Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 25-26, 2012

Development of Test Platform for Digital I&C System Evaluation

Young-Mi Kim and Yong-Il Kwon

Korea Institute of Nuclear Safety, P.O.Box 114, Yuseong-gu, Daejeon, Korea, 305-600
Corresponding author: ymkim@kins.re.kr

1. Introduction

Nuclear I&C (Instrument & Control) systems which need safety-critical function have adopted various control units and communication protocols. These trends have been enlarged new nuclear plants design and upgrading of operating plants. Applying to these digital technologies to nuclear power plants has many good advantages, such as upgrade of functionality and performance and improvement of efficiency and economics. But, it also has several flaws. System designs have been more complicated and software reliability analysis and risk analysis have been more difficult. Also, cyber security problems came to the fore as I&C systems are connected through networks. The vulnerabilities of computer systems are vital to nuclear safety. Coping with the new IT technology of new and operating power plants, it is necessary to analyze verification technology and obtain regulatory technology through establishment of test platform. This paper presents test platform for digital I&C system evaluation of NPP.

2. Research Background

Fig. 1 shows the several new regulatory issues of nuclear digital I&C system. Cyber security, CPLD/FPGA, wireless communication and smart transmitter are representative.

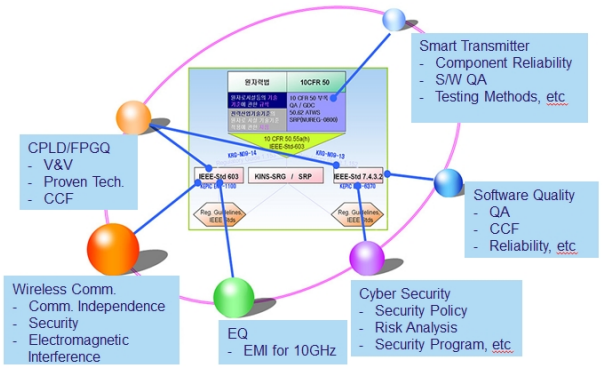

Fig. 1 New Regulatory Issues of Nuclear I&C System

2.1 Cyber Security

The objective of cyber security is to prevent unauthorized accesses to information, software and data for the prevention of an accident, an unsafe situation or plant performance degradation. Nuclear digital I&C systems must be protected against malicious acts.

We can group malicious acts as follows [1]:

- Information gathering attacks aimed at planning and executing further malicious acts;
- Attacks disabling or compromising the attributes of one or several computers crucial to facility security or safety;
- Compromise of one or several computers combined with other concurrent modes of attack, such as physical intrusion to target locations.

In accordance with KINS RG 8.22, a licensee must provide cyber security program and plan to KINS that digital I&C systems are adequately protected against cyber attacks[2,3]. Fig. 2 shows a example of test environment for mock cyber attacks.

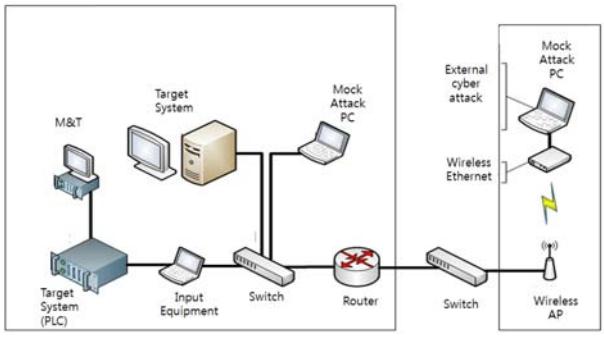

Fig. 2 Example of test environment for mock attack

2.2 CPLD/FPGA

Use of Field-programmable gate arrays (FPGAs) is increasing in safety nuclear I&C systems. FPGAs have been widely applied in other industries, but they are still new to the nuclear industry, particularly for safety application. In Shin-Kori 3&4, Component Interface Modules(CIMs) which were implemented using FPGA were used for safety critical component control. CIM module receives component control signals from the safety system and from the diverse non-safety based system and arbitrates the signal to the plant component according to a selectable priority. The reliability and

diversity design of the CIM modules are under regulation of KINS.

