Nuclear Engineering and Technology 49 (2017) 517–524

Available online at ScienceDirect

Nuclear Engineering and Technology

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

Original Article

Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET

Jinsoo Shin [a], Hanseong Son [b,*], and Gyunyoung Heo [a]

[a] Department of Nuclear Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 446-701, Republic of Korea

[b] Computer and Game Science, Joongbu University, 201 Daehak-ro, Chubu-Myeon, Geumsan-gun, Chungnam 312-702, Republic of Korea

ARTICLE INFO

Article history:
Received 6 July 2016
Received in revised form
23 October 2016
Accepted 8 November 2016
Available online 28 November 2016

Keywords:
Activity–Quality
Architecture Analysis
Bayesian Network
Cyber Security
Reactor Protection System
Research Reactor

ABSTRACT

Cyber security is an important issue in the field of nuclear engineering because nuclear facilities use digital equipment and digital systems that can lead to serious hazards in the event of an accident. Regulatory agencies worldwide have announced guidelines for cyber security related to nuclear issues, including U.S. NRC Regulatory Guide 5.71. It is important to evaluate cyber security risk in accordance with these regulatory guides. In this study, we propose a cyber security risk evaluation model for nuclear instrumentation and control systems using a Bayesian network and event trees. As it is difficult to perform penetration tests on the systems, the evaluation model can inform research on cyber threats to cyber security systems for nuclear facilities through the use of prior and posterior information and backpropagation calculations. Furthermore, we suggest a methodology for the application of analytical results from the Bayesian network model to an event tree model, which is a probabilistic safety assessment method. The proposed method will provide insight into safety and cyber security risks.

1. Introduction

The development of digital technology related to instrumentation and control (I&C) systems influences many industries. The transition from analog to digital equipment has a number of benefits, but it also presents challenges. Cyber security has been emphasized recently due to the extensive use of digital I&C systems and the importance of cyber security in protecting these systems against cyber infrastructure attacks. Cyber attacks have been discussed over the past 15 years [1]. During this time, the importance of cyber security has increased in many parts of the energy sector due to the expansion of digital I&C systems in power generation facilities. Research budgets have been allocated to cyber security in accordance with its importance. Although many infrastructure systems involve supervisory control and data acquisition (SCADA), which can be used to protect against a cyber attack, no system can be completely protected. Cyber attacks have become an important issue for nuclear facilities due to associated safety concerns. At facilities such as nuclear power plants, safety is the most important consideration because nuclear accidents can lead to serious hazards. In January 2003, the Davis Besse

* Corresponding author.
E-mail address: hsson@joongbu.ac.kr (H. Son).
http://dx.doi.org/10.1016/j.net.2016.11.004

nuclear power plant in Ohio, USA, was infected by the SQL Slammer worm. Nuclear facilities in Iran have been targeted by cyber attacks, including the one in 2010 known as "Stuxnet" [2]. In this study, we focus on cyber security for nuclear facilities.

Various organizations and researchers have investigated means to control or prevent cyber attacks on nuclear facilities. Regulatory authorities have published many regulatory requirement documents, such as U.S. NRC Regulatory Guide 5.71 [3], 1.152 (versions 2 and 3) [4,5], IEEE Standard 7-4.3.2 [6], and the Korea Institute of Nuclear Nonproliferation and Control (KINAC) Regulatory Standard 015 [7]. Cyber security evaluations must consider these regulatory guides. The National Security Research Institute and the Korea Atomic Energy Research Institute are developing a nuclear power plant cyber security evaluation system [8]. Cyber security research involving nuclear facilities has encountered difficulties in obtaining data through penetration experiments. As an alternative, we propose the use of a cyber security risk evaluation method using a Bayesian network (BN) model [9].

A BN is used in this model because it has the advantage of easily modeling complex dependencies and is useful for composing a model that uses prior information, posterior information, and backpropagation calculation [10]. The proposed cyber security risk model with a BN consists of two views: architecture and management. The target system for cyber security risk evaluation is the nuclear reactor protection system (RPS) of a nuclear research reactor, which is a safety-critical I&C system.

In this study, we propose a methodology for constructing an event tree for the cyber security risk evaluation of a nuclear I&C system. Event tree analysis is the most popular methodology used in probabilistic safety assessment (PSA) [11]. Although PSA is the most popular analysis methodology, it has not yet been used to consider cyber security. However, PSA models can be used effectively by implementing a BN model to evaluate the effects of cyber attacks [12]. The proposed method will provide insight into safety and cyber risks for a given facility.

We explain two methodologies, BN and PSA, in Section 2. Section 3 describes the cyber security risk evaluation for an RPS. We describe the BN cyber security risk evaluation model for an RPS and propose a method for applying the BN cyber security risk evaluation model to an event tree model.

