Development of Cyber Security Test Technology for Nuclear I&C System

Jong Gyun Choi, Jae Gu Song, Jun Young Son, Dong Young Lee, Jung Woon Lee, Cheol Kwon Lee
Korea Atomic Energy Research Institute, 989-111, Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Korea
**Corresponding author: choijg@kaeri.re.kr*

1. Introduction

In the various nuclear facilities such as nuclear power plants, research reactors, nuclear fuel fabrication facility and radioactive waste treatment facility, digital technologies such as computers and communication networks began to be applied to nuclear instrumentation and control systems, which are responsible for the safe operation of nuclear facilities, by acquiring, analyzing, processing and controlling various data from/to field devices and equipment.

As the instrumentation and control system is digitized, cyber security has become an important issue because there were various cyber-attacks on nuclear facilities over the last decade. In 2003, a slammer worm penetrated a private computer network at the Davies-Besse nuclear plant in Ohio and disabled a safety monitoring systems for nearly five hours [1]. In 2008 Unit 2 of the Hatch nuclear power plant automatically shut down after an engineer applied a software update to a computer on the plant's business network [2]. In particular, after Stuxnet computer worm struck the Iranian nuclear facility in 2010 to cause the failure of its uranium centrifuges and shut down its operations, cyber security measures have been required not only for nuclear facilities, but also for major national infrastructures [3].

In order to respond to cyber threats to nuclear facilities such as commercial nuclear power plants and research reactors, the following cyber security should be strengthened.

- Cyber threat information collection, analysis, response and management
- Security threat analysis and prevention
- Response and recovery technology in case of cyber incident
- Cyber security education and training

2. Research Goals and Contents

The goal of this research is to establish a cyber attack response system that can be applied to nuclear facilities. By establishing a cyber attack response system that can be useful commonly to nuclear facilities in our country, this research is to prepare for new types of cyber threats emerging by advancement in cyber technologies, to secure technologies responsive to potential cyber attacks against the nuclear facilities, to develop a training facility for personnel working in the nuclear facilities, and to maintain a cooperative system for cyber threat response among national critical infrastructures.

As shown in Figure 1, in the first step, a test bed for cyber security test and analysis was built. The test-bed was made of the same hardware and software as the instrumentation and control equipment applied to the APR1400 nuclear power plant so that the cyber security incident analysis or vulnerability analysis results through this test bed can be practical and applied to recommend the design complements.

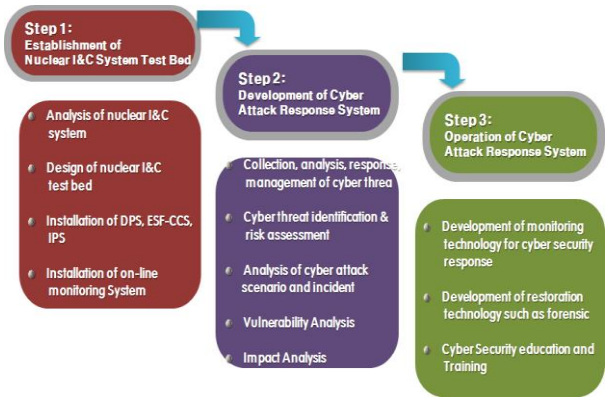

Figure 1. The stage of the research

In the second step, cyber threat information that can occur in nuclear facilities is collected and analyzed. Cyber-attack scenarios are constructed in nuclear facilities, and cyber attack tests are performed directly on the test bed to identify cyber security vulnerabilities and provide countermeasures.

In the third step, monitoring and restoration technology is developed. Education and training programs for cyber security are developed.

3. Research Results

3.1 Establishment of nuclear I&C system test-beds

As shown in Figure 2 and Figure 3, the I&C system test-bed based on Shin-hanul unit 1&2 was designed and developed. This test bed includes IPS (Information Processing System), ESF-CCS (Engineering Safety Features Component Control System) and DPS (Diverse

Protection System), which are representative instrumentation and control systems of nuclear power plants. The hardware and software of the test bed is identical to that of the system applied to Shin-hanul unit 1&2, but the scale was reduced. In addition, a recording and monitoring equipment capable of storing and analyzing the data transmitted and received between the systems was connected with the test bed to understand the operation status of the systems during vulnerability test such as penetration test.

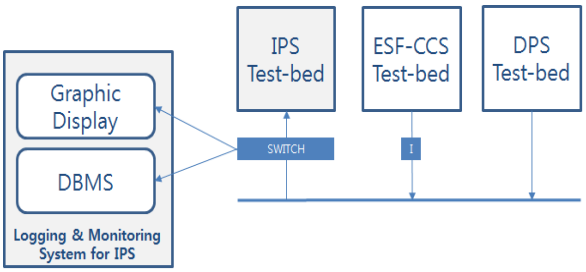

Figure 2. Schematic Diagram of Test-Bed

Figure 3. Test-Bed of Nuclear I&C System

3.2 Analysis of simulated cyber incidents

The following simulated cyber incidents were analyzed through the test bed.

(1) Control logic attack and countermeasure analysis through modulation of engineering software
- Analyze modulation scenario of engineering software
- Analyze engineering software serial communication spoofing through DLL injection attack
- Analyze engineering software program communication port modulation possibility through DLL injection attack
- Analyze monitoring data corruption through serial communication spoofing

(2) Development of IPS penetration test and procedure using a commercial offensive PT tool
- Get latest vulnerability list and analysis list for IPS test bed
- Classify the exploitable list and analyze countermeasure through penetration test

(3) Simulated incident analysis and testing of IPS
- Analyze vulnerability through network packet collection and analysis of IPS
- Analyze 143 vulnerability test items for IPS
- Perform vulnerability analysis of gateway server

3.3 Device-wise, system-wise test and impact analysis

The following security tests were performed at the equipment level for the safety grade control devices applied to the instrumentation and control system of the nuclear power plant.

(1) Analyze authentication vulnerability of logic control device
(2) Perform security test of QNX operating system

3.4 Others

We have developed cyber security education programs and demonstration kits to raise awareness of cyber security, and have participated in international joint research projects such as IAEA CRP and PCG to promote cyber security international cooperation.

4. Conclusion

A cyber attack response system should be established and operated to safely protect nuclear facilities from cyber threats that are continuously increasing and becoming more intelligent. This research has begun to establish this response system, and step 2 is underway. The test bed constructed through this research is used jointly with national security research institutes such as NSR and ETRI for research on cyber attack response and countermeasures.

In the future, we expect that it will be possible to support cyber incident response by continuing this research against intelligent and persistent cyber attack and by sharing the cyber threat information with national cyber security related organizations.

REFERENCES

[1] Guan J, Graham J, Hieb J., A digraph model for risk identification and management in SCADA systems, 2011 IEEE international conference on intelligence and security informatics (ISI), IEEE CP., 2011, p. 150–5.
[2] Brain Krebs, Cyber Incident Blamed for Nuclear Power Plant Shutdown, Washington Post, June 5, 2008.
[3] Miller B, Rowe D., A survey SCADA of and critical infrastructure incidents, Proceedings of the 1st annual conference on research in information technology, ACM; 2012.