Validation of LOBO Nuclear CyberSecurity (LOBO NCS) Platform and Demonstration of Manipulate Process I/O (ManiPIO) Framework for Cybersecurity Testing and Evaluation

Mohamed S. EL-Genk, Timothy Schriener
Institute for Space and Nuclear Power Studies and Nuclear Engineering Department, The University of New Mexico, Albuquerque, NM, USA

Andrew S. Hahn, Raymond E. Fasano, Christopher Lamb
Sandia National Laboratories, Albuquerque, NM, USA

Technical Work Scope: *Nuclear Energy–Cybersecurity Research Topics and Metrics Analysis (NE-1).* DOE-NEUP Project 18-15055. DOE Contract No. Nu-18-NM-UNM-050101-01 to University of New Mexico (UNM)

Performance Period: 09-15-2020 to 06-30-2021

Report No. UNM-ISNPS-01-2021
Institute for Space and Nuclear Power Studies, The University of New Mexico, Albuquerque, NM, USA, http://isnps.unm.edu/reports/

July 2021

Executive Summary

The expanding uses of digital instrumentation and control (I&C) systems in commercial nuclear power plants and energy infrastructure raise cybersecurity concerns and emphasizes the needs for high-fidelity testing capabilities and effective counter measures. The Nuclear Instrumentation & Control Simulation (NICSim) platform, currently being developed at the University of New Mexico's Institute for Space and Nuclear Power Studies (UNM-ISNPS) in collaboration with Sandia National Laboratories (SNL) under a DOE NEUP award, attempts to address some of these needs. This platform links physics-based Matlab Simulink models to emulated or physical Programmable Logic Controllers (PLCs) in I&C systems. An efficient data transfer interface and broker have been developed to manage and coordinate communication between the emulated PLCs and the Simulink models. The developed components are compatible with the DOE SCEPTRE cybersecurity framework at SNL.

The LOBO Nuclear CyberSecurity (LOBO NCS) platform that is based on NICSim architecture is being developed at UNM-ISNPS in collaboration with SNL to support cybersecurity investigations and offering academic education and professional training. LOBO NCS is used to demonstrate the NICSim platform's capabilities for investigating cyber vulnerabilities of digital I&C systems of a representative Pressurized Water Reactor (PWR) plant and components during simulated operation transients. The Manipulate Process I/O (ManiPIO) program developed by SNL provides a safe and repeatable of simulating cybersecurity events on the PLCs within the emulated I&C systems in the LOBO NCS platform. ManiPIO does not contain any exploits or security concerns and enables users to write the inputs and outputs of the PLCs using the Modbus TCP communication protocol. The program scripts sequences of control interference events that can be initiated by process variables or timed sequences. Therefore, ManiPIO can replicate highly customized and complex cybersecurity events. The ManiPIO program's network capture utility records the simulated nuclear power I&C systems' response and allows deep packet inspection of the Ethernet traffic.

The fidelity of the LOBO NCS platform is demonstrated by comparing results of a simulated transient using a compiled Simulink pressurizer model linked to the emulated pressure PLC using the DOE SCEPTRE framework to those obtained separately using the LOBO NCS platform. The produced transient values of the water level in the pressurizer and of the system pressure by the two platforms are practically identical. The differences in the network architectures used in conjunction with the LOBO NCS and SCEPTRE result in small timing differences of actuating the immersed electrical heaters and subcooled water spray in the pressurizer during the simulated transient. This transient involved sequential surge-in and surge-out events of water into and from the pressurizer to the hot leg of the PWR plant. The transient results using the DOE SEPTRE framework confirm the accuracy and validates the soundness of the architecture implemented in the LOBO NCS framework.

Results are also presented to demonstrate the capabilities of the LOBO NCS platform linked to the ManiPIO program in simulating a cyber-compromise of the PLCs in a representative PWR plant. These transient results include those of the steam generator's feedwater PLC following a 10% increase in in the steam load demand. Similar results are presented for the pressurizer and the pressure PLC during simulated surge-in and surge-out transients. The obtained results for nominal transient operations and when the emulated PLCs are subjected to simulated false data injection attacks (FDIAs) are presented and compared. The results of the performed simulated cybersecurity scenarios for both an emulated PLC developed using the OpenPLC runtime and a

commercial hardware Allen-Bradley PLC are practical identical. This confirms that emulated PLCs could be used in future simulation and investigation of cybersecurity events, which are much less expensive and easy to implement compared to the hardware PLCs, without compromising the results.

In the conducted cybersecurity scenario involving the steam generator and feedwater PLC, the ManiPIO program simulated an FDIA on the emulated PLC's memory registers to manipulate it into thinking that the water level remained constant. During nominal transient operation, the emulated feedwater PLC maintains the water level to within 0.9% of its initial steady state by adjusting the feedwater rate to the steam generator. While under the FDIA, the emulated PLC could not maintain the feedwater rate commensurate with the increase in the steam load demand. Consequently, the water level in the steam generator decreased enough to reach the set point for activating the Auxiliary Feedwater Actuation System.

The performed separate tests of linking the PWR pressurizer model to the emulated and the Allen-Bradley PLCs investigated the effects of a series of FDIAs targeting the pressure PLC on the transient response of the pressurizer during the simulated surge-in and surge-out events. In the first test, ManiPIO is scripted to write a false low-pressure value to the PLC's input register to override the pressure state variable. The second test used ManiPIO to overwrite the memory register for the water spray control value for the pressurizer. The results show that the ManiPIO program successfully manipulated the responses of the Allen-Bradley hardware PLC and the emulated open PLC using the simulated FDIAs targeting the system pressure and the water spray function for the pressurizer. The transient responses of the emulated and hardware PLCs are comparable, but for small differences in the frequency of the simulated FDIAs to successfully overwrite the PLCs registers. For the first test case the ManiPIO program overwrites the holding register for the pressure 99.8% of the time with the Allen-Bradly PLC and 94.1% of the time with the emulated PLC. The overwriting frequency is less for the FDIA targeting the register for the water spray control signal. This FDIA successfully disabled the water spray 89.3 % of the time with the Allen-Bradley hardware PLC and 93.6 % of the time with the emulated PLC. These differences could be attributed to the difference in how the hardware and emulated PLCs handle the Modbus TCP network traffic and the frequency of updating the input and output registers.

The LOBO NCS platform and ManiPIO program will be subjected to further testing and investigations while completing the remaining tasks of the NICSim project. These will include simulating cybersecurity events of the emulated PLCs in the I&C systems linked to the physics-based Simulink model of a representative fully integrated PWR plant. The LOBO NCS platform could support future cybersecurity research and the development of next generation cybersecurity and autonomous control technology and methods for terrestrial nuclear reactor power plants, space nuclear power systems, and other energy systems. The LOBO NCS platform could also be used for academic education and professional training of a new cadre of nuclear cybersecurity researchers and engineers.

List of Contents

List of Figures

List of Tables

Nomenclature and Abbreviations

I:	Integral gain constant for PI controller
P:	Proportional gain constant for PI controller
t:	Time (s)

Abbreviations

CHFR	Critical Heat Flux Ratio
CPC	Core Protection Calculator
DOE:	Department of Energy
EC	Event Constructor
ESF:	Engineered Safety Features
ESFAS:	Engineered Safety Features Actuation System
FDIA	False Data Injection Attack
GUI	Graphical User Interface
IAPWS:	International Association for the Properties of Water and Steam
I&C:	Instrumentation and Control
ICS:	Industrial Control System
I/O:	Input-Output
IT:	Internet Technology
LOBO NCS	LOBO Nuclear CyberSecurity
MGMT	Management Network
ManiPIO	Manipulate Process Input/Output
NEUP:	Nuclear Engineering University Program
NICSim:	Nuclear Instrumentation and Control Simulation
PI:	Proportional-Integral
PLC:	Programmable Logic Controller
PMS	Protection and Safety Monitoring System
PWR:	Pressurized Water Reactor
PZ	Pressurizer
SG:	Steam Generator
SNL:	Sandia National Laboratories
TCP:	Transmission Control Protocol
TCP/IP:	Transmission Control Protocol over Internet Protocol
UNM-ISNPS:	University of New Mexico's Institute for Space and Nuclear Power Studies
VLAN	Virtual Local Area Network
VM:	Virtual Machine

1. Introduction

Digital Industrial Control Systems (ICSs) for industrial and energy infrastructures and facilities worldwide have recently been the target of vicious and debilitating cyberattacks. Examples are the Stuxnet, Havex, BlackEnergy III, and CrashOverride cyber-attacks, just to mention a few (Dragos Inc., 2017a; Dragos Inc., 2017b; Falliere, Murchu, Chien, 2011; Karnouskos 2011). These malicious attacks attempt to compromise the operation and/or disable the specialized computing systems, such as the Programmable Logic Controllers (PLCs), within ICSs of the target facility or installation. The PLCs monitor and control different specific aspects and functions such as measurement sensors, instrumentation, control actuators, as well as the computers that are designed to maintain stable and safe operation within preprogrammed setpoint of the different state variables. Potential cyber-attacks could cause the PLCs to malfunction and force them to falsify operation and/or trigger a system shutdown. Falsified operation of the PLCs could compromise the safety and reliability of critical infrastructure essential to the functioning of modern societies.

