A Test Bed for Digital I&C and Cyber Security for NPPs

Yongkyu AN, Calogero SOLLIMA, and Rizwan-uddin
Department of Nuclear, Plasma, and Radiological Engineering
University of Illinois at Urbana-Champaign
216 Talbot Laboratory, 104 South Wright Street, Urbana, IL, 61801
an24@illinois.edu; csollima@illinois.edu; rizwan@illinois.edu

Daniel CHEN, Zbigniew KALBARCZYK, and Tim YARDLEY
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
1308 West Main Street, Urbana, IL, 61801
dchen8@illinois.edu; kalbarcz@illinois.edu; yardley@illinois.edu

William SANDERS
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
306 North Wright Street, Urbana, IL, 61801
whs@illinois.edu

ABSTRACT

In nuclear power plants (NPPs), digital I&C systems are expected to lead to increasing level of safety and improved performance in communication, maintenance, and signal processing. They are expected to be used in all new NPP designs, while existing NPPs are being evaluated for the switch from analog to digital control systems. Switching from analog to digital or working with hybrid systems has posed a bigger challenge than, for example, designing a completely digital control room. The goals of this project are to identify possible faults and to evaluate resiliency of safety-critical digital I&C systems destined for future NPPs [1]. For this purpose, a test bed is being developed which consists of a reactor simulator, a digital controller, and a signal transmitter. A Triple-Modular Redundant (TMR) architecture system is selected as a digital controller for better reliability. A simple real time NPP simulator has been developed in-house in LabVIEW. A data transmitter and an application program provide the communications between the NPP simulator and the TMR controller. Fault injection techniques are applied to the test bed. The test bed is equipped with a set of specialized fault/error injectors to introduce a range of faults/errors, including both transient and permanent. A fault analyzer is also developed. The paper describes the details of the test bed, the associated fault injection system, and some preliminary results of the fault injection studies for digital I&C of NPPs to assess their reliability, tolerance, and resiliency.

Key Words: Cyber Security, Digital I&C, Fault Injection, Nuclear Power Plant, Reliability

1 INTRODUCTION

New control systems based on digital instruments (digital I&C) are being designed for implementation in advanced nuclear power plants (NPPs). With the state of the art technology, better performance and even higher safety levels are expected especially in communication of both detections and responses against either systematic errors or outside trespassing to the system. While new NPP designs are primarily based on digital technology, challenge exists in totally or partially converting existing NPPs from analog to digital controls.

Recent work in this area has generally focused on switching from analog to digital control rooms in NPPs. Huang and Yang reported a critical digital review (CDR) procedure to integrate and replace I&C systems [2]. Suh et al worked on developing an architecture to help upgrade reactor control to digital I&C systems [3]. Jang et al studied human error probabilities for NPPs advanced main control room and assessed its performance using various scenarios to draw statistical data [4].

We here report recent progress of work being carried out in our group in this area [5]. The goal of this work is to establish a test bed for testing NPP digital I&C equipment. The part of the overall project is aimed at identifying possible faults, and to test reliability of digital I&C systems by performing simulation based fault injection methods. The same test bed may also, in the future, be used for assessment of cyber security of digital I&C systems at NPPs.

2 TEST BED CONFIGURATIONS

The test bed is comprised of three main components: a NPP simulator, a Triple-Modular Redundant (TMR) digital controller, and a signal transmitter. LabVIEW has been selected to develop a real time NPP simulator. LabVIEW is also used to program control logic. The basic scheme of the test bed is shown in Figure 1. Details of the configuration have been described in the reference [5].