2. Methodology

Nuclear facilities have a SCADA system that is separated from outside systems, and used to control and monitor measurement data from the I&C system. Although the SCADA system is separated from the outside, cyber attacks occur in nuclear facilities such as nuclear power plants and centrifugation facilities that enrich uranium. The nuclear field is not exempted from cyber attacks, as shown by the Stuxnet incident in Iran [1,13]. Nevertheless, research into cyber security at nuclear facilities is still at an early stage, as it is difficult for nuclear facilities to obtain data through penetration tests.

Section 2.1 explains the RPS as a target system. Section 2.2 explains the cyber threat for the RPS. In Section 2.3, a BN cyber security evaluation model for nuclear facilities, such as the RPS, is suggested. Section 2.4 shows an event tree for an example when cyber security is considered. Lastly, Section 2.5 suggests a methodology for using the suggested BN cyber security evaluation model, if PSA is used to consider cyber security.

2.1. Reactor protection system

The KINAC regulatory agency published Regulatory Standard 015 (KINAC/RS-015) to enact cyber security regulations in Korea. The KINAC/RS-015 proposes criteria for the application of cyber security as follows [7]: (1) safety related and important to safety; (2) security; (3) emergency preparedness; and (4) others that can adversely affect the above functions.

In nuclear facilities such as nuclear power plants and nuclear research reactors, I&C systems are categorized into safety class and nonsafety class according to their level of safety and available system functions for protecting, controlling, and monitoring the facility. This study focuses on an RPS, one of the safety class systems for cyber security risk evaluation. An RPS guarantees the security of a nuclear facility in the event of an emergency. Generally, an RPS is a critical safety system and is one of the I&C systems that can cause a reactor trip, protecting the core by generating a reactor trip signal to insert a shutdown rod. Concretely, the role of the RPS is to perform security functions in the system while maintaining facility safety in case of an emergency among the facility's various I&C systems. I&C has the role of inserting a shutdown rod into the core to trip the reactor. This happens not only when a reactor shuts down due to regular overhaul, but also when the system recognizes a situation in which the nuclear facility cannot be controlled due to an accident or any other cause.

An RPS consists of three or four channels depending on its function, e.g., nuclear power plant or research reactor, and it performs a logic calculation, e.g., two out of three or two out of four. An RPS in a single channel is composed of a bistable processor (BP), a coincidence processor (CP), a maintenance and test processor (MTP), and an interface and test processor (ITP) [14]. The BP receives signal information that indicates the status of the nuclear power plant. Among these signals is the reactor trip signal, generated when a nuclear reactor is in an abnormal state. The generated trip signal transmits from the BP to the CP. The CP can receive a trip signal from other channels as well, and it has a role in determining logically whether the trip signal generated from the BP is an error. An MTP is the main human–machine interface of an RPS; it provides a display for the RPS to support operations and transfer information to an information processing system. An ITP monitors the condition of each RPS channel and provides information from the RPS to the postaccident monitoring system. The composition of an RPS for a single-unit research reactor is shown in Fig. 1 [15].

2.2. Cyber threat and mitigation measures for RPS

To develop a cyber security risk evaluation model, four cyber threats and six mitigation measures are defined in the literature for each RPS component, including BP, CP, ITP, MTP, and other channels. Each threat defines a cyber-attack method for

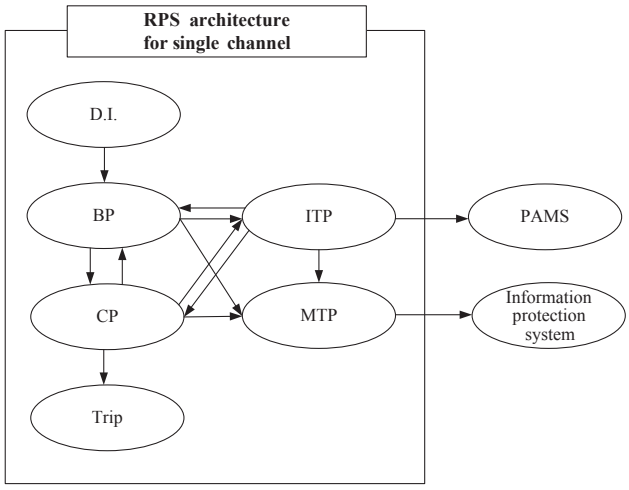

Fig. 1 – RPS single-channel architecture. DI, digital input; BP, bistable processor; CP, coincidence processor; ITP, interface and test processor; MTP, maintenance and test processor; PAMS, postaccident monitoring system; RPS, reactor protection system.

the system, and each mitigation measure is a method of preventing cyber attacks. Cyber attacks on the SCADA system and nuclear facilities still occur. Cyber threats and mitigation measures show the force of cyber attacks on nuclear facilities including SCADA and infrastructure systems [13,16,17]. The list of cyber threats is shown and explained below: (1) virus (T1); (2) Trojan (T2); (3) worm (T3); and (4) denial of service (DoS; T4) [18,19]. A virus is a piece of code that will attach itself to other programs and will run when those other programs are running. A Trojan is a program that adds subversive functionality to an existing program. A worm is a program that propagates itself by attacking other machines and copying itself onto those machines. A DoS is an exploit intended to block someone from using a service, for example, by crashing or hanging a program or the entire system. Table 1 shows the characteristics of these cyber threats.