Target ICS infrastructures may include, but not limited to, military and research facilities, transportation network, electric grids, oil refineries, chemical and food processing plants, manufacturing facilities, electrical power generation and distribution, nuclear and fossil fuel and renewable power plants, hydroelectric dams and water resources, among others. These energy and industrial infrastructure ICSs mostly rely on digital controllers like PLCs within their I&C systems to ensure proper operation, reduce cost and improve efficiency and reliability. Increased uses of digital rather than analog control of nuclear power plants have markedly improved operation reliability and safety, and significantly increased the plants load factors to the low 90% for decades, compared to low 60% in the 1980s, and supported incremental power uprates for existing plants (National Research Council, 1997). The increase in the electricity generation capacity because of the high load factors by the current 96 operating reactor power plants in the US is equivalent to that of 16 new build nuclear reactor plants (Nuclear Energy Institute 2021).

On the other hand, digital I&C systems in nuclear power plants might potentially introduce cyber-vulnerabilities despite that fact that these plants operate within fully isolated networks (Nuclear Energy Institute 2010). The analog I&C systems in nuclear power plants had been developed many decades ago and gradually been supplemented or replaced with digital systems. These systems are being optimized to enhance operation reliability, safety, and efficiency, but neither for the avoidance nor for effective countermeasures against sophisticated cyberattacks. Therefore, there is a need to develop effective tools and platforms that emulate the operation of the nuclear power plants to help investigate and assess the vulnerabilities of the PLCs in I&C systems of these plants to potential cyberattacks. Such platforms could double up as testbeds for developing and qualifying future digital I&C systems architectures, could be used for academic education, and for professional training to recognize the response and malfunction of the PLCs while under cyberattacks. A highly adaptable and modular platform could also support the development of I&C systems for advanced and small and micro nuclear reactors plants, some of which would be deployed and operated remotely with a high degree of autonomous control. This would be an added challenge that needs sophisticated and advanced countermeasures to protect against potential cyberattacks (Cetiner and Ramuhalli 2019; Trask, Jung, and MacDonald 2014). Future uses of autonomous control and operation technology and methods further emphasize the need for a versatile emulated platforms to investigate potential cybersecurity vulnerabilities of digital I&C systems in nuclear power plants and critical energy and industrial infrastructures.

A few simulation and emulation capabilities with varying degrees of inclusivity and breadth are being developed worldwide to investigate cyber vulnerabilities of nuclear power plants (Zhang and Coble 2020; Busquim E. Silva, et al 2020). Zhang and Coble (2020) have developed a toolkit, which links physical PLCs to a Pressurized Water Reactor (PWR) simulator as hardware-in-the-loop. They used this toolkit to investigate the effects of a false data injection on the response of the feedwater control PLC for the steam generator and to record the PLC digital signature while under cyberattack attack (Zhang and Coble 2020). The Asherah Nuclear Power Plant Simulator has been developed as a multi-national IAEA effort to conduct cybersecurity investigations of nuclear power plants (Busquim E. Silva, et al 2020). This simulator links a transient model of a representative PWR plant to either simulated models or physical hardware integrated as hardware-in-the-loop of the PLCs in the I&C systems.

High fidelity emulation models of the PLCs have advantages over simpler, low fidelity simplified models, which would be ineffective in investigating cyber-vulnerabilities of the software and firmware. The physical PLC hardware-in-the-loop also offers highest fidelity but is costly and difficult to scale up for cybersecurity research. On the other hand, emulated PLCs in the I&C systems could be easily scaled up, and quickly set up and torn down in secure sandboxed virtual testing environments.

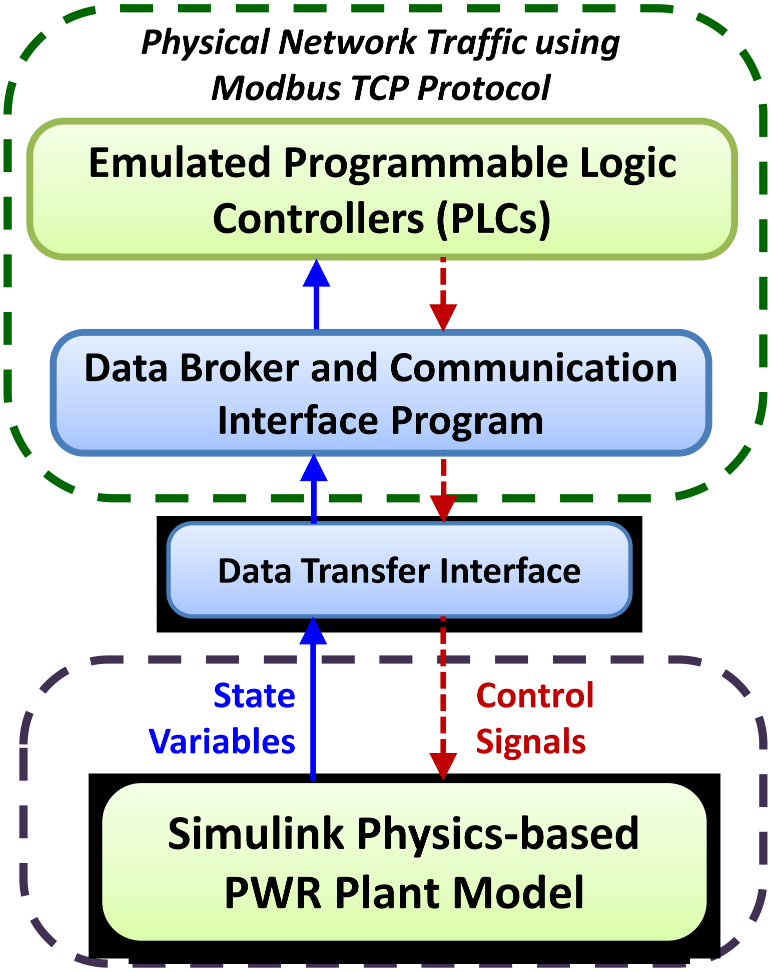

Physical Network Traffic using Modbus TCP Protocol
Emulated Programmable Logic Controllers (PLCs)
Data Broker and Communication Interface Program
Data Transfer Interface
State Variables
Control Signals
Simulink Physics-based PWR Plant Model

Fig. 1.1: A layout of the NICSim and LOBO NCS Platforms (El-Genk et al., 2020a, 2020b, 2020c; El-Genk et al. 2021).

The present work under a DOE NEUP award is developing the Nuclear Instrumentation and Control Simulation (NICSim) platform at the University of New Mexico's Institute for Space and Nuclear Power Studies in collaboration with Sandia National Laboratories (SNL) to investigate cyber-vulnerabilities of nuclear reactor plants (El-Genk et al., 2020a, 2020b, 2020c). This platform links Matlab Simulink (The Mathworks 2020) physics-based models of a representative PWR plant and various components to emulated PLCs in the digital I&C systems (Fig. 1.1). The NICSim platform is modular and could be easily extended to other nuclear power plant types and I&C system architectures. It is also compatible with the Department of Energy's (DOE's) SCEPTRE cybersecurity framework at SNL (Camacho-Lopez 2016). This framework supports integrating emulated I&C system elements, physical PLCs, and ICS components into a virtual Ethernet network and a variety of ICS communication protocols that include Modbus, DNP3 over TCP, IEC-104, among others. This technical report documents the development of cybersecurity testing and evaluation capabilities at UNM-ISNPS and presents the results of simulated cyber events on the emulated PLCs in the representative PWR plant's I&C systems.

The objectives of this report are to: (a) demonstrate the utility of the LOBO NCS platform to simulate the transient response of the feedwater PLC of the steam generator in a representative PWR plant following an increase in load demand, (b) carryout similar investigations of the pressurizer's pressure and water level PLCs during simulated surge-in and surge-out transients. These investigations are for performed first during nominal transient operation and when the emulated PLCs are subject to simulated false data injection attacks (FDIAs). Furthermore, demonstrate the fidelity of the LOBO NCS platform by comparing simulation results of the pressurizer model linked to the pressure PLC to those generated for the same models using the DOE SCEPTRE framework at SNL. These comparisons are caried out both during nominal operation and when the PLCs are subjected ton FDIA of their registries.