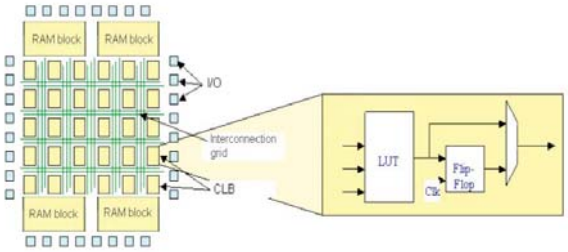

Fig. 3 Typical FPGA Architecture [4]

Fig. 3 shows the typical FPGA Architecture. FPGA-based safety systems need to be developed according to life cycle process and V&V process. The V&V process may be established using IEEE Std 7-4.3.2[5]. FPGA-based regulatory guide have been prepared by KINS.

2.3 Wireless Communication

Wireless Communications are gaining increased attention worldwide for application in many industries. In case of nuclear power plants, many wireless communication-based systems are used in non-safety system, but it is not used in safety systems yet. It is necessary to develop evaluation technology of wireless communication for future regulatory preparedness [6].

2.4 Smart Transmitter

Newly constructed nuclear power plants have adopted smart transmitters even for safety grade system. In case of Shin-Kori unit 3, about 59 safety grade smart transmitters and about 180 non-safety grade smart transmitters are used for measuring various signals. Smart transmitters can use microprocessor with internal memory and software application for internal processing. They can even use communication network for maintaining and monitoring. Software V&V, EQ and cyber security should be evaluated for smart transmitters. It is necessary to develop evaluation technology for smart transmitters.

3. Architecture of Test Platform

Fig. 4 shows a basic architecture of test platform for experimental study. Our platform will be made up of several safety-grade PLCs and equipment for testing and monitoring.

In the first phase, the test platform will be established. Integrated architecture design will be executed and requirements for experimental test will be drawn. Established integrated architecture will be used for the second phase for experimental study and analysis. We expect that regulatory issues such as CPLD/FPGA software verification and cyber security penetration tests are able to be carried out using this test platform.

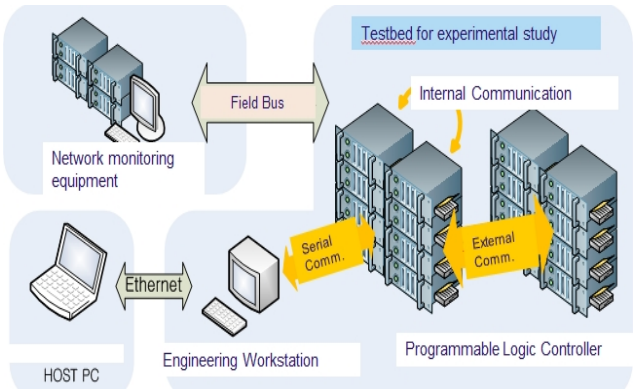

Fig. 4 Test platform for Experimental Study

Third phase, we have plan to develop or revise regulatory guides for new regulatory issues such as CPLD/FPGA and cyber security. We expect that these regulatory guides can be applied to operating plants on a trial basis.

4. Conclusions

Nuclear I&C (Instrument & Control) system which needs safety-critical function has adopted various control units and communication protocols. Coping with the new IT technology of the new and operating power plants, it is necessary to analysis for verification technology and obtaining regulatory technology through establishment of test platform. Using test platform, we will execute CPLD/FPGA verification and cyber security threat analysis, and have plan to revise regulatory guides for regulatory activities. It is expected to obtain efficient and realistic regulatory technology from test platform establishment for nuclear I&C system.

REFERENCES

[1]IAEA Safety Standard Series No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, 2002.
[2]KINS regulatory guide 8.22, Cyber security for nuclear I&C
[3]US NRC regulatory guide 5.71, Cyber security program for nuclear facilities
[4]Guidelines on the use of field programmable gate arrays (FPGAs) in Nuclear Power Plant I&C Systems, 2009.
[5]NUREG/CR-7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems, 2009.
[6]KINS/RR-890, A Study on Evaluation Technique of Wireless Communication System for Digital I&C System, 2011.