The available mitigation measures are described in detail below: (1) firewall (M1); (2) online monitoring after regular patching and testing (M2); (3) online monitoring using an existing vaccine (M3); (4) intrusion prevention system (IPS; M4); and (5) intrusion detection system (IDS; M5). Online monitoring can perform a status check of the system using a vaccine and/or a system test. A regular patch regularly upgrades the security program or an operating system to prevent any new cyber threat. A firewall is a technological barrier designed to prevent unauthorized or unwanted communications between computer networks and hosts. Traffic inspection area of a firewall involves only the transport and the network. An IDS detects inbound and outbound network activities and identifies any doubtful patterns. It detects an intrusion, logs the attack, and sends an alert to the administrator. The design policy of an IDS and a firewall are different. The IDS forbids only prohibition rules and the firewall approves only permission rules. The IDS needs to reduce damage from a cyber attack when the firewall cannot prevent this attack. An IPS prevents cyber attacks in real time by preventing intrusion or blocking hazardous traffic. An IPS is a technique to prevent and take action in advance, while an IDS is a technique to detect and take posterior action. The traffic inspection areas of IDS and IPS are application, presentation, session, transport, and network.

The cyber threat of each RPS component is determined by considering its functions. Mitigation measures are then selected based on the characteristics of the determined cyber threat. For example, four mitigation measures can be selected to reduce the influence of a virus on a BP. Fig. 2 shows a firewall, online monitoring after regular patching and testing, online monitoring using an existing vaccine, and an IPS. A firewall blocks a virus by controlling access. Online monitoring after a regular patch can respond to a novel virus and detect an unknown virus. If online monitoring is not upgraded through the use of a regular patch, online monitoring can protect against a virus by using an existing vaccine. If these mitigation measures do not protect against a virus, perhaps because of an insider cyber attack, the system can respond to a virus using an IPS. To prevent the use of a Trojan, the I&C system requires four mitigation measures: a firewall, online monitoring using an existing vaccine, an IDS, and an IPS. The firewall blocks the Trojan by controlling access. The Trojan is detected by online monitoring. If the Trojan passes the firewall, perhaps due to an insider cyber attack, the IDS can detect the cyber cracking and the IPS can respond to the Trojan. To reduce the risk presented by a worm, five mitigation measures can be used to protect the BP, including online monitoring after regular patching and testing, online monitoring using an existing vaccine, an IDS, and an IPS. Before the IPS stage, the operator can take appropriate action by obtaining information on the existence of a worm from the IDS. There are four measures to mitigate a DoS as follows: a firewall, online monitoring using an existing vaccine, an IDS, and an IPS.

Table 1 – Characteristics of viruses, Trojans, worms, and DoS.

	Virus	Trojan	Worm	DoS
Propagation	Possible	Possible (needs other software)	Possible	Impossible
Type	Parasitic/hiding	Independent	Independent	Dependent C&C
Characteristic	Destruction of data and file systems/harmful actions/ disruption	Replication by e-mail or Internet/excessive traffic /abusing network write access	Remote control of infected computers/concealment of symptoms	Bandwidth consumption/ system resource (CPU, memory) depletion

C&C, command and control; CPU, central processing unit; DoS, denial of service.

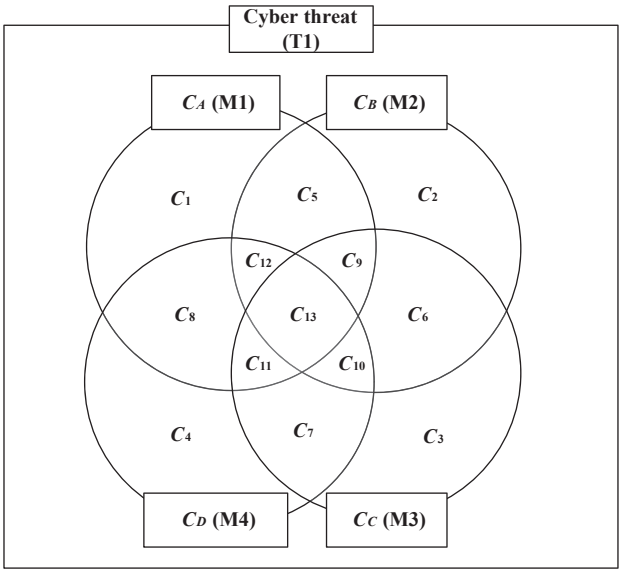

Fig. 2 – Venn diagram example for a cyber threat and related mitigation measures. M1, firewall; M2, online monitoring after regular patching and testing; M3, online monitoring using an existing vaccine; M4, intrusion prevention system; T1, virus.

Applying the classification described above as an example, the relationship between a cyber threat and mitigation measures for a virus can be represented by a Venn diagram, as shown in Fig. 2.