Section 2 - LOBO Nuclear CyberSecurity (LOBO NCS) Platform introduces and describes the architecture and capabilities of the LOBO NCS platform (El-Genk, et al. 2021), developed based on the NICSim architecture. The LOBO NCS is also being developed at UNM-ISNPS in collaboration with SNL in open access environment for future uses for academic education and both students and professional training. Both NICSim and the LOBO NSC (Fig. 1.1) link physics-based Simulink models of a representative PWR plant and components to the emulated PLCs in the plant's I&C systems using a fast and reliable data transfer interface and broker program (Hahn, Schriener, and El-Genk 2020). The LOBO NCS platform includes a user-friendly graphic interface with plotting capabilities for a real-time display of simulation results. It incorporates the Manipulate Process Input/Output (ManiPIO) framework developed by SNL to simulate cybersecurity events on both emulated and hardware PLCs.

The ManiPIO framework could be programed to write false values to the inputs and outputs of the PLCs using the Modbus TCP communication protocol. It allows for sequences of simulated cybersecurity events that can be initiated by monitoring the process variables for the PLCs in the network or by using a timed schedule. This allows the ManiPIO framework to replicate series of highly customized and complex cyber events. This framework includes a network data capture and inspection utility which records and decodes Modbus TCP packets sent through the Ethernet testing network connecting the emulated or physical PLCs. Additional details on the ManiPIO platform are included in *Appendix A - Manipulate Process I/O (ManiPIO) Framework*. The fidelity of the LOBO NCS platform is demonstrated by comparing the results of a simulated transient to those produced using the DOE SCEPTRE framework at SNL. The developed PWR pressurizer model and that of the emulated pressure PLC are incorporated into both the LOBO NCS and the SCEPTRE topology. A sequence of in-surge and out-surge events are simulated with the pressurizer model linked to the emulated PLC. The simulation results are compared to determine the differences in the control responses and the values of the simulation state variables for the pressurizer model using the two platforms.

Section 3 - Simulated False Data Injection Attacks (FDIA) on Emulated and Hardware Programmable Logic Controllers further demonstrates the capabilities of the LOBO NCS platform and the ManiPIO cybersecurity program for investigating the responses of an emulated and a commercial hardware PLC to a series of simulated FDIAs on the pressurizer PLC. In this demonstration, the pressurizer Simulink model is linked separately to an emulated PLC based on the open-source OpenPLC runtime (Alves, et al. 2014) and a commercial hardware Allen-Bradley Micrologix PLC (Allen-Bradley 2013).

The pressurizer model is used to simulate an operational transient involving sequential surge-in and surge-out events of water from and to the hot leg of the primary loop of a representative PWR plant. In the first simulated FDIA, the ManiPIO program sends a false low pressure state variable to the Modbus holding registers of the PLC. In the second simulated FDIA the ManiPIO program alters the holding register of the control signal for the water spray function to prevent the PLC from activating the water spray. The results are then compared of the responses of the emulated and commercial hardware PLCs while linked to the physics-based model of the pressurizer.

2. LOBO Nuclear CyberSecurity (LOBO NCS) Platform

The LOBO Nuclear CyberSecurity (LOBO NCS) platform is being developed at the University of New Mexico to investigate the transient response of a representative fully integrated PWR plant and various components during simulated operation transients with the PLCs in the I&C systems are the target of simulated cyberattacks. The physics-based Simulink models of the PWR plant and components in the LOBO NCS platform communicate to the emulated PLCs in the I&C systems using a fast and reliable data transfer interface and broker program (Figs. 2.1). The user-friendly graphic interface with plotting capabilities in the LOBO NCS provides a real-time display of simulation results. The modular LOBO NCS platform can support simulations of a wide range of nuclear reactor power plant types for terrestrial power generation, including advanced small and micro-modular reactors. It can also support the development of secure remote control of nuclear reactor systems using reference model adaptive control methods or digital twins, including those for planetary surface power and space exploration missions (Metzger, El-Genk, and Parlos 1991; Hahn, Schriener, and El-Genk 2020).

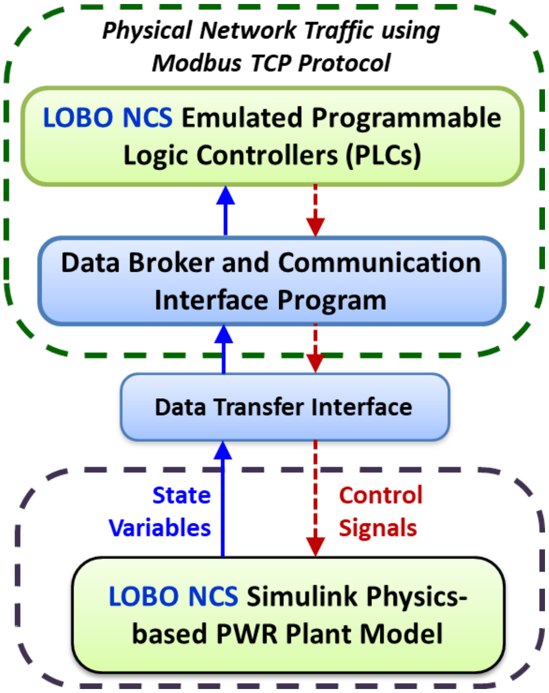

Physical Network Traffic using
Modbus TCP Protocol
LOBO NCS Emulated Programmable Logic Controllers (PLCs)
Data Broker and Communication Interface Program
Data Transfer Interface
State Variables
Control Signals
LOBO NCS Simulink Physics-based PWR Plant Model

Fig. 2.1: A layout of the LOBO NCS Platform architecture.

2.1. Platform Description

This subsection describes the architecture, various components models, the emulated PLCs in the I&C systems, and the simulation capabilities of the LOBO NCS platform for cybersecurity investigations. The LOBO NCS platform is comprised of Matlab Simulink (The Mathworks 2020) physics-based dynamic models of a representative integrated PWR plant and components. These models are linked to the emulated PLCs in the plants' I&C systems using fast and reliable data transfer interface and broker programs (Hahn, Schriener, and El-Genk 2020) (Fig. 2.1). These programs transfer state variables calculated by the Simulink models to the emulated PLCs and return the control signals generated by the PLCs to the Simulink models to adjust plant operation. The Modbus TCP protocol is used for communication between the data broker and PLCs (Fig. 2.2).

A representative integrated PWR plant Simulink model incorporates models of various plant components with built-in inputs for their control systems. Components models are those of the primary loops, the reactor coolant pump, the steam generator, the pressurizer, and reactor point-kinetics for simulating operation transients. Examples are reactor startup and shutdown and following changes in reactor thermal power, system pressure, or the steam load demand. Calculated state variables of the plant include the position of control elements in the reactor core, the reactor thermal power level, the fuel and coolant temperatures in the reactor core, the temperatures and coolant flow rate in the primary loops, the pressure and water level in the pressurizer, the exit steam quality and water level in the steam generator, the feedwater flow to the steam generator, and the shaft rotation speed of the primary coolant pumps.

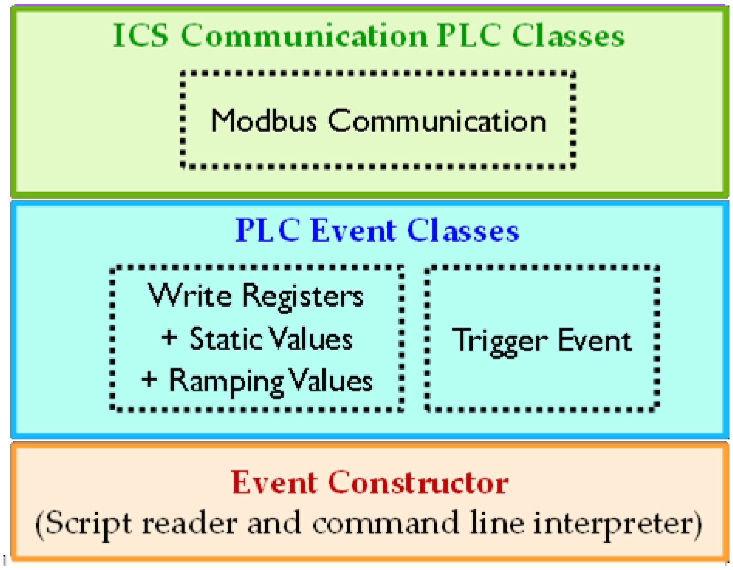


Fig. 2.2: A schematic of the internal structure of ManiPIO cybersecurity testing framework.