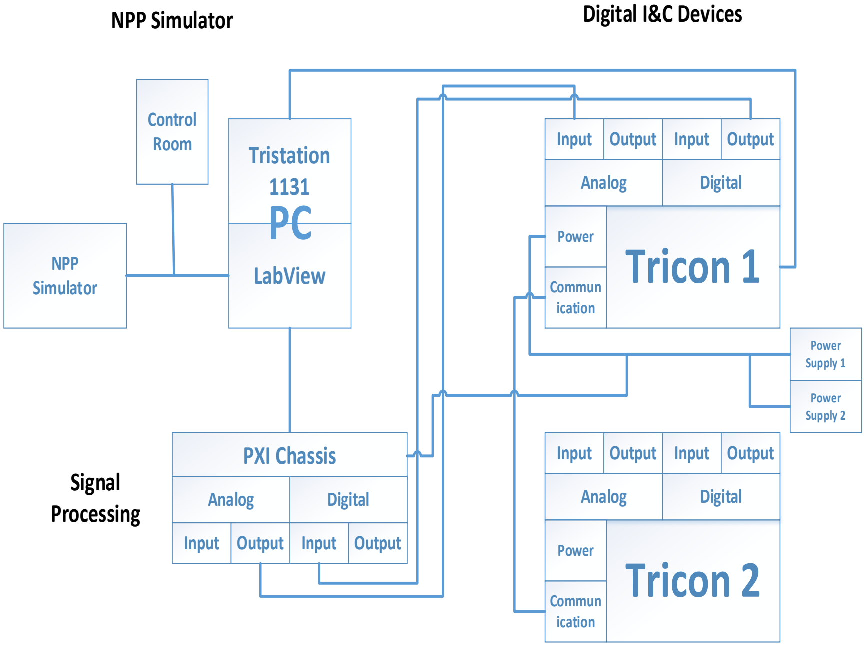

Figure 1. Structure of the test bed [5].

2.1 NPP Simulator (LabVIEW)

The NPP simulator is designed based on the general lay out of a 1000MWe Westinghouse pressurized water reactor (PWR). It simulates the reactor core and related components in real-time. Models for the core, pressurizer, and pump modules were reported in Ref. [5]. Additional components have been added, and they are reported below.

2.1.1 Steam Generator Module

The primary loop of the NPP simulator in LabVIEW is updated by adding a simple model of a steam generator (SG). The controllable variables are primary inlet/outlet temperatures, secondary inlet/outlet temperatures, and pressures in each loop. Energy and mass balance equations are used to model each SG module. The model is given below [6].

$$\dot{Q} = \dot{m}_{PI}\,(h_{PO} - h_{PI}) \tag{1}$$

$$h_{SO} = x * h_{SO,s} + (1-x)\,\mathrm{h}_{SO,w} \tag{2}$$

$$\dot{m}_S = \frac{\dot{Q}}{h_{SI} - h_{SO}} = \frac{\dot{m}_{PI}\,(h_{PO} - h_{PI})}{h_{SI} - h_{SO}} \tag{3}$$

where $\dot{Q}$ is the amount of heat transfer in kW, $\dot{m}_{PI}$ is primary inlet mass flow rate in steam generator in kg/sec, $\dot{m}_S$ is secondary loop mass flow rate in the steam generator in kg/sec, and x is the quality of steam in the steam generator.

2.1.2 Multiple Display Front Panels

The primary loop consists of a core, a pressurizer, four pumps, and four steam generator modules. In order to arrange all indicators and controllers (e.g. thermometers, pressure gauges, knobs, buttons, etc.) for the entire loop, multiple displays (two monitors and a TV screen) are used by splitting the main front panel into three front panels for setting up a model of the simple digital main control room (MCR). A TV screen displays general information of the entire system and the other two monitors are to control the simulator. In this way, operators' observability and controllability may be increased comparing to the single displayed NPP simulator. Figures 2, 3 and 4 show the composition of the simulation front panels.

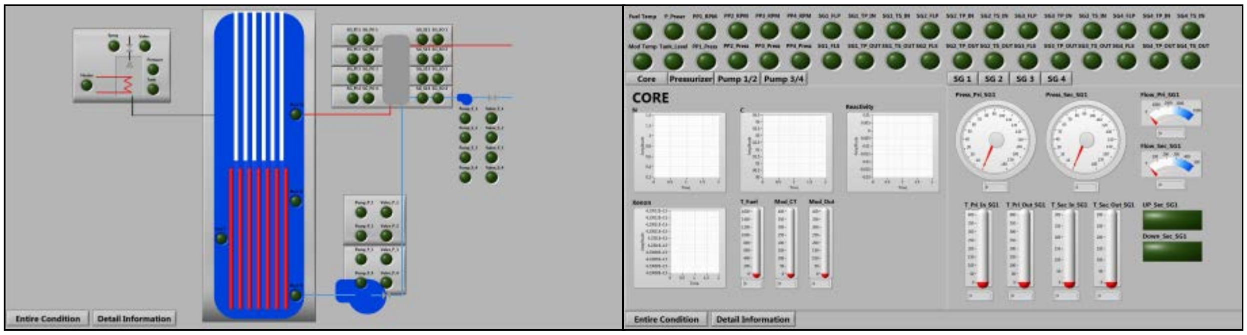

Figure 2. First Front Panel (Indicator Panel).