Here, C_X represents coverage by mitigation measure X when a system encounters a cyber threat. In Fig. 2, we have drawn a Venn diagram to represent the relationship between a cyber threat and its mitigation measures, represented by T1, M1, M2, M3, and M4. In C_n, "n" is a number representing coverage by C_X when a system is presented with a cyber threat such as T1. For example, C_1 can cover the cyber threat using only M1. C_{13} can cover the cyber threat with all mitigation measures, M1, M2, M3, and M4.

The Venn diagram can represent Eqs. (1–4) as follows [20]:

$$C_A = (C_1 + C_5 + C_8 + C_9 + C_{11} + C_{12} + C_{13})[1 - f_A] \quad (1)$$

$$C_B = [C_2 + C_6 + C_{10} + (C_5 + C_9 W_{BC} + C_{12} W_{BD} + C_{13} W_{BCD}) f_A][1 - f_B] \quad (2)$$

$$C_C = (C_3 + C_7 + C_{11} f_A + C_6 f_B + C_9 f_A f_B + C_{10} f_B W_{CD} + C_{13} f_A f_B W_{CD})[1 - f_C] \quad (3)$$

$$C_D = (C_4 + C_8 f_A + C_7 f_C + C_{12} f_A f_B + C_{10} f_B f_C + C_{11} f_C f_A + C_{13} f_A f_B f_C)[1 - f_D] \quad (4)$$

Here, f_k is the failure probability of the mitigation measure function, as shown in Fig. 3; w_{nm} represents detection by the mitigation measure "n" among mitigation measures "n" and "m"; and w_{lnm} represents detection by mitigation measure "l" among mitigation measures "l," "n," and "m."

The specific contents of f_k are explained in Section 3.3 with the cyber security risk model using a BN.

2.3. *Cyber security risk evaluation model using a BN*

We have chosen an RPS as an object that has a close relationship with nuclear I&C system security, to develop a cyber security risk evaluation model using a BN, and we have reviewed the validity of the model [21,22]. Our reasons for using a BN are as follows: (1) the ease of modeling complex dependencies; (2) the utility of representing prior and posterior information; and (3) the availability of both quantitative and qualitative information. The cyber security risk model using a BN evaluates the probability of an RPS malfunction caused by a cyber attack (Fig. 4).

The risk model includes an activity–quality model and an architecture model [9]. The activity–quality model evaluates the implementation of cyber security regulation guidelines for a nuclear facility. The architecture model reflects the structural characteristic of an RPS. As a guide to evaluate the activity–quality model, this study refers to cyber security regulation

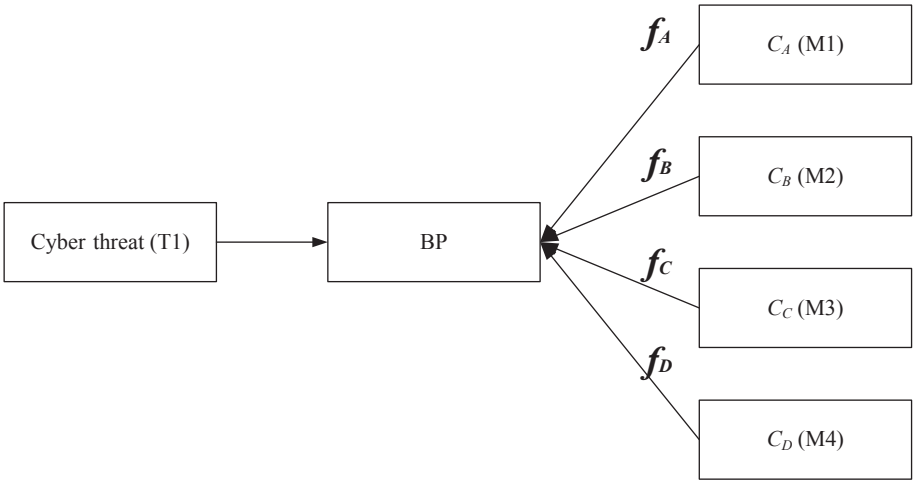

Fig. 3 – The f_k parameters between a cyber threat and its mitigation measures. BP, bistable processor; M1, firewall; M2, online monitoring after regular patching and testing; M3, online monitoring using an existing vaccine; M4, intrusion prevention system; T1, virus.

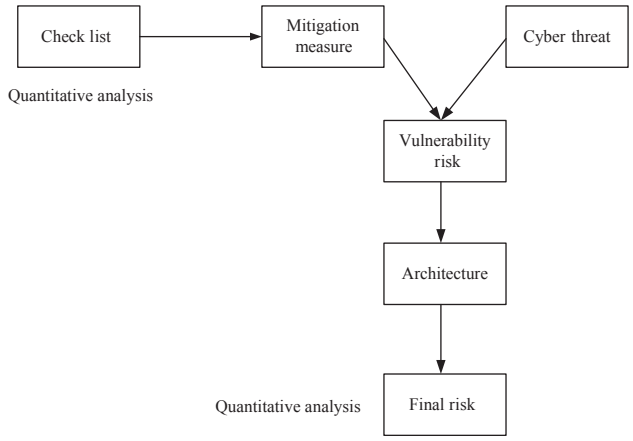

Fig. 4 – Flow chart for a cyber security risk model using a BN. BN, Bayesian network.