The calculated values of various state variables by the Simulink models during simulated operation transients are communicated to the data transfer interface (Fig. 2.1). This fast and reliable interface relays the values received to the data broker and the communication program (Hahn, Schriener, and El-Genk 2020). Thus, this program is intermediary between the data transfer interface and the emulated or hardware PLCs in the I&C systems. The data broker maintains a record of the calculated state variables and of the returned control signals from the PLCs (Fig. 2.1). The communications between the Simulink models and both the PLCs and the data broker are carried out using the Modbus TCP protocol on an isolated network. The data transfer interface and the broker programs run on the same main server node for the Simulink models and the Graphical User Interface (GUI). Each of the emulated PLCs in the I&C systems runs within a separate Virtual Machines (VM) located on multi-processor server nodes connected to the Ethernet network. The physical hardware PLCs can also be connected to the network in place of, or in conjunction with, the emulated PLCs.

The Manipulate Process Input/Output (ManiPIO) framework is incorporated into the LOBO

NCS platform to initiate simulated cybersecurity attacks on the PLCs in the I&C systems (Fig. 2.2). This framework consists of several modules of simulating cybersecurity attacks on the PLCs and for capturing and inspecting network traffic for further analysis. The cybersecurity simulation modules run on a Linux PC and communicate directly to the PLCs on the network. The data capture module records and inspects the Modbus packets sent through the network (Fig. 2.2). The isolated Ethernet network handles all traffic between the different computers and both the hardware and emulated PLCs and the computer running the capture module.

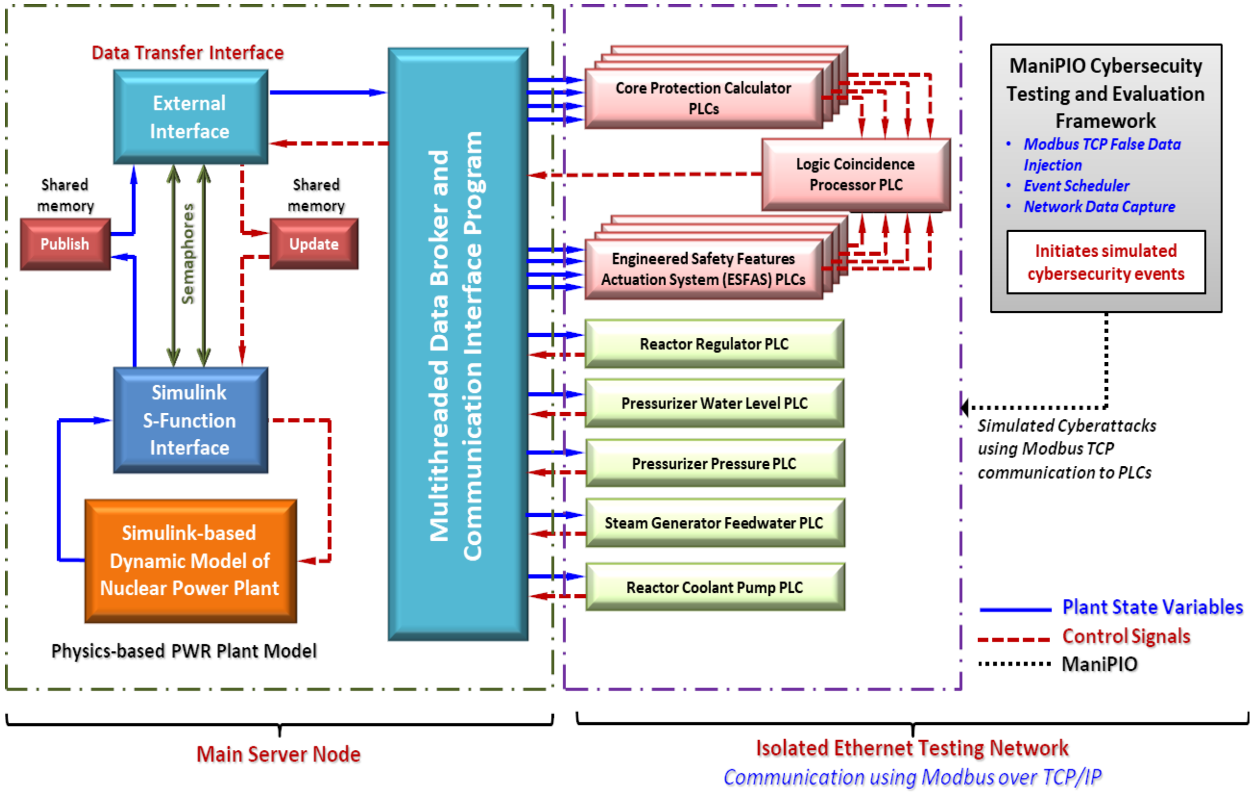

Data Transfer Interface
External Interface
Shared memory
Publish
Semaphores
Shared memory
Update
Simulink S-Function Interface
Simulink-based Dynamic Model of Nuclear Power Plant
Physics-based PWR Plant Model
Multithreaded Data Broker and Communication Interface Program
Core Protection Calculator PLCs
Logic Coincidence Processor PLC
Engineered Safety Features Actuation System (ESFAS) PLCs
Reactor Regulator PLC
Pressurizer Water Level PLC
Pressurizer Pressure PLC
Steam Generator Feedwater PLC
Reactor Coolant Pump PLC
ManiPIO Cybersecuity Testing and Evaluation Framework
Modbus TCP False Data Injection
Event Scheduler
Network Data Capture
Initiates simulated cybersecurity events
Simulated Cyberattacks using Modbus TCP communication to PLCs
Plant State Variables
Control Signals
ManiPIO
Main Server Node
Isolated Ethernet Testing Network
Communication using Modbus over TCP/IP

Fig. 2.3: Block diagrams of LOBO NCS platform for a representative PWR plant model and emulated PLCs in the I&C systems.

The physics-based models in the LOBO NCS platform utilize a custom Simulink S-Function to transfer the calcuted state variables and the returning control signals to and from PLCs, respectively (Fig. 2.3) (Hahn, Schriener, and El-Genk 2020). The S-function enables shared memory inter-process communication for writing the state variables to be transmitted to the PLCs to a shared memory location called Publish. It also reads the returning control signals from a second shared memory location called Update (Fig. 2.3).

The S-function keeps the control signal values constant throughout the minor timestep iterations while allowing the Simulink solver to reach convergence. This ensures that the S-function communicates only the proper, converged values of the state variables values to the PLCs in the I&C system. The inter-process communication semaphores that coordinate access to the Publish and Update shared memory locations enhance reliability and prevent communication interruptions and/or race conditions where the S-function and data transfer interface try to simultaneously access the same shared memory location. The semaphores also ensure that

Simulink models function in lockstep with the external interface program. The data transfer interface can be used to synchronize the transient simulation with a real-time clock function for use with PLCs using time-dependent functions such as PID controllers.

2.1.1. Data Broker and Communication Interface

The multithreaded data broker and communication interface program in the LOBO NCS exchanges information between the data transfer interface and the emulated or the physical PLCs in the I&C systems. The data broker program serves as a central repository of the received values of the calculated state variables values from the Simulink models and the returning control signals from the PLCs (Fig. 2.3). This program creates separate communication threads for each of the individual PLCs in the isolated network (Figs. 2.1, 2.3). The threads pass information to and from the central data broker using inter-process communication data queues. Each thread has one queue for the PLC's state variables and another for the control signals. These threads run independently and allow asynchronous updates from the PLCs with different internal scan times.

The broker program also communicates the current record of the state variables and the PLCs' control signals to the GUI to display the simulation results both numerical and graphically in real time on a large-format screen. The screen is connected remotely to the main server node running the data broker program (Fig. 2.3). The GUI allows the user to continuously update the two-dimensional plots of the values of various state variables calculated by the Simulink models. The user could also serve as an operator and send manual command signals through the data broker to the Simulink PWR plant model and/or to the PLCs.

2.1.2. ManiPIO Cybersecurity Testing and Evaluation Framework

The ManiPIO framework (Fig. 2.2) allows users to design and execute simulated ICS manipulations on the PLCs within the testing network. A priority cybersecurity concern is to stop interference, influence, or manipulation of the PLCs. This framework can help understand the mechanisms of interfering with the process control systems following a successful cyber-compromise within the I&C network. ManiPIO can safely simulate potential manipulations of the PLCs by malicious actors. It can manipulate the signals to the PLCs' memory registers using established ICS network communication protocols and simulates how real cyberattacks would affect the PLCs within a representative reactor plant. The ManiPIO framework and the network capture and recording program are void of any cybersecurity risks. The main or sub programs are built using open-source tools and common python libraries and do not contain any malicious software.

The highly modular ManiPIO framework is adaptable, and customizable to keep up with evolving sophisticated cyberattacks targeting the PLCs in the I&C system. The python program in MainPIO is divided into sections. The main section reads the input script and constructs the timeline of the simulated cyberattack (Fig. 2.2). This program includes ICS communication classes based on converted open-source python ICS protocol libraries. The Modbus TCP protocol is the standard communication function in the ManiPIO program. Other protocols for additional ICS communication classes could be added as needed.

