Contribution ID: **97** Type: **Oral Presentation**

Methodology on Cyber Security for Digital I&C system in Research Reactors

Wednesday 18 November 2015 17:30 (20 minutes)

Cyber security has become one of major issues in nuclear field both commercial power plants and research reactors. For cyber security in nuclear field, the regulatory agencies in the world published a lot of guidance. It is necessary to evaluate cyber security considering the conformance with these regulatory guides. In this study, we introduce the cyber security risk evaluation model with Bayesian network (BN) for cyber security of digital instrumentation and control (I&C) system in particularly, research reactors. We propose the methodology of making the event tree which is one of tools for probabilistic safety assessment (PSA) for risk management.

Our first sample system was the nuclear reactor protection system (RPS), one of the safety-critical systems, for cyber security risk evaluation. The BN has an advantage of easily modeling complex dependencies, and being useful for composing the model which uses prior information and posterior information, and back propagation calculation. The BN is used for vulnerability study of cyber security, for which it is difficult to perform the penetration test. For a nuclear facility which a penetration test cannot be conducted in reality, the quantitative value provided by the BN model can address cyber security in research reactor with quantitative manner. The proposed cyber security risk evaluation model consists of two views: the activity-quality model and the architecture model. The activity-quality model analyses how people and/or organization comply with the cyber security regulatory guides for nuclear facilities. Meanwhile, the architecture model analyses vulnerabilities and mitigation measures according to architectural characteristics of RPS on the basis of the BN. The integrated BN model can be used to evaluate comprehensive cyber security risk for RPS. Furthermore, it informs the useful information about vulnerability risk by using input branch values in the event tree model. Though the node probability tables were decided by expert judgment as prior information, we will perform Bayesian update to get posterior information for using true data by experiment test to make more robust the model.

The conventional PSA model does not consider the cyber security yet. However, it is expected to cover the effects of cyber-attacks in risk management. In order to achieve this technical goal, we tried to use event tree models, which enables to represent the cause-consequence relationships between vulnerabilities and mitigation measures of an I&C system. In terms of cyber security, vulnerability can be considered as an initiating event in an event tree model since the vulnerabilities are the starting point of cyber-attack. The input value of the branch probability in the event tree model was referred from the analysis results obtained from the BN cyber security risk evaluation model. The event tree model is also able to show the visual information about the mitigation measures for each vulnerability with prior information, posterior information, and back propagation calculation. Furthermore, it informs the quantitative information about vulnerability risk based on the input branch value from the BN model. After Bayesian update for the BN model with experimental data, it provides the vulnerable route on target architecture by evaluating the cyber security risk instead of penetrate test.

The cyber security risk evaluation model can substitute for enormous penetration test on nuclear facility by evaluation the vulnerability against cyber-attack and providing information that which route or point has more vulnerable than others. It can be used to prepare the cyber security analysis report for regulatory authority.

Organization

Kyung Hee University

Country

Republic of Korea

Author: Mr SHIN, Jinsoo (Kyung Hee University)

Co-authors: Prof. HEO, Gyunyoung (Kyung Hee University); Prof. SON, Hanseong (Joongbu University); Dr SUH, SangMoon (Korea Atomic Energy Research Institute)

Presenter: Prof. HEO, Gyunyoung (Kyung Hee University)

Session Classification: Security of Research Reactors

Track Classification: Security of Research Reactors