guides such as regulatory guide 5.71 [3], which is issued for nuclear facilities. The checklists used are derived by analyzing the regulatory guides and include 34 items [9]. These checklists can be allocated to each phase of the cyber security lifecycle, which comprises the entire cycle of cyber security activity including "establish program," "integrate," "continuously monitor," "review," "change control," and "record." It is possible to systematically evaluate overall activity–quality without an omitted portion by evaluating the checklist in accordance with the cyber security lifecycle. After the checklists are systematized, as mentioned above, they are transformed into the nodes of the BN model. The architecture model consists of BP, CP, ITP, MTP, and other channels, the last of which describes communication with other channels as a single channel for the reflection of architectural characteristics, as shown in Fig. 1. This structure offers a general perspective for the construction of the architecture model. The four cyber threats correspond to each component of the RPS, which are BP, CP, ITP, MTP, and other channels, as well as penetration methods corresponding to the characteristics of each cyber threat. The primary cyber threats of BP, CP, and ITP are viruses and worms. The primary cyber threats of an MTP are viruses, worms, and Trojans, with the consideration that a Trojan hides itself under another software program to run without being detected by the user. A DoS crashes or hangs a program or the entire system, and can occur in a coincidence circuit such as the two-out-of-three logic of the CP. When considering these DoS characteristics, we assume that a DoS can occur at any channel. The number of cyber-threat cases is 10, where the BP has two, CP has two, ITP has two, MTP has three, and other channels has one, as mitigation measures are determined according to cyber threats. The activity–quality model and the architectural model for cyber security are integrated into one BN cyber security risk evaluation model, as shown in Fig. 5.

Nodes in the BN model have five states. In the architecture model, these node states range from "probability of attack occurrence is very low" to "probability of attack occurrence is very high." In the activity–quality model, these node states range from "level of compliance with implementation is very good" to "level of compliance with implementation is very bad." These states are displayed in Table 2.

The BN cyber security risk evaluation model informs the cyber security risk of each variable through a cyber security risk index (CSRI) value, which can be calculated using Eq. (5):

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

Such that weights "w_s" of stages "s" are

$$\sum_{s=1}^{5} w_s = 1 \tag{6}$$

where "s" is a numeric value of the activity–quality checklist node or architecture cyber threat at each stage. These values are presented in Table 1. Here, "w_s" is the weight of the "s" stage, which denotes the sharing of a single node. The value of "w_s" for a single node is 1, aggregating each weight from Stage 1 to Stage 5. Using Eq. (5) in the BN model, it is possible to convert the model from a qualitative evaluation of cyber security to a quantitative evaluation.

The CSRI value for a mitigation measure is used as the value of "f_k" in Eqs. (1–4). For example, in Eq. (1), "f_A" represents the failure probability of the coverage of M1 when T1 occurs at BP, as shown in Fig. 3. To determine "f_A," numeric values of the "virus" node and the "cyber threats for BP" node in Fig. 5 are set such that the weight factor "W_1" of 1 represents hard evidence for assuming that the "probability of attack occurrence" of a virus is "very high." As we want to determine information about the failure probability of the coverage of M1, the other numeric values for all mitigation measures including M2, M3, and M4 are set to a weight factor "W_1" of 1, representing hard evidence for assuming that the "level of compliance with implementation" of mitigation measures is "very bad." The numeric value of M1, like the "firewall" node, is set to weight factor "W_5," where "1" represents hard evidence for assuming that the "level of compliance with implementation" of mitigation measure M1 is "very good." Then, the CSRI for the "BP" node is determined and the CSRI value can be used as the "f_A" parameter.

2.4. *Event tree considering cyber security*

An event tree model is a PSA model. An event tree is composed of an initiating event, a heading, and a branch. In terms of a PSA for a nuclear facility, an initiating event is an incident that requires an automatic or operator-initiated action to bring the plant into a safe and steady-state condition, where in the absence of such an action core damage states of concern can result in severe core damage. The PSA is usually categorized by divisions of internal and external initiators reflecting the origin of the event [23]. Headings are safety systems used to mitigate the initiating event; the branch probability is the success probability of the heading. In terms of cyber security, a cyber threat can be considered an initiating event in an event tree model [12]. Cyber threats such as viruses, Trojans, worms, and DoS are the starting points of cyber attacks. As a heading represents a safety function to mitigate the initiating event in an event tree, when considering cyber security, measures can be considered headings according to the relevant cyber threat. Each cyber threat requires a different mitigation measure. Applying the method described above to

