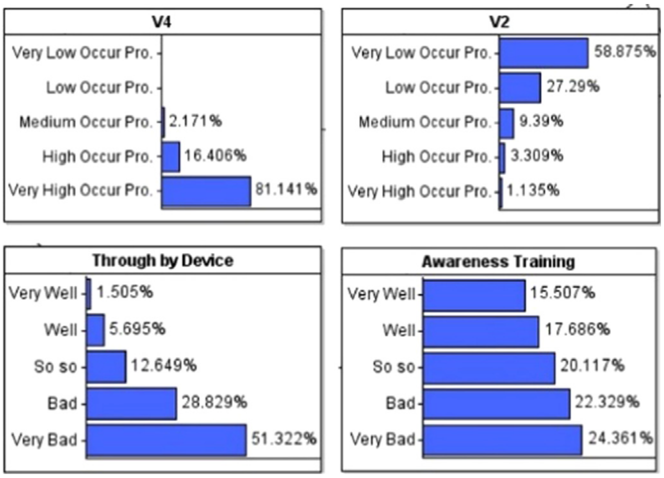


Fig. 7. Analysis results for the vulnerabilities and the activity-quality checklists when a cyber-attack occurs to the MTP.

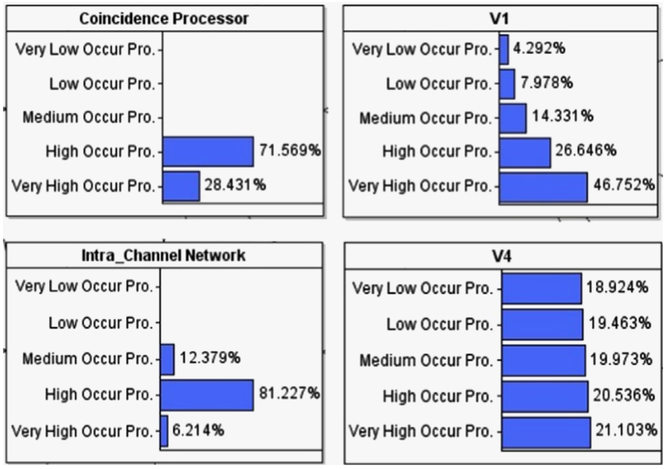


Fig. 8. The analysis results for the vulnerabilities and the RPS components when a cyber-attack occurs to the RPS.

3.2. Analysis of the vulnerability and mitigation measure when a cyber-attack occurs on the RPS

This analysis will derive the risk information on the vulnerabilities and mitigation measures of the RPS in the case of a cyber-attack on the RPS by using the back propagation feature of the BN. To perform this analysis, 50 points were initially assigned to all the checklists and vulnerability nodes as soft evidence, and 10 points were assigned to the "Final Risk" node as hard evidence because of the initial condition of an attack on the RPS is assumed.

After the back propagation with the BN model, the CSRI of the BP (31.38 points), CP (24.31 points), ITP (32.56 points), MTP (36.79 points), and intra-channel (31.18 points) decreased. This result shows that the CP and intra-channel are more risk significant than the others. There may be two prominent methods to illegitimately control the control rod as a result of a cyber-attack on the RPS. One method is generating trip signals through the CP inappropriately or forcedly blocking them despite their necessity. The other method is distorting the information via intra-channel that results in running an unexpected process on the RPS. Fig. 8 shows that the occurrence probabilities of a cyber-attack are high or very high. This means that the analysis result of the BN model adequately reflects two possible attacks on the RPS mentioned above.

The points of cyber security vulnerability are 29.28 points (V1), 31.78 points (V2), 29.28 points (V3), 48.91 points (V4), and 34.96 points (V5). This means that the occurrence probability is greater in the following order: V1 and V3 (both are in the same rank), V2, V5, and V4. This means that V1 and V3 affect the cyber security of the RPS more significantly than V4 and V5, if there is no hard evidence that a specific system or component is under attack. This becomes obvious if it is considered that V1 and V3 are linked to more components than other vulnerabilities.