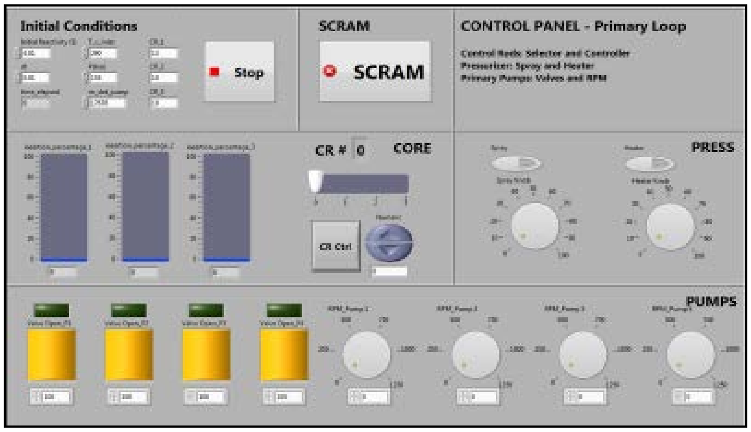
Initial Conditions
Stop
SCRAM
SCRAM
CONTROL PANEL - Primary Loop
Control Rods: Selector and Controller
Pressurizer: Spray and Heater
Primary Pumps: Valves and RPM
CR # 0
CORE
CR Ctrl
PRESS
PUMPS

Figure 3. Second Front Panel (Controlling Panel, Core/Pressurizer/Pump).

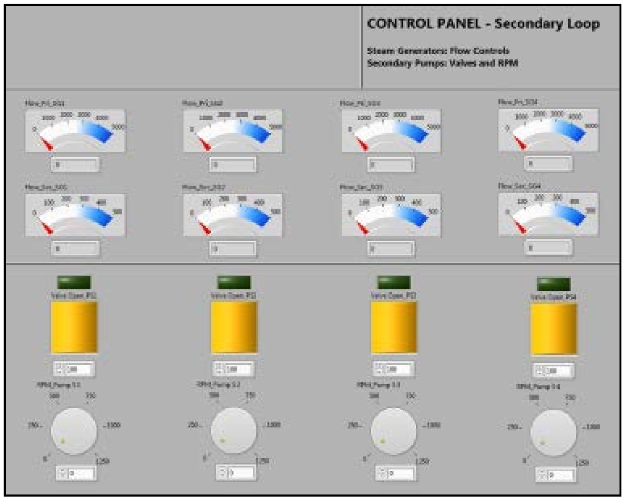
CONTROL PANEL - Secondary Loop
Steam Generators: Flow Controls
Secondary Pumps: Valves and RPM

Figure 4. Third Front Panel (Controlling Panel, Steam Generator/Pump).

3 EXPERIMENTAL FAULT INJECTION SETUP

One of the goals of this project is to carry out a systematic fault injection and error analysis of the combined reactor and control room system, and to assess reliability of the system. A fault injection methodology has been applied to corrupt the system both directly and indirectly. Sensor faults are simulated in LabVIEW as an indirect malfunction, and reverse engineering methodology has been implemented to break internal TMR structures as direct invasion. Experimental setups are under development for future simulation exercises.

3.1 Fault Injection Modules (LabVIEW)

A fault injection module consists of three parts: a fault list manager (FLM), a fault injection manager (FIM), and a result analyzer (RA). The preliminary setup has been completed and described in detail in Ref. [5]. An updated version of the fault injection module for the entire primary loop NPP simulator is in development stages.