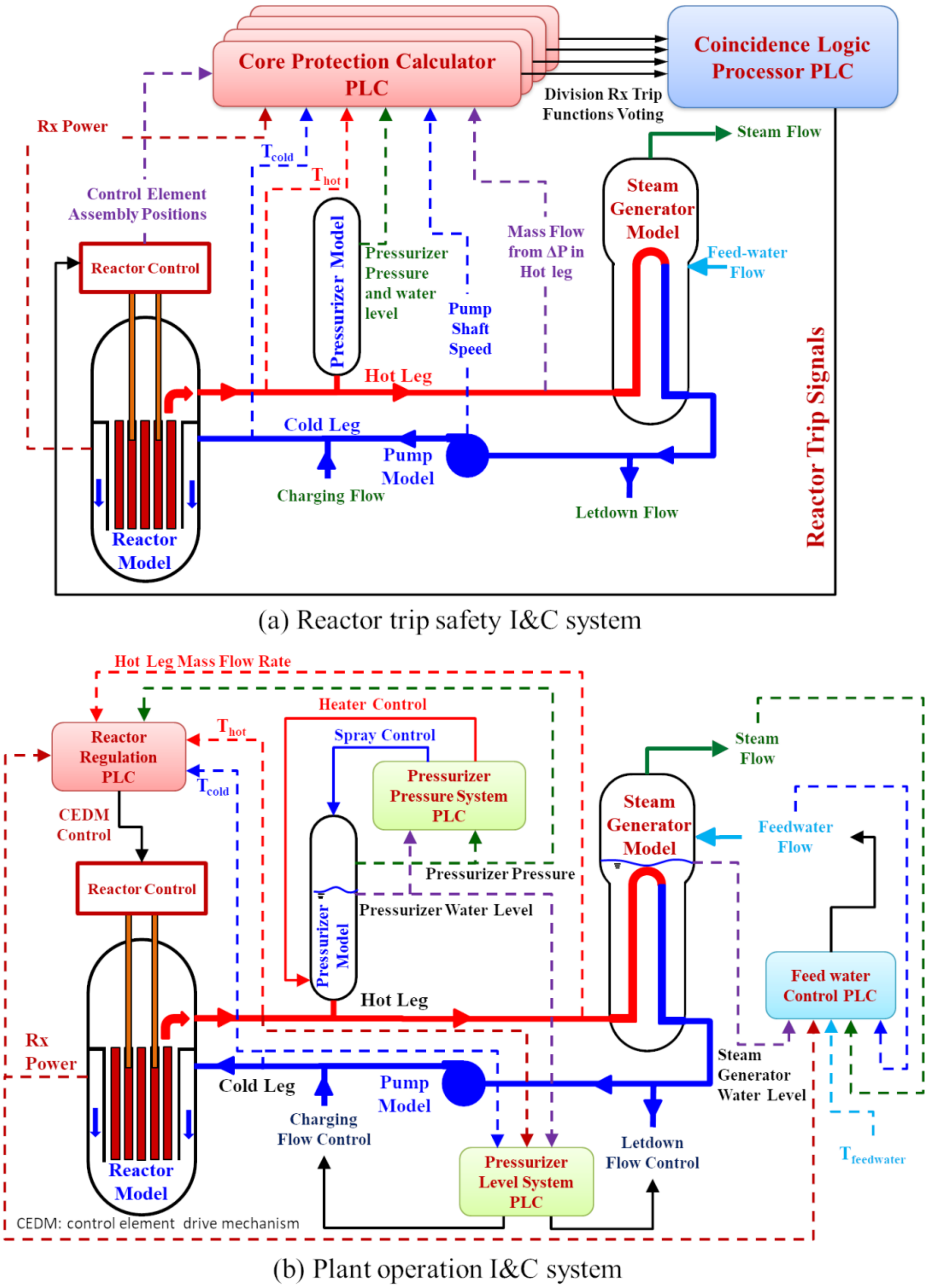
The ManiPIO program can script three major event types, namely, single, ramping values, and executing triggers. In a single event, the program writes specified value to the PLC memory registers either once or using persistent rewriting. In a ramp event, the written values to the memory registers change linearly over time. In the trigger event to monitor process, the variables stored in the PLC's memory registers could be initiated when a monitored value(s) satisfies preprogrammed setpoints. Users can schedule time delays of all event classes to create a predesigned sequence of events that could be launched on the PLCs. An Event Constructor (EC) coordinates the sequence of the events specified in the user generated input scripts and builds the simulated manipulations of the PLCs in the I&C system (Fig. 2.2). The user script informs the constructor of the communication protocols to use, the target memory registers of the PLCs, and the types of events and when to start them. The constructor then executes the events in individual threads and monitors them for safe completion. The modular design, adjustable execution schemes, and protocol flexibility enables ManiPIO users to simulate a wide range of potential cyberattacks.

The ManiPIO's network traffic capture utility records and performs deep inspection of the Modbus TCP packets on the isolated testing network. This utility is based on the Scapy Python library (Biondi 2021). It is separate from the main ManiPIO program to run on any computer on the network. It monitors the ethernet and internal loopback networks for the Modbus TCP packets, and captures, decodes, and records the information to a log file. The log provides useful data on the effects of simulated cyber events on the response of the control system. The data could be investigated to assess the vulnerability, functionality, and the fidelity of the nuclear plant models.

In summary, the ManiPIO framework (Fig. 2.2) could be used to simulate cybersecurity attacks on the PLCs in I&C systems of a representative PWR plant within the LOBO NCS platform. It uses the Modbus TCP communication protocol to simulate events which could write to the inputs and/or the outputs of the PLCs. Users can script sequences of cybersecurity attacks on one or more PLCs. The attacks could be initiated by either monitoring the PLCs process variables or using timed sequences. A combination of triggered and timed events could be replicated to investigate the effects of sophisticated cyberattacks on the functionality and response of I&C systems in a representative nuclear power plant. The network capture module in ManiPIO records the Modbus TCP traffic of the simulated control system network. The captured traffic is decoded for deep inspection of data communicated to and from the PLCs. Users can investigate the collected data for the state of communication across the network and the response characteristics of the PLCs during simulated cybersecurity events. Further details on the ManiPIO program are included in *Appendix A - Manipulate Process I/O (ManiPIO) Framework.*

2.1.3. A Representative PWR Plant Simulink Models and I&C System Architecture

The LOBO NCS platform incorporates modular physics-based models of a representative PWR plant and various components and emulated PLCs in the Protection and Safety Monitoring System (PMS) and in the Plant Operation I&C system (Figs. 2.4a and 2.4b) (El-Genk, et al. 2020a). The PMS PLCs provide essential regulatory safety functions of autonomously tripping of the reactor or actuating the Engineered Safety Features when the values of the state variables of the plant exceed preprogramed setpoints. The PLCs in the Plant Operation I&C system autonomously regulate the plant's operation state variables within programed setpoints (Figs. 2.3, 2.4). They receive the values of state variables calculated by Simulink physics-based models of a fully integrated representative PWR plant and of various plant components. Each PLC is emulated using a virtual machine running the open-source OpenPLC software to manage its control logic program (Alves, et al. 2014). The OpenPLC software runs IEC 61131-3 standard PLC programming languages and communicates using the Modbus TCP ICS protocol.



(a) Reactor trip safety I&C system

(b) Plant operation I&C system

Fig. 2.4: Block diagrams of physics-based models of a representative integrated PWR plant and components with the emulated PLCs in the I&C systems (El-Genk, et al. 2020a).

The Simulink models of the various components in a representative PWR plant are those of (a) the reactor, which couples thermal-hydraulics and point-kinetics sub-models in the reactor core, (b) the primary loops thermal hydraulics model, which solves the overall mass, momentum, and energy balance to calculate the primary coolant temperatures and flow rate, (c) a three-region nonequilibrium pressurizer model that regulate the system pressure and the water level in the pressurizer (El-Genk, Altamimi, and Schriener 2021), (d) a steam generator model that regulates the water level and exit quality in the steam generator as well as the feedwater flow rate, and (e) a primary pump model that relates the coolant flow rate to the shaft rotation speed based on the pump characteristics (El-Genk, et al. 2020a).

These models are modular for adapting the LOBO NCS platform to different plant designs. This could be done by specifying the type, dimensions, masses, and materials of the various components, the reactor kinetics parameters, the reactivity worth of reactor control elements, the temperature and burnup reactivity feedback parameters, the pump characteristic curves, and the secondary loop thermodynamic parameters (El-Genk, et al. 2020a).