Finally, the points representing the completeness of the mitigation measures for cyber security vulnerability are 36.80 points (M1), 36.67 points (M2), 36.04 points (M3), 36.30 points (M4), 44.63 points (M5), and 37.06 points (M6). This means that the completeness of the mitigation measures decreases in the following order: M3, M2, M1, M6, and M4. Based on these results, we could suggest a good practice in which the mitigation measures can be prioritized according to the resulting order of the activities related to cyber security after a cyber-attack.

3.3. Analysis of the RPS cyber security risk and the optimal mitigation measures regarding vulnerabilities

This analysis is for analyzing the cyber security risk and the optimal mitigation measures with respect to each vulnerability of the RPS.

In this analysis, 30 points are assigned to the nodes of every mitigation measure, which means the mitigation measures have a relatively low completeness. Meanwhile, 70 points are assigned to all the vulnerabilities, which denotes low occurrence probabilities. To analyze how weak the components of the RPS are against each vulnerability by raising the occurrence probability of each vulnerability one-by-one, we examined the effect of the probability-raised vulnerability on cyber security. As shown in Table 4, the BP and CP are weakest versus the vulnerability of V1, V2 and V3. The ITP is also weakest versus V1 and V3. The intra-channel is the weakest versus V5. For the RPS architecture, the cyber security risk increases according to the vulnerability in the following increasing order: V1 and V3, V2, V5, V1, and V4. These analysis results show that V1 and V3 are the most significant for the RPS cyber security. This is because V1 and V3 are related to more components of the RPS than other vulnerabilities, and its influence cannot be more easily reduced by mitigation measures.

To determine the optimal mitigation measures for each vulnerability, we increased the score of each node, representing the completeness of the mitigation measures. Table 5 provides the analysis results for V3. This result shows that M4 (i.e., monitoring networks) is the most critical to cyber security. In fact, M4 significantly reduced the risk of nearly all vulnerabilities as its completeness increased. M5 (i.e., installing an encryption equipment) and M6 (i.e., vulnerability patch) are not significant for V3. Meanwhile, other mitigation measures such as M1 (firewall), M2 (intrusion prevention system), M3 (network monitoring), and M4 (monitoring external memory) have significance for cyber-attacks. M6 is the most effective measure for defending an inherent malware attack or DoS attack from other systems, such as V4.

Table 4
Part of analysis results for RPS cyber security risk.

	BP	CP	ITP	MTP	Intra-Ch	Final risk
	50.1911	46.3718	46.5533	47.3280	47.0961	46.7245
V1	40.0991	36.9303	34.5371	35.9281	40.1144	37.0731
(Gap)	10.0920	9.4415	12.0162	11.3999	6.9817	9.6514
V2	40.0991	36.9303	41.9942	43.4081	44.1814	38.5956
(Gap)	10.0920	9.4415	4.5591	3.9199	2.9147	8.1289
V3	40.0991	36.9303	34.5371	35.9281	40.1144	37.0731
(Gap)	10.0920	9.4415	12.0162	11.3999	6.9817	9.6514
V4	50.1911	46.3718	47.0961	42.5732	45.3986	46.4325
(Gap)	0	0	0.5428	4.7548	1.6975	0.292
V5	50.1911	46.3718	47.0961	42.5732	31.6413	42.6569
(Gap)	0	0	0.5428	4.7548	15.4548	4.0676

Table 5
Part of analysis results for optimal mitigation measures.

