

Development of an NPP Cyber Security Test Bed: 1st Phase Development Case

In Hyo Lee*

Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Daejeon, Republic of Korea 34101

*Corresponding author: lih9103@kinac.re.kr

1. Introduction

Industrial and control (I&C) systems in old NPPs were changed from analog to digital due to the discontinuation of components. Furthermore, the latest NPP, such as Shin-Hanul units 1&2, is fully digitalized [1]. The digital I&C system is convenient for maintenance; however, vulnerable to cyber-attacks. Also, cyber-attacks have characteristics that evolve as time goes on, so cyber security has become an essential issue in the nuclear field.

Penetration test on digital I&C systems is an effective way to evaluate cyber security and vulnerabilities of the digital I&C system [2]; however, penetration test on actual digital I&C systems of NPPs is almost impossible due to safety concerns. Therefore, an NPP test bed is necessary to analyze vulnerabilities and assess the cyber security of NPPs.

KINAC has been developing an NPP test bed with the goal of completion in two years. The 1st phase of test-bed development was finished at the end of 2022, and the full-scope test bed will be developed at the end of 2023. This paper describes the 1st phase of the test bed development case.

2. NPP Cyber Security Test-bed

The main objectives of the NPP test bed are analyzing vulnerabilities of digital I&C systems and assessing of cyber security of NPPs as described above. The vulnerability analysis is in a microscopic manner, and the cyber security assessment is macroscopic; the test bed is required for this micro-macro study. For this reason, KINAC designed a hardware-in-the-loop (HIL) test bed for physical and digital I&C systems, and an NPP simulator is connected.

The NPP test bed consists of three main parts, as shown in Fig. 1: ① NPP simulator, ② digital controller, and ③ remote input-output (RIO) system.

The NPP simulator simulates behaviors of NPP, such as reactor physics, thermodynamics, and system dynamics. The APR-1400 reactor was used as a reference power plant.

Physical digital I&C systems are required to perform vulnerability assessments and pen-tests, so digital I&C systems used in NPP sites, such as POSAFE-Q programmable logic controller (PLC) and OPERA distributed control system (DCS), were built.

Because the NPP simulator was not designed to communicate with I&C systems but to emulate the I&C systems, more components are necessary to link the NPP simulator with digital I&C systems. The RIO system provides that function.

3. Integration Performance Test of HIL System

3.1 Scenario for Integration Performance Test

An integration performance test should be performed since different systems were integrated by redesigning the initial design. For the integration performance test, a simple scenario simulating a pressurizer (PZR) pressure decrease situation was developed due to forced manipulation of variables. In this scenario, all PZR heaters are failed, and sprays are opened because of the forced manipulation. Then, PZR pressure decreases, and the reactor is tripped. After that, PZR pressure continues to decrease, and the safety injection actuation signal (SIAS) is generated when PZR pressure drops below the setpoint. Under normal conditions, SI pumps will start; however, a SI pump fails to run because the variables were manipulated.

3.2 I/O Variables Mapping and Logic Modification

The PZR pressure control system (PPCS) and engineered safety features-component control system (ESF-CCS) are implemented in DCS and PLC hardware separately to demonstrate the scenario. After that, I/O variables of PPCS and ESF-CCS and simulator tags mapping were conducted to link with the simulator.

3.3 Integration Performance Test Results

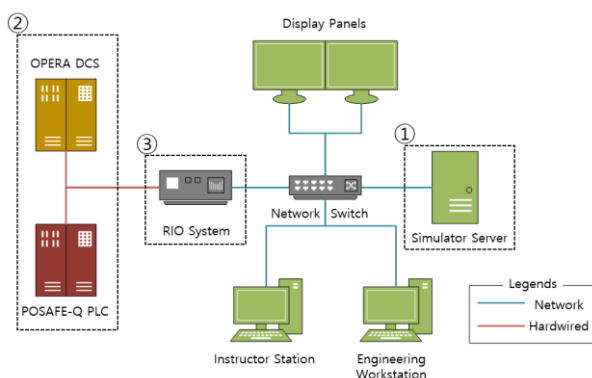


Fig. 1. Simple Configuration of Test-bed

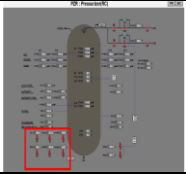
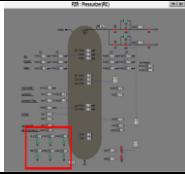
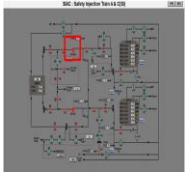
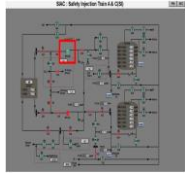
The integration performance test was performed to test whether the HIL system works as designed. Before the test, variables of PPCS and ESF-CCS components are forced manipulated in DCS and PLC, respectively. The examples are shown in Table I.

Table I: Examples of Variables Setting

Variables Status	Heater A1 ON	Heater A1 OFF
Original Variable Status	False	False
Manipulated Variable Status	False	True

When the simulator is synchronized with DCS and PLC, the components of PZR and SI are worked as designed in the test scenario, as shown in Table. II.

Table II: Comparisons Table of Components Status

Conditions Components	Original Variable	Manipulated Variable
PZR Heater		
SI Pump		

4. Conclusions and Future Works

The HIL test bed was developed to establish an environment for cyber security tests, and different types of systems were interfaced, such as a software-based NPP simulator and hardware-based digital I&C systems. It is verified that these systems work organically by conducting the integration performance test using a test scenario. This shows the possibility that compromised digital I&C systems may affect NPP behaviors.

Suppose other digital I&C systems are connected to the NPP simulator; an advanced cyber security test environment is expected to be established. This advanced cyber security test-bed will make vulnerability analysis, pen tests, and cyber security assessment possible. To do this, KINAC plans to develop the full-scope cyber security test bed by the end of this year.

REFERENCES

- [1] Seo-ryong Koo and Kook-hun Kim, Project Experience of MMIS for Shin-Hanul units 1&2 (Component Design, Manufacturing and Testing), Transactions of the Korean Nuclear Society Autumn Meeting, Oct.29-30, 2015
- [2] Vijay Kumar Velu, Mobile Application Penetration Testing, Packt Publishing, Birmingham, pp.13, 2016.