Figure 2.4a shows the portion of the PMS that performs the reactor trip voting function of the PWR plant. The four independent Core Protection Calculator (CPC) PLCs receive the values of the calculated state variables by the Simulink models of the integrated plant and various components. These variables include the reactor thermal power, the control element assembly positions, the water temperatures in the primary loops hot and cold legs, and the pressure and water level in the pressurizer, the water level in the steam generator and the feedwater rate to SG. The CPC determines the coolant flow rate in the primary loops using two separate means, namely: (a) from the intersection of the pressure losses demand curve for the primary loops and the reactor pumps' supply curves, and (b) from the measured differential pressure across a piping section of the hot leg.

The CPC program then calculates: the (a) Critical Heat Flux Ratio (CHFR) in the reactor core at the specified thermal power, (b) the coolant flow rate in the reactor core and in the primary loops, and (c) the temperature margin from saturation temperature at the system pressure for the coolant exiting the reactor core. The received state variables and the calculated parameters based on these variables are compared to preset safety setpoints for the different reactor trip functions. Exceeding any of the setpoints prompts the CPCs to communicate a vote to trip the reactor to the coincidence logic processer PLC (Figs. 2.3, 2.4a). This PLC compares all four voting signals and generates and signals to the nuclear plant model to trip the reactor if at least 2/4 CPCs votes are to trip.

The PLCs in the Plant Operation I&C system for the autonomous operation of various components within a representative reactor's primary loop are indicated in Fig. 2.4b. These are the reactor regulation PLC, the pressurizer's pressure and water level PLCs, the steam generator's water level and feedwater control PLCs, and the reactor coolant pumps' PLCs. These PLCs receive the values of the state variables calculated by the Simulink models of the plant's components and send back control feedback signals to the integrated plant model. The coefficients for the control programs of these PLCs have been investigated to ensure smooth control responses during simulated plant operation transients (El-Genk, et al. 2020a). The reactor regulation PLC monitors and adjusts the reactor thermal power within specified setpoints by the operators. It compares the differences between the desired reactor power and those calculated by the coupled reactor's kinetics and the primary loops thermal-hydraulics models. When these differences exceed the allowed tolerance, the PLC indicates the need for a corrective action to the operator.

The pressure PLC monitors and maintains the system pressure in the primary loop within preprogramed setpoints. This is done by controlling the electrical power level to the immersed proportional heaters, turning on or off the electrical power to the immersed backup heaters, and changing the opening of the water spray nozzle. This PLC intermittently opens the relief valve for the pressurizer if the system pressure surpasses a maximum setpoint. The water level PLC monitors and regulates the water level in the pressurizer and the total water inventory in the primary loops. The water inventory in the primary loops is adjusted by controlling the rates of water inflow into the primary loop from the charging pumps and water outflow through the letdown valves (Figs. 4a,b). The pressurizer's water level and pressure PLCs work together to adjust the pressure and water inventory in the primary loops.

The steam generator feedwater PLCs control the water inventory in the Steam Generators (SGs) and ensures that the U-tube bundles in the SG are adequately covered with water. These PLCs monitor the measured water level in the downcomer of the SG and adjust the rate of feedwater flow. They also accommodate the change in the steam generation rate in response to a change in the electrical load demand (Fig. 2.4b). The feedwater rate is controlled by adjusting the opening of the throttle valve between the feedwater pumps and the water injection into the steam generators. PLCs regulate the shaft rotation speed of the reactor pumps connected to the cold legs of the primary loop. This PLC uses the calculated water flow rate and total pressure losses in the primary loops to determine the target shaft rotational speed and adjusts those of the pumps to match the target value.

2.2. Simulated Steam Generator Transients Nominally and Under an FDIA Attack

This section presents and discusses the results of a simulated nominal operation transient of a SG in a representative PWR plant following a 10% increase in steam load demand and then the return to nominal operation condition. These results are compared to those of the same transient but while the emulated feedwater PLC for the SG is under a False Data Injection Attack (FDIA) launched by the ManiPIO program (Fig. 2.2). These transient simulation analyses confirm the fidelity of the SG Simulink model and the emulated feedwater PLC and demonstrate the capabilities of the LOBO NCS platform for cybersecurity investigations. The SG physics-based Simulink model and the emulated feedwater and water level control PLCs are described in detail elsewhere (El-Genk, et al. 2020b).

The SG starts simulated transient at nominal steady state conditions. These are steam generation and feedwater flow rates of 660 kg/s, water level of 74.5% and water temperature of 594.1 K in the hot leg of the primary loops of a representative PWR plant (Fig 2.5). During the simulated transient, the flow rate and temperature of the water entering the U-Tubes of the SG are kept constant at their nominal steady state values. However, the water level in the SG's downcomer and the exit steam quality are allowed to change commensurate with the change in the steam load demand.

The transient operation begins at t = 100 s (point 1 in Fig. 2.5) in response to a 10% linear increase in the steam load demand over a period of 600 s (point 2 in Fig. 2.5). Subsequently, the steam load demand holds steady for 600s (point 3 in Fig. 2.5) before decreasing at t = 1,300 s (point 4 in Fig. 2.5) linearly to zero during a period of 600s. Beyond this time the SG returns to nominal steady state operation conditions. The results show that in response to the linear increase and decrease in the steam load demand (Fig. 2.5a) the feedwater PLC increases and decreases the feedwater flow rate, respectively (Fig. 2.5b). Conversely, the water level in the downcomer of the SG decreases and increases, respectively (Fig. 2.5c). The emulated feedwater PLC uses a Proportion-Integral (PI) controller to adjust the feedwater rate to SG by adjusting the position of the feedwater throttle valve (Fig. 2.6). The values of the proportional and integral control constants used for the PI controller of the PLC, P = 0.02, and I = 0.6, produce the smoothest transient results (El-Genk, et al. 2020b).

The increase in the steam generation rate in response to the linear increase in the steam load demand increases the rate of heat removal from the water flowing in the U-Tubes of the SG to support the boiling of the secondary loop water flowing on the shell side (Figs. 2.6a, 2.7). Results in Fig. 2.5a, show the water level in the SG (Fig. 2.5c) decreases to 74.5%, which is 0.9% lower than its initial steady state value of 75.4% (Fig. 2.6c). When the increase in the steam load demand ceases, the water level in steam generator returns to its nominal value (points 1 and 4 in Fig. 2.5c). At should time, the feedwater PLC returns the rate of feedwater to its initial value (points 1 and 4 in Fig. 2.5b).