	BP	CP	ITP	MTP	Intra-Ch	Final risk
V3	40.0991	36.9303	34.5371	35.9281	40.1144	37.0731
M1	60.1822	43.4156	61.4195	63.3357	50.7319	60.2271
(Gap)	20.0831	6.4853	26.8824	27.4076	10.6175	23.154
M2	60.1822	63.3028	61.4195	63.3357	50.7319	60.2271
(Gap)	20.0831	26.3725	26.8824	27.4076	10.6175	23.154
M3	60.1822	63.3028	61.4195	47.0614	48.7908	59.9117
(Gap)	20.0831	26.3725	26.8824	11.1333	8.6764	22.8386
M4	60.1822	63.3028	61.4195	63.3357	68.6534	64.8828
(Gap)	20.0831	26.3725	26.8824	27.4076	28.539	27.8097
M5	40.0991	36.9303	34.4456	52.1529	44.646	38.7283
(Gap)	0	0	0.0915	16.2248	4.5316	1.6552
M6	40.0991	36.9303	34.4456	35.9281	55.8885	41.501
(Gap)	0	0	0.0915	0	15.7741	4.4279

4. Conclusions

For cyber security evaluation, the activity-quality analysis model was proposed to check how people and/or organizations comply with the cyber security regulatory guide. This model helps to analyze the relationships of the activity-quality checklists and their influence on cyber security. The architecture analysis model was also developed, particularly for the RPS of a research reactor for illustrative purposes. For the definition of the critical cyber-attack scenarios on research reactors, the vulnerabilities and mitigation measures were analyzed. Furthermore, the cyber security risk model was constructed through the integration of the activity-quality analysis model and the architecture analysis model. This model can be utilized for the quantitative analysis by using the proposed measure cyber security risk and for various qualitative analyses. This analysis is possible because the activity-quality model, architecture analysis model and integrated cyber security risk model are all based on the BN.

A few types of analyses with respect to cyber security were performed by using the cyber security risk model. The analysis of the vulnerability and activity-quality checklist was performed with the assumption that a cyber-attack occurred on a component of the RPS's MTP. In this analysis, important checklists could be identified with respect to the cyber security quality activities. Further, the vulnerabilities and mitigation measures were analyzed when a cyber-attack to the RPS is assumed. If a cyber-attack occurs on a system scale, it is important to have confidence in which component is the key element corresponding to the attack situation. This analysis proved that the developed model could provide this type of information through the back propagation feature of the BN. Finally, the analysis of the RPS cyber security risk and optimal mitigation measures regarding vulnerabilities was performed. This analysis suggests that the use of the cyber security risk model makes it possible to create simulated penetration test scenarios.

In this work, the values of the NPTs that represent the correlation among the lists were selected based on expert opinions. Because the completeness of a BN model is affected by the accuracy of the NPT, future research will be performed to improve the values of the NPTs by incorporating additional expert opinions and information.

Acknowledgments

This work was supported by the Advanced Research Center for Nuclear Excellence (ARCNEX) program and was funded by the Ministry of Education, Science and Technology (Grant number: 2012-055432).

References

[1] Gan B, Brendlen Jr JH. Nuclear power plant digital instrumentation and control modifications. In: Nuclear science symposium and medical imaging conference, conference record of the 1992 IEEE; October, 1992. p. 730–732.

[2] Kesler B. The vulnerability of nuclear facilities to cyber attack. Strategic Insights 2011;10:15–25.

[3] Collins S, McCombie S. Stuxnet: the emergence of a new cyber weapon and its implications. J Polic Intell Count Terror 2012;7:80–91. http://dx.doi.org/10.1080/18335330.2012.653198.

[4] Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of cyber-warfare. Comput Secur 2012;31:418–36. http://dx.doi.org/10.1016/j.cose.2012.02.009].

[5] Miller B, Rowe D. A survey SCADA of and critical infrastructure incidents. In: Proceedings of the first annual conference on research in information technology; October, 2012. p. 51–56.

[6] USNRC. NRC Regulations. 10 CFR Part 73.54, protection of digital computer and communication systems and networks. Available at 〈http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html〉; 2009.

[7] USNRC. Regulatory guide 1.152, Revision 2, Criteria for use of computers in safety systems of nuclear power plants. Available at 〈http://pbadupws.nrc.gov/docs/ML0530/ML053070150.pdf〉; 2006.

[8] USNRC. Regulatory guide 1.152, Revision 3, Criteria for use of computers in safety systems of nuclear power plants. Available at 〈http://pbadupws.nrc.gov/docs/ML1028/ML102870022.pdf〉; 2011.