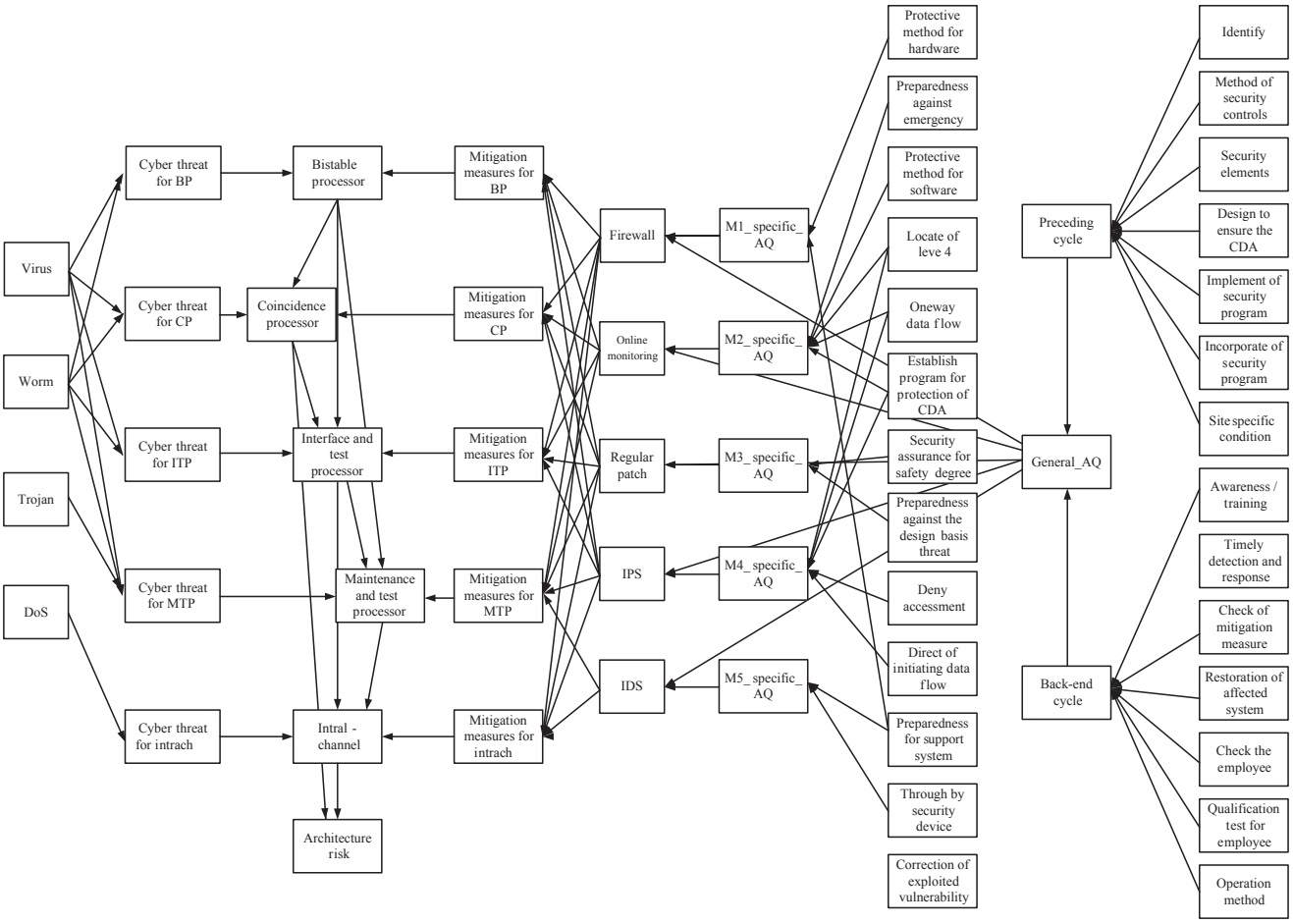

Fig. 5 – BN model for the cyber security risk evaluation of a digital nuclear reactor protection system. BN, Bayesian network; BP, bistable processor; CP, coincidence processor; DoS, denial of service; IDS, intrusion detection system; IPS, intrusion prevention system; MTP, maintenance and test processor.

Table 2 – Numeric value of stages in the architecture and activity–quality models.

Architecture model		Activity–quality model	
Numeric value of stage	Mean (probability of attack occurrence)	Numeric value of stage	Mean (level of compliance with implementation)
5	Very low	5	Very good
4	Low	4	Good
3	Medium	3	So-so
2	High	2	Bad
1	Very high	1	Very bad

generate an event tree reflecting cyber security, the attack of a virus on a BP, as shown in Fig. 3, should be represented as shown in Fig. 6. The cyber security risk model with an event tree, as shown in Fig. 6, can appraise visual analysis information about mitigation measures for each cyber threat using the event tree.

2.5. *Application of analytical results from a BN model to an event tree model*

Generally, the nuclear field has used event trees and fault trees as PSAs. However, it is difficult to use fault trees for cyber security risk evaluation due to certain characteristics of cyber security. To overcome the limitations of using fault trees, we used a BN model. An event tree model is used to apply analytical results from the BN model. The process of creating the event tree model as a PSA model considering cyber security is as follows:

(1) The initiating event is defined as a cyber threat to which a cyber attack can occur.
(2) The heading is defined as a mitigation measure in response to each cyber threat that executes a safety function.