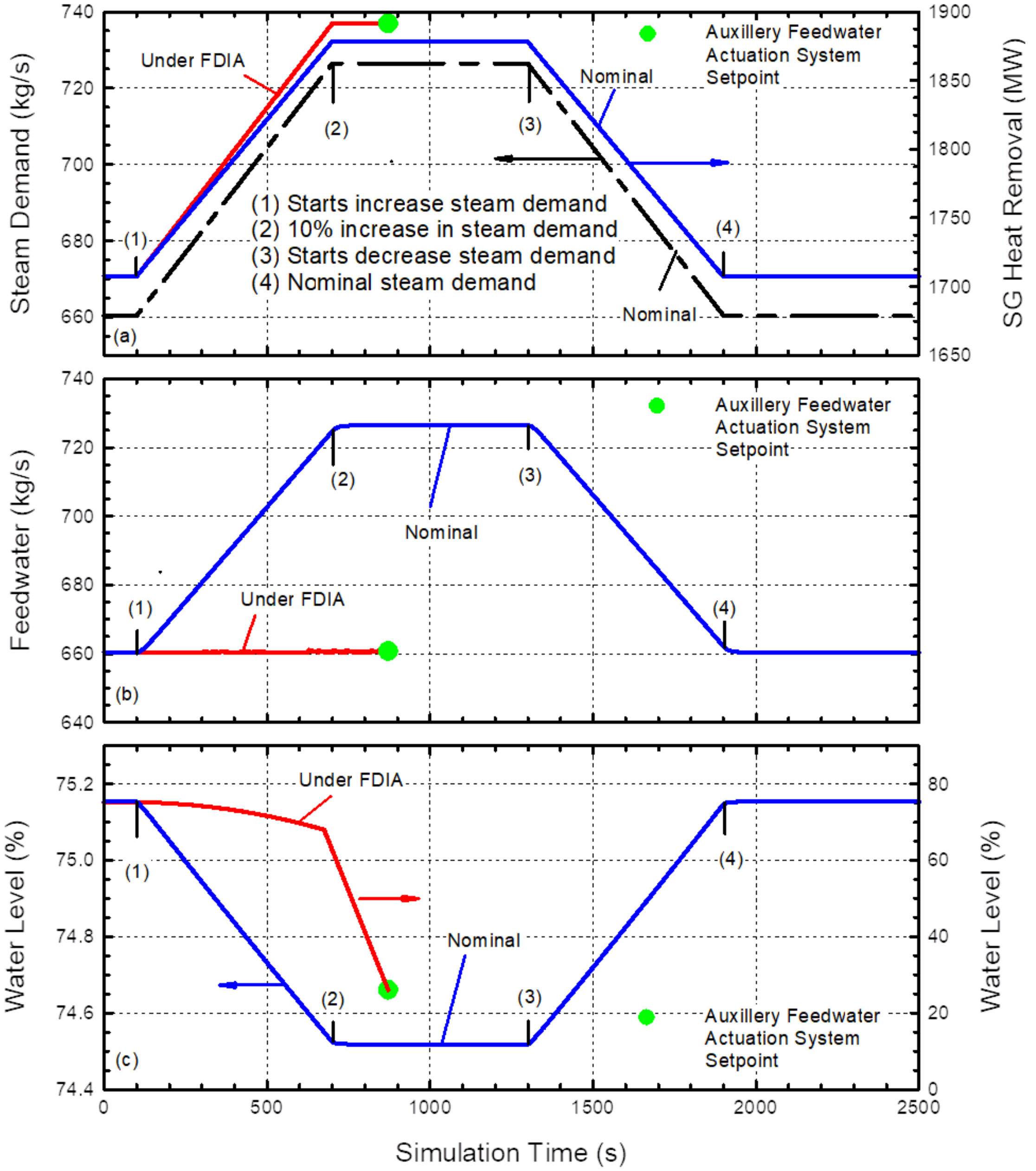


Fig. 2.5: Simulated transients of SG linked to the feedwater PLC following a 10% increase in steam demand nominally and when subject to an FDIA.

The simulated operation transient is repeated with the emulated feedwater PLC is under a simulated FDIA using the ManiPIO program. The obtained results are compared to those presented in Figs. 2.5a-c during normal operation conditions. The simulated malicious FDIA program monitors the input memory registers of the OpenPLC runtime of the emulated feedwater PLC. It triggers the FDIA when the water level in the SG decreases in response to a 10% linear increase in the steam load demand. During the FDIA, the ManiPIO program repeatedly overwrites the memory register of the emulated feedwater PLC with the water level steady state value prior to the simulated transient. As the steam demand increases (Fig. 2.5a) the FDIA continues to manipulate the PLC to maintain the feedwater injection rate constant and equal to its nominal steady state value (Fig. 2.5b). This causes the water level in the steam generator to decrease faster than nominal (Fig. 2.5c). The resulting change in the slope of the decreasing the water level in the SG (Fig. 2.5c) is due to the change in cross sectional area of the annular downcomer from the wider upper section to the narrower lower section (Fig. 2.6).

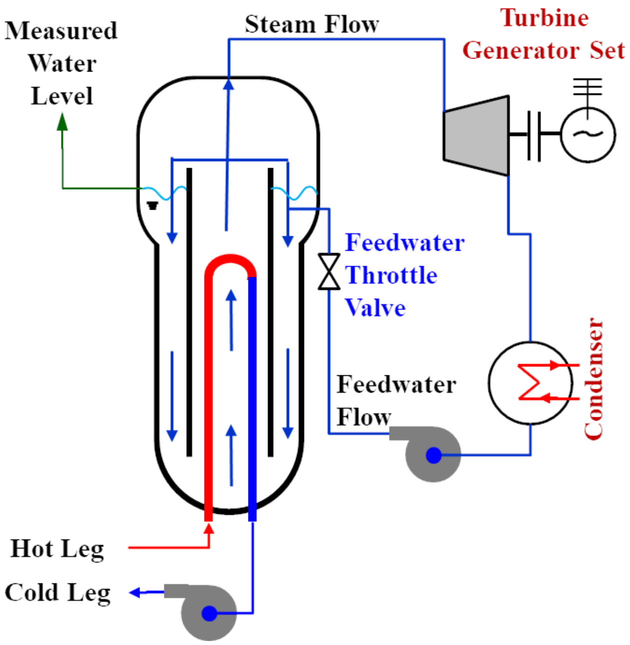


Fig. 2.6: A schematic of steam generator model linked to the secondary loop in a PWR plant.

The water level in the SG downcomer continues to decrease until reaching the setpoint for the Engineered Safety Features Actuation PLC, indicated by solid circle symbol in Fig. 2.5a-c. This activates the Auxiliary Feedwater Actuation System at t = 872 s of the simulated transient while the feedwater PLC is under the simulated FDIA attack. At such time, the simulated transient is terminated, as the indicated in Fig. 2.5a with a higher heat removal than nominal. The corresponding water level in SG of 26% is much lower than nominal level of 74.5% prior to the initiation of the simulated transient. The results presented in Figs 2.5a-c, demonstrate that the ManPIO program within of the LOBO NCS Platform can successfully simulate FDIA cybersecurity events on the emulated PLCs of a representative PWR plant and components.

2.3. Comparison of Simulation Results of the Pressurizer Model and PLCs in SCEPTRE Framework and LOBO NCS Platform

To further confirm the fidelity and demonstrate the capabilities of the LOBO NCS platform the results of a simulated transient of the pressurizer Simulink model linked to the emulated pressure PLC (El-Genk, Altamimi, and Schriener 2021) are compared to those obtained for the same transient using the established DOE SCEPTRE framework at SNL. In this comparison, the Simulink model of the pressurizer is separated from the integrated PWR model in a standalone configuration. It is compiled using the Simulink C-coder into an executable and the water surge-in and surge out rates into and from the pressurizer to the hot leg, and water temperature in the hot and cold legs are specified in the model input. The DOE SCEPTRE framework links the executable Simulink pressurizer model (referred to as a provider) to either emulated PLCs within VM environments or embedded physical hardware PLCs. SCEPTRE handles intercommunication across a virtual computer network using real ICS communication protocols. It uses an orchestration environment named Phenix that allows simulation of large-scale networks of VMs (Phenix SCEPTRE Development Team 2021). The Phenix environment is built upon the capabilities of the MiniMega program (Crussell, et al. 2015) with an improved user interface and additional support for industrial control networks. The MiniMega program developed at SNL enables the automatic initiation and networking of VMs within the virtual networks.

The SCEPTRE environment produces accurate virtual representations of real control system networks and enables the collection of network and simulation data. For a given ICS, SCEPTRE simulates two networks: (a) a top-level visible network representing the physical Ethernet network in the plant, and (b) a separate management network that handles the transfer of physical process data to sensors and actuators and returns the control signals from the PLCs to the connected simulation models. SCEPTRE can capture and analyze traffic across both networks.

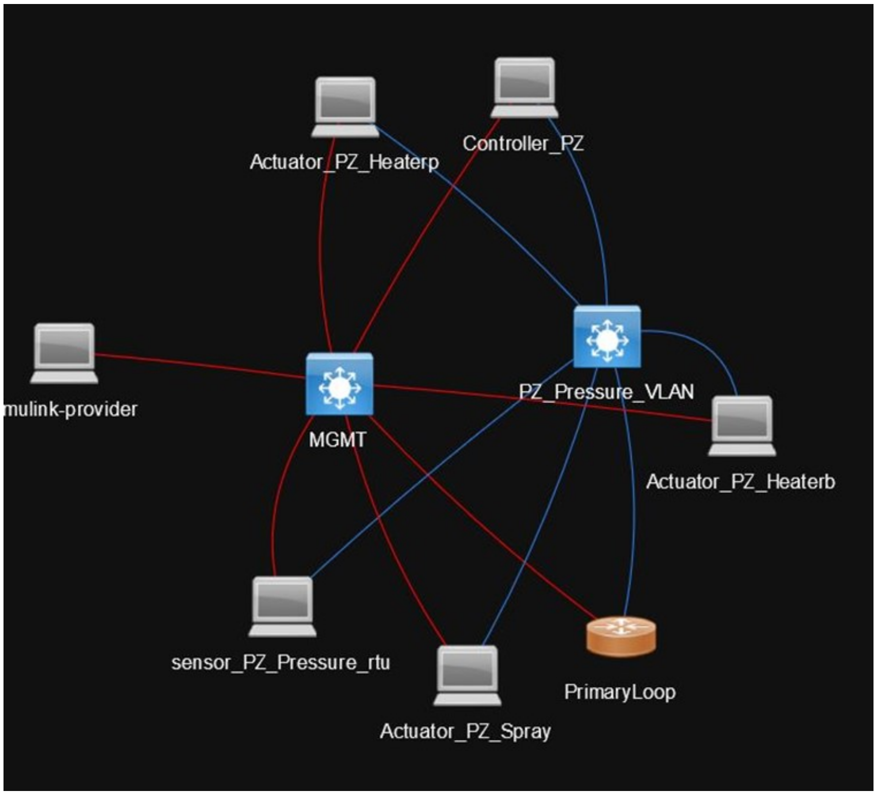


Fig. 2.7: Network topology of Phenix environment in the SCEPTRE framework for the simulated transient of the Simulink pressurizer model and the emulated pressure PLC.