3.1.1 Fault List Manager (FLM)

The FLM loads a list of fault models which includes the location (e.g. which sensor) and the fault type. All possible fault injection parameters of the primary loop are included in the list to cover all of the components of the current NPP simulator. A new feature of the updated version of the FLM allows selection of the injection methods: manual or random fault injection (while old version only generated faults randomly). The selection panel is shown in Fig. 5. The selected faults are then sent to the FIM. All fault locations and types contained in the FLM are listed in Table I.

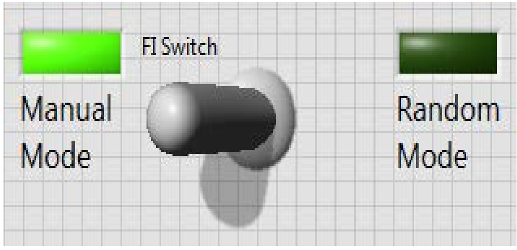

Figure 5. FI Mode Selector.

Table VII. Locations and Types of Faults

Fault Types	Locations						
	Input			Output			
	Core	Pressurizer	Pump	Core	Pressurizer	Pump	SG
Analog Typed Fault Multiplying Add Noise Shift Up Shift Down Cut-out	Control Rod 1	Heater Knob	RPM	Fuel Temp	Pressure	Pressure	P. Pressure
	Control Rod 2	Spray Knob	Valves	Mod C. Temp	Tank Level	Temp	S. Pressure
	Control Rod 3			Mod O. Temp		RPM	P. Flow
				Power Level		Flow Rate	S. Flow
				Reactivity			P.I. Temp
				Xenon Level			P.O. Temp
							S.I. Temp
							S.O. Temp
Boolean Typed Fault Cut-out Stuck Always True	Control Rods Selector	Heater Button					
		Spray Button					

3.1.2 Fault Injection Manager (FIM)

The FIM injects faults into the system. It reads out the selected faults from the FLM; “corrupts” the original values according to the type of fault; and then injects the corrupted value back into the system. The updated version has the same algorithm as that in Ref. [5]. However, the number of channels have been increased to allow larger number of input and output signals for the entire primary loop.

3.2 Cyber Security

It is essential to evaluate the potential cyber-security vulnerabilities of the digital I&C system. With increasing capability of the digital systems, PLCs, engineering workstations, etc. that are connected in a network, or even connected to the outside network, cyber-attack is a real threat. There are several potential attack surfaces. In this study we focus on studying the potential attack vectors in the communication link between the Tristation 1131 to the Tricon Controller.

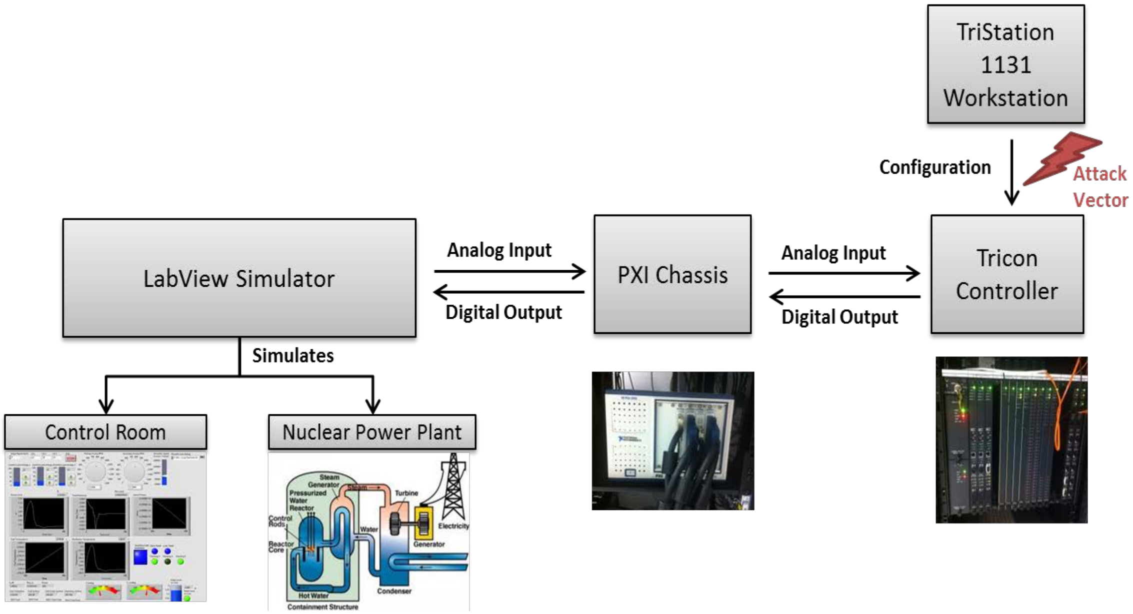

Figure 6. Test Bed Setup for Cyber Security.