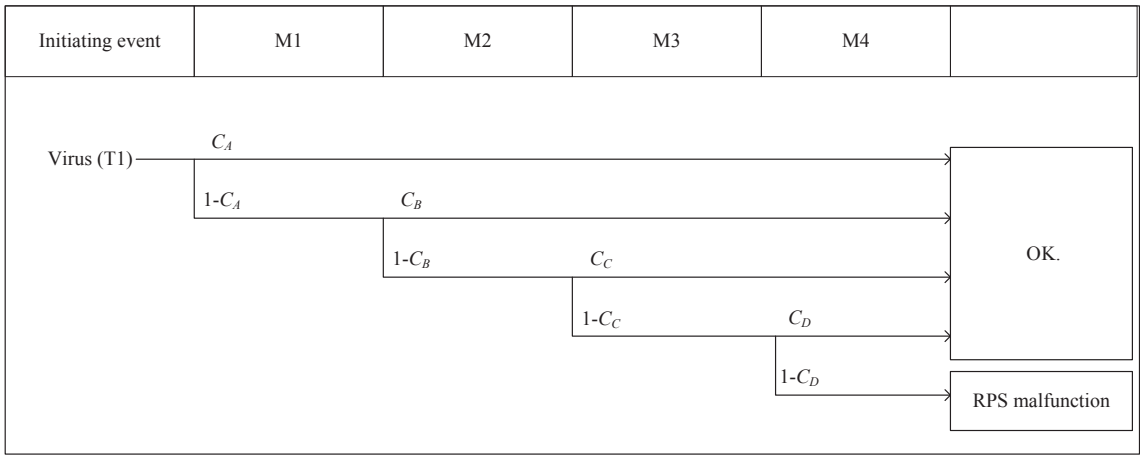

Fig. 6 – Event tree example of cyber security when a virus attacks the BP. BP, bistable processor; M1, firewall; M2, online monitoring after regular patching and testing; M3, online monitoring using an existing vaccine; M4, intrusion prevention system; RPS, reactor protection system.

(3) The input value of the branch probability uses the CSRI value obtained from the BN cyber security risk evaluation model using Eqs. (2–5).
(4) The final RPS malfunction probability is calculated for each initiating event.

Using this methodology, applying cyber security to an event tree allows the use of the BN model mentioned in Section 3.4 and shown in Fig. 6. For a nuclear facility on which a penetration test cannot be conducted, using the quantitative value of CSRI provided by the BN model, one can solve the quantitative value problem and provide useful information on cyber-threat risk using input branch values from the BN model.

3. Discussion

This study proposes a methodology for constructing an event tree for the cyber security risk evaluation of a nuclear I&C system. An event tree is a type of PSA methodology. Generally, in the nuclear field, event trees and fault trees are used as PSAs. However, if the PSA methodology is applied to the cyber security of a nuclear facility for risk evaluation, it is difficult to use a fault tree methodology, which is used for accident-cause analysis. To overcome this limitation, in Section 3.3, this study proposes a cyber security risk model using a BN and CSRI values from this model. The "C_X" is used to apply the proposed methodology with "C_{ij}," "f_k," and "W_{nm}" parameters as in Eqs. (3–5). In Section 3.3, "f_k" is derived from the CSRI of the cyber security risk model using a BN. However, it is difficult to determine the "C_{ij}" and "W_{nm}" parameters in the same manner as the "f_k" parameter, because these parameters depend on the relationship between a cyber threat and the mitigation measure. Instead, these parameters are determined by experimental data. In this study, we describe further experiments to determine the relationship between a cyber threat and a mitigation measure; we propose a methodology for constructing an event tree for the cyber security risk evaluation of a nuclear I&C system.

4. Conclusion

In this study, we propose a cyber security risk model using a BN for an RPS, which is a nuclear I&C system, and a methodology for applying analytical results from a BN model to an event tree model. The nuclear field has previously used event trees and fault trees as PSAs. However, it is difficult to use a fault tree for cyber security risk evaluation due to certain characteristics of cyber security. To overcome the limitations of fault trees, we instead use a BN model.

First, we introduce a cyber security risk model for the evaluation of cyber security using a BN. Our model is composed of an activity–quality model and an architecture model. The activity–quality model analyzes how people and/or organization comply with the cyber security regulatory guides for nuclear facilities. The architecture model analyzes four cyber threats and six mitigation measures according to the architectural characteristics of an RPS. The integrated BN model can be used to evaluate the cyber security risk for the RPS, in terms of activity–quality and architecture, using the CSRI. In the activity–quality and architecture models, the CSRI represents the state of cyber-attack occurrence and the compliance with cyber security regulatory guidelines, respectively, as index values from 10 to 90.

Second, we propose a methodology for applying analytical results from a BN model to an event tree model and show case studies using the suggested methodology. Use of an event tree model for cyber security has several advantages: (1) the event tree model shows visual analysis information on the mitigation measures for each cyber threat; (2) it provides, according to each cyber threat and component of the RPS, sequenced mitigation measures that are systematic and intuitive for the user; and (3) it provides quantitative information on cyber threats and risks based on input branch values from the BN

model. The proposed method is expected to provide insight into safety and cyber security for the facility.