For the simulation transient the network topology in SCEPTRE is comprised of the pressurizer Simulink model as the provider, three actuators, a sensor, and the emulated pressure PLC (Fig. 2.7). This figure shows the connections between all these components on both the management network (MGMT) in red, and the top-level plant network in blue. The top-level network for the pressurizer is connected by a Virtual Local Area Network (VLAN) supported by the emulated network router labeled *PrimaryLoop* (Fig. 2.7). This network represents that of the physical I&C system in a plant and allows data traffic or exchange between the sensors, actuators, and the PLC. The management network is a separate VLAN, which provides the sensors with values of the process state variables and returns the control signals from the PLC to the pressurizer Simulink model. The management network can be thought of as the copper wires for transmitting the analog voltage and current signals between the physical process sensors and the actuators and their respective controllers.

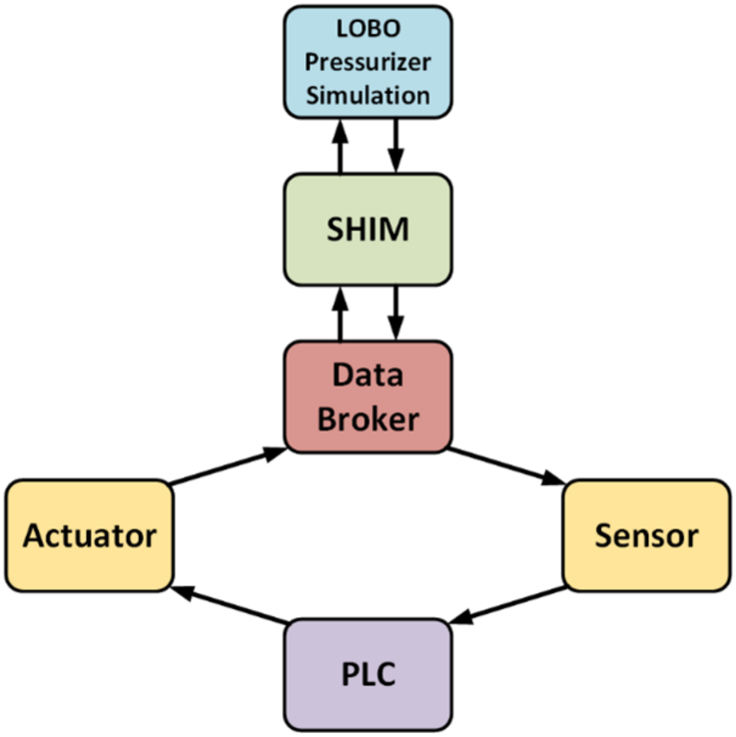


Fig. 2.8: A sketch of data communication scheme used in SCEPTRE for the transient simulation of pressurizer Simulink model and the emulated PLC**.**

The developed Simulink model of the pressurizer is linked to the management network in the Phenix environment using an interface called a SHIM (Fig. 2.8). The SHIM program communicates with the Simulink model through a shared memory data transfer interface that is synchronized with semaphores (Fig. 2.8). This interface is like that implemented in the LOBO NCS platform (Figs. 2.3 and 2.9). The SHIM program sends the state variables calculated by the Simulink model to the data broker in Phenix to broadcast through the management network. Programs running on the sensor VMs in the topology read these variables and send them to the pressurizer PLC across the plant network (Figs. 2.7-2.8). Programs on the actuator VMs within the topology read the control signals generated by the PLC and send them to the data broker before being passed to the SHIM program. The control signals are then transmitted to the

Simulink pressurizer model via shared memory communication (Figs. 2.8, 2.9).

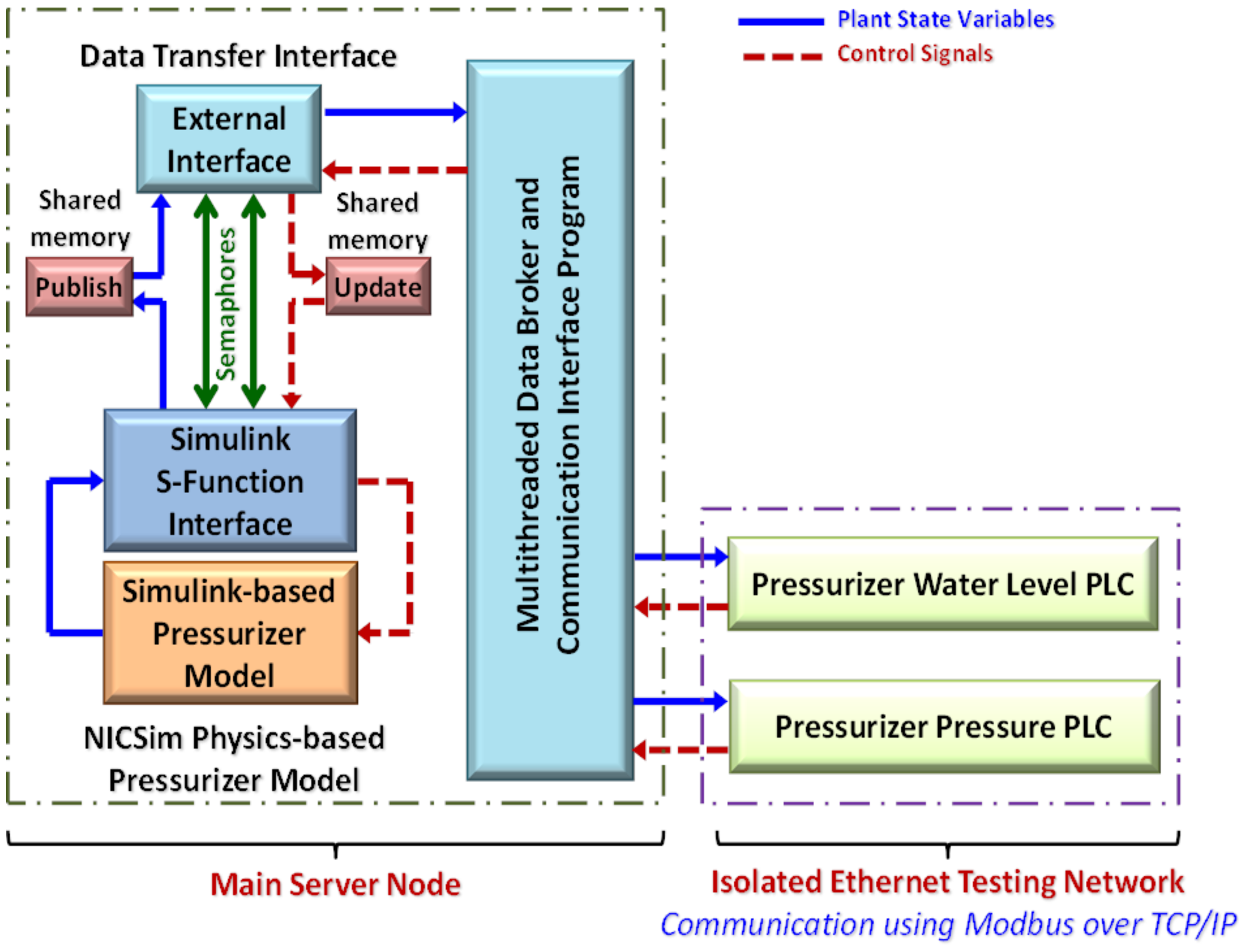

Plant State Variables
Control Signals
Data Transfer Interface
External Interface
Shared memory
Publish
Semaphores
Shared memory
Update
Multithreaded Data Broker and Communication Interface Program
Simulink S-Function Interface
Simulink-based Pressurizer Model
NICSim Physics-based Pressurizer Model
Pressurizer Water Level PLC
Pressurizer Pressure PLC
Main Server Node
Isolated Ethernet Testing Network
Communication using Modbus over TCP/IP

Fig. 2.9: A layout of the setup of linking physics-based Simulink model of the pressurizer to the emulated PLCs.

2.3.1. Simulation Results of the linked Pressurizer Model to PLCs within LOBO NCS Platform

Figure 2.9 is the layout in the LOBO NCS platform used for performing simulation transients of the pressurizer Simulink model linked to the emulated PLC. The model is compiled as a stand-alone C-executable to run on the main server node with the data transfer interface, data broker and the communication program. The emulated pressure and water level PLCs are connected to the data broker and the communication interface on an isolated Ethernet testing network.

The emulated PLCs with the OpenPLC runtime run inside VMs on a multiprocessor server node. The control signals from the PLCs are returned to the Simulink model to actuate the immersed heaters and the water spray in the pressures as needed. Since the performed operation transients are for the pressurizer model disconnected from the primary loops of a representative PWR plant, the water charging and letdown systems in the primary loops and, hence (Fig. 2.4b) the water level PLC would not affect simulation results (Fig. 2.10).