Figure 6 depicts the test bed setup. One of the potential attack vectors for the Tricon TMR Controller is during its configuration phase. To configure the Tricon Controller, it needs to be connected to a workstation computer that runs the Tristation 1131 configuration software. Compare to the Tricon controller, the workstation is more susceptible to attacks and compromises due to potential connections to the outside network or accidental infection of viruses through removable devices such as a USB drives. If the workstation that runs the Tristation 1131 software is compromised, then the attacker could hijack either the Tristation 1131 software itself or the communication channel from the Tristation 1131 to Tricon, and use it to send malicious configuration to the Tricon controller.

The Tristation 1131 communicates with the Tricon controller using a proprietary protocol. Currently, the method of reverse engineering of the proprietary communication protocol undertakes to find potential vulnerabilities to attack the Tricon controller. This is done by capturing the packets when Tristation 1131 downloads the configuration file to the Tricon controller using Wireshark and feed the packet to Netzob, an open source protocol reverse engineering tool, to analyze and identify the fields within the captured packets. Part of the communication protocols are already mapped out. Understanding the communication protocol between the Tristation 1131 and Tricon allows to craft potential malicious packets to alter the configuration on the Tricon controller.

4 CONCLUSIONS

A test bed with a complete primary loop of NPP simulator is almost complete. The NPP simulator has been extended to capture the dynamics of the entire PWR and to simulate malfunctions by fault injections in real time. The simulator model and the fault injection module still need further improvements (e.g. a secondary loop of PWR, RA, etc.) for more realistic simulations and to allow the models reported here to be connected to power grid simulators available at CSL. The data set of fault injection module also needs to be extended to examine the level of safety, reliability, and resiliency of digital I&C systems. Reverse engineering methods also need to advance in parallel to define the map of the communication protocols for the internal failure of a digital controller.

Once the construction of the test bed and the analysis of the communication protocols are complete, the test bed will be used to carry out numerical experiments to assess reliability and resiliency of the digital controller. It will also be used for cyber security assessments. It may also be used to study issues associated with human machine interface and a human error factor engineering of the digitalized main control room in NPPs.

5 ACKNOWLEDGMENTS

This work is supported by a strategic research initiative (SRI) grant from the College of Engineering, University of Illinois at Urbana-Champaign.

6 REFERENCES

1. A. Benso and P. Prinetto, *Fault Injection Techniques and Tools for Embedded Systems Reliability Evaluation*, Kluwer Academic Publishers, Boston, U.S.A, (2003).
2. H. Huang and W. Yang, "Integration Technique of Digital I&C Replacement and its Critical Digital Review Procedure," *Annals of Nuclear Energy*, **51**, pp.146-155 (2013).
3. Y. S. Suh, J. Y. Keum, and H. S. Kim, "Developing Architecture for Upgrading I&C Systems of an Operating Nuclear Power Plant using a Quality Attribute-driven Design Method," *Nuclear Engineering and Design*, **241**, pp.5281-5294 (2011).
4. I. Jang, A. Kim, M. Harbi, S. Lee, H. Kang, and P. Seong, "An Empirical Study on the Basic Human Error Probabilities for NPP Advanced Main Control Room Operation using Soft Control," Nuclear Engineering and Design, **257**, pp.79-87 (2013).
5. Y. An, D. Chen, Z. Kalbarczyk, W. Sanders, C. Sollima, and Rizwan-uddin, "Digital I&C and Cyber Security for Nuclear Power Plants," *ISOFIC/ISSNP 2014 Proceedings*, Jeju, Republic of Korea, Aug 24-28 (2014).
6. M. J. Moran and H. N. Shapiro, *Fundamentals of Engineering Thermodynamics*, John Wiley & Sons, Inc., Danvers, U.S.A (2008)