Conflicts of interest

No conflicts of interest.

Acknowledgments

This work was supported by a National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP) (grant number: NRF-2011-0031773).

REFERENCES

[1] B. Miller, D. Rowe, A survey SCADA of and critical infrastructure incidents, Conference on Information Technology Education, Canada, 2012, p. 1–6.
[2] S. Collins, S. McCombie, Stuxnet: the emergence of a new cyber weapon and its implications, J. Policing Intell. Counter Terrorism 7 (2012) 80–91, http://dx.doi.org/10.1080/18335330.2012.653198.
[3] U.S. NRC [Internet], Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010. Available from: http://nrc-stp.ornl.gov/slo/regguide571.pdf.
[4] U.S. NRC [Internet], Regulatory Guide 1.152, Revision 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, 2006. Available from: http://pbadupws.nrc.gov/docs/ML0530/ML053070150.pdf.
[5] U.S. NRC [Internet], Regulatory Guide 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, 2011. Available from: http://pbadupws.nrc.gov/docs/ML1028/ML102870022.pdf.
[6] IEEE, IEEE Std 7–4.3.2-2010—IEEE standard criteria for digital computers in safety systems of nuclear power generating stations, 2010. http://dx.doi:10.1109/IEEESTD.2010.5542302.
[7] Korea Institute of Nuclear Safety, KINAC/RS-015, Regulatory Standard on Cyber Security for Computer and Information System of Nuclear Facilities, 2014.
[8] J.G. Song, J.W. Lee, C.K. Lee, K.C. Kwon, D.Y. Lee, A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nucl. Eng. Technol 44 (2012) 919–928, http://dx.doi.org/10.5516/NET.04.2011.065.
[9] J. Shin, H. Son, R. Khalil, G. Heo, Development of a cyber security risk model using Bayesian networks, Reliab. Eng. Syst. Saf 134 (2015) 208–217.
[10] J.M. Bernardo, Reference posterior distributions for Bayesian inference, J. R. Stat. Soc. Ser. B (Methodol.) 41 (1979) 113–147.
[11] C.K. Park, J. Ha, Probabilistic Safety Assessment, Brain Korea, Seoul, 2003.
[12] J. Shin, G. Heo, H.G. Kang, H. Son, Methodology for applying cyber security risk evaluation form BN model to PSA model, International Symposium on Future I&C for Nuclear Power Plants (ISOFIC), Jeju, Republic of Korea, August 24–28, 2014.
[13] B. Kesler, The vulnerability of nuclear facilities to cyber attack, Strategic Insights 10 (2011) 15–25.
[14] D.Y. Lee, J.G. Choi, J. Lyou, A safety assessment methodology for a digital reactor protection system, Int. J. Control Autom. Syst. 4 (2006) 105–112.
[15] G.Y. Park, S.H. Bae, D.I. Bang, T.G. Kim, J.K. Park, Y.K. Kim, Design of instrumentation and control system for research reactors, 11th International Conference on Control, Automation and Systems, Gyeonggi-do, Republic of Korea, October 26–29, 2011, p. 1728–1731.
[16] Z. Bonnie, A. Joseph, S. Sastry, A taxonomy of cyber attacks on SCADA systems, Internet of things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, IEEE, 2011.
[17] W. Gao, T. Morris, B. Reaves, On SCADA control system command and response injection and intrusion detection, eCrime Researchers Summit (eCrime), IEEE, 2010.
[18] S. Hobbs [Internet]. Cyber Threats: Viruses, Worms, Trojans, and DoS Attacks, Global Information Assurance Certification Paper, SANS Institute, December, 2000. Available from: https://www.giac.org/paper/gsec/300/cyber-threats-viruses-worms-trojans-dos-attacks/100898.
[19] M. Karresand, Separating Trojan horses, viruses, and worms—a proposed taxonomy of software weapons, Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, 2003.
[20] B.G. Kim, H.G. Kang, H.E. Kim, S.J. Lee, P.H. Seong, Reliability modeling of digital component in plant protection system with various fault-tolerant techniques, Nucl. Eng. Des. 265 (2013) 1005–1015.
[21] J. Shin, H. Son, G. Heo, Cyber security risk analysis model composed with activity-quality and architecture model, International Conference on Computer, Networks and Communication Engineering, Beijing, China, May 23–24, 2013, p. 609–612.
[22] J. Shin, H. Son, G. Heo, Comparative study of cyber security characteristics for nuclear systems, in: Frontier and Innovation in Future Computing and Communications, Lecture Notes in Electrical Engineering Vol. 301, Springer, 2014, pp. 87–93.
[23] IAEA [Internet]. IAEA-Tecdoc-719, Defining initiating events for purposes of probabilistic safety assessment, 1993. Available from: http://www-pub.iaea.org/MTCD/publications/PDF/te_719_web.pdf.