[9] USNRC. Regulatory guide 5.71, Cyber security programs for nuclear facilities. Available at 〈http://nrc-stp.ornl.gov/slo/regguide571.pdf〉; 2010.

[10] IEEE. IEEE Std 7-4.3.2-2010, IEEE standard criteria for digital computers in safety systems of nuclear power generating stations. doi: 10.1109/IEEESTD.2010.5542302; 2010.

[11] IAEA. IAEA nuclear security series no. 17, Computer security at nuclear facilities. Available at 〈http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf〉; 2011.

[12] Korea Institute of Nuclear Safety. KINS/RG-N08.22, Cyber security for I&C system; 2009.

[13] Park JK, Park JY, Kim YK. A graded approach to cyber security in a research reactor facility. Prog Nucl Energy 2013;65:81–7.

[14] Son HS, Kim SG. Defense-in-depth strategy for smart service sever cyber security. In: Computer applications for communication, networking, and digital contents. Berlin: Springer Verlag; 2012. p. 181–188.

[15] Song JG, Lee JW, Lee, Lee, Kwon KC, Lee DY. A cyber security risk assessment for the design of I&C systems in nuclear power plants. Nucl Eng Technol 2012;44:919–28. http://dx.doi.org/10.5516/NET.04.2011.065.

[16] Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. Comput Secur 2010;29:196–207. http://dx.doi.org/10.1016/j.cose.2009.09.002.

[17] Lee DY, Choi JG, Lyou J. A safety assessment methodology for a digital reactor protection system. Int J Control Autom Syst 2006;4:105–12.

[18] Park GY, Bae SH, Bang DI, Kim TG, Park JK, Kim YK. Design of instrumentation and control system for research reactors. In: Eleventh international conference on control, automation and systems; October, 2011. p. 1728–1731.

[19] Chu TL, Yue M, Varuttamaseni A, Kim MC, Eom HS, Son HS, et al. Applying Bayesian belief network method to quantifying software failure probability of a protection system. San Diego, CA: NPIC&HMIT; 2012 (July 22-26; 2012.).

[20] Sommestad T, Ekstedt M, Johnson P. A probabilistic relational model for security risk analysis. Comput Secur 2010;29:659–79. http://dx.doi.org/10.1016/j.cose.2010.02.002.

[21] Heckerman D. A tutorial on learning with Bayesian networks. In: Jordan M, editor. Learning in graphical models. Cambridge, MA: MIT Press; 1999.

[22] Fenton NE, Neil M, Caballero JG. Using ranked nodes to model qualitative judgments in Bayesian networks. IEEE Trans Knowl Data Eng 2007;19:1420–32. http://dx.doi.org/10.1109/TKDE.2007.1073.

[23] Bhatia S, Schmidt D, Mohay G, Tickle A. A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. Comput Secur 2014;40:95–107. http://dx.doi.org/10.1016/j.cose.2013.11.005].

[24] Zonouz S, Haghani P. Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior. Comput Secur 2013;39:190–200. http://dx.doi.org/10.1016/j.cose.2013.07.003].

[25] Shin JS, Son HS, Heo GY. Cyber security risk analysis model composed with activity-quality and architecture model. In: International conference on computer, networks and communication engineering 2013:609–12.

[26] Shin J, Son H, Kim S, Heo G. Application of Bayesian network methodology for evaluating industrial control system. Int J Control Autom 2014;7:189.

[27] Shin J, Son H, Heo G. Comparative study of cyber security characteristics for nuclear systems. In: Park JJ, editor. Frontier and innovation in future computing and communications. Dordrecht: Springer Verlag; 2014. p. 87–93.

[28] Wagner S. A Bayesian network approach to assess and predict software quality using activity-based quality models. Inf Softw Technol 2010;52:1230–41. http://dx.doi.org/10.1016/j.infsof.2010.03.016.

[29] Fenton N, Neil M. Ranked nodes: a simple and effective way to model qualitative judgements in large-scale Bayesian networks. Queen Mary, University of London, Department of Computer Science; 2005.