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/

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,