Development of a Demonstrable Nuclear Cyber Security Test-Bed and Application Plans

Chanyoung Lee [a], Cheol Kwon Lee [b], Jong Gyun Choi [b], Poong Hyun Seong [a*]
[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, Republic of Korea*
[b] *Nuclear ICT Research Division, Korea Atomic Energy Research Institute, 1045 Daedeok-daero, Yueseong-gu, Daejeon 34057, Republic of Korea*
[*] *Corresponding author: phseong@kaist.ac.kr*

1. Introduction

The introduction of digital technology to NPPs led to the reliable, efficient, and intelligent nuclear digital I&C systems, but new issues such as cyber security have emerged in the nuclear industry. In order to address the cyber security issue, regulatory organizations developed cyber security regulatory requirements such as RG 5.71 [1], RS-015 [2] and published a number of guidance to help nuclear utilities meet the regulatory requirements. In addition, many methods for enhancing cyber security of NPPs and evaluating cyber risk have been proposed in the nuclear research community. However, there are few studies that proved their obtained results through conducting cyber-attack experiments. It is because that conducting cyber-attack experiments on actual plants is impossible and developing an experimental platform that simulating complicated nuclear digital I&C systems requires considerable effort and cost.

Even though, conducting cyber-attack experiments and demonstrating their impact on systems are essential to assess cyber risk of NPPs and to evaluate cyber security systems. For this reason, a testbed that can be used for proving results obtained from cyber security researches is necessary in the nuclear research community.

In the nuclear industry, many experimental simulators such as various types of CNS (Compact Nuclear Simulator) were developed. However, the existing simulators have following limitations for conducting cyber security researches.

- They cannot implement cyber-attack scenarios.
- They cannot survive or provide results of the effects arising from simulated cyber-attacks.
- They cannot capture the data needed for security forensics and analysis.

In order to support practical nuclear cyber security researches and to address the mentioned limitations, a new type of applicable and demonstrable test-bed has been developed in this study.

2. Design Concepts of a Test-Bed

In the industry of CPS (Cyber Physical System), a key challenge to progress in CPS is the lack of robust platforms for experiment and testing, which is NIST (National Institute of Standards and Technology) is addressing. The NIST suggested general design principles useful to all CPS testbed developers [3]. According to the design principles, an experimental platform should be integrative, reconfigurable, reproducible, scalable, and usable in multi-domains. In this study, based on the suggested design principles, three design concepts have been suggested for applicable and demonstrable test-bed in the nuclear cyber security research.

First, a test-bed must include both of software driven plant simulators and physically configured devices. Synchronizing plant simulators with physical devices allows simultaneous and multiple interpretation range from malicious actions performed on control equipment to impact on the plant safety.

Second, interface modules between plant simulator and physical devices must be flexible enough to be changed according to the experiment purpose and targeted systems. The interface modules connecting simulators and physical devices should be interchangeable, which allows a test-bed to enable rapid reconfiguration for various experiments and specific domain applications.

As the last design concept, a test-bed should be designed to cooperate with other test-beds which are differently configured or placed remote locations to analyze the impact of multiple cyber attacks on various types of devices.

Using a test-bed based on the suggested design concepts, several research activities such as developing an experimental design and test method, running an experiment or test, monitoring testbed functionality, and analyzing data from testbed are possible.

3. Development of a Test-Bed

3.1 Test-Bed Description

The test-bed developed in this study consists of a plant simulator, a physical control system, and an interface module.

In order to implement plant simulations, the hypothetical plant model "*Asherah*", designed based on several existing pressurized water reactor (PWR) plants by the IAEA coordinated research project [4], was modelled by the *MATLAB/Simulink* program. In addition, a physical water level control system is constructed and synchronized with the hypothetical plant model "*Asherah*" through the data interface

module. The interface module sends the measured water level value to the plant simulator and changes the water level according to the state of the plant simulator. When conducting cyber attack experiments using the developed test-bed, the physically constructed level control system can be a pressurizer level control system or a steam generator level control system, or a condensate level control system depending on the function design of applied data interface modules.

3.2 Test-Bed Configuration

The configuration of the test-bed developed in this study is shown in Fig. 1. The physical system is controlled by programmable logic controller (PLC). An engineering work station (EWS) is connected with PLC to download and upload software codes. Human machine interface (HMI) provides controller screen and displays process variables and equipment operating status, whose communication protocol is *Profibus* that is *Siemens's* standard communication protocol. Then PLC communicates with *MATLAB/Simulink* model of the hypothetical plant and other clients through a switch. In order to corporate with other test-beds, the open platform communication unified architecture (OPC UA) protocol is applied as communication protocol between or among clients.

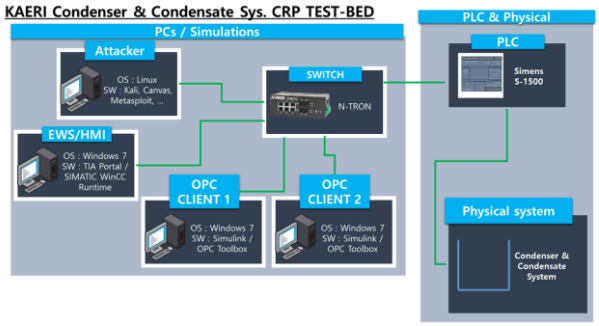

Fig. 1. Configuration of Cyber Security Experimental Platform

4. Application Plans of the Developed Test-Bed

Various cyber security studies such as developing methodologies to identify malfunctioning control operations and to determine the impact on the plant safety and impact propagation vectors are being conducted to improve the ability to respond to cyber attacks. When it comes to responding to cyber attacks, impact analysis is crucial and the analysis performance can be enhanced by conducting cyber-attack experiments on demonstrable simulators. The test-bed developed in this study can be used to enhance the cyber incident analysis performance by supporting the multiple analysis from impact on equipment to impact on facilities.

Cyber security systems deployed in nuclear I&C systems should not only detect cyber attacks, but also isolate damages, and preserve the integrity of the data for future incident analysis. However, the effectiveness of commercial cyber security systems may be uncertain when they are applied to nuclear I&C system. The test bed developed in this study is flexible enough to contain cyber security systems so that it can be used to determine cyber security systems that can be applied to nuclear I&C systems.

According to RG 5.71, the cyber security incident response team (CSIRT) should be organized and trained periodically. Training program to mitigate damages from cyber attacks can supports assessment of cyber attack induced situation, complicated and comprehensive, and is as important as existing safety related training programs. Testbed developed in this study can support the training programs by simulating cyber attack induced events. In addition, it can help to develop test cases or cyber attack scenarios.

5. Conclusion

In order to support practical nuclear cyber security researches, a new type of applicable and demonstrable test-bed has been developed in this study and address the limitations of the existing nuclear simulators. Based on the suggested design principles by NIST, three design concepts have been suggested. A test-bed must include both of software driven plant simulators and physically configured devices, and interface modules between plant simulator and physical devices must be flexible enough to be used in multi-domain. In addition, a test-bed should be designed to cooperate with other test-beds. Based on the suggested design concepts, a physical water level control system is constructed and synchronized with the hypothetical plant "*Asherah*" through the data interface module. There are several application plans of the developed test-bed. The test-bed allows for research analyzing the impact of cyber attacks on NPPs and can be used to evaluate the effectiveness of applied cyber security systems. In addition, it can support the training programs by simulating cyber attack induced events.

ACKNOWLEDGEMENTS

This work was supported by the Development of Cyber Security Test and Validation Technology for Nuclear I&C System of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Trade, Industry and Energy.

(No. 20171510102100)

REFERENCES

[1] US Nuclear Regulatory Commission. "Regulatory Guide 5.71." Cyber Security Programs for Nuclear Facilities, Washington, DC, 2010.
[2] KINAC, KINAC. "RS-015." Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities, 2014.
[3] Kellerman, Christina. "Cyber-Physical Systems Testbed Design Concepts.", 2016.
[4] IAEA CRP J02008: Enhancing Computer Security Incident Analysis and Response Planning at Nuclear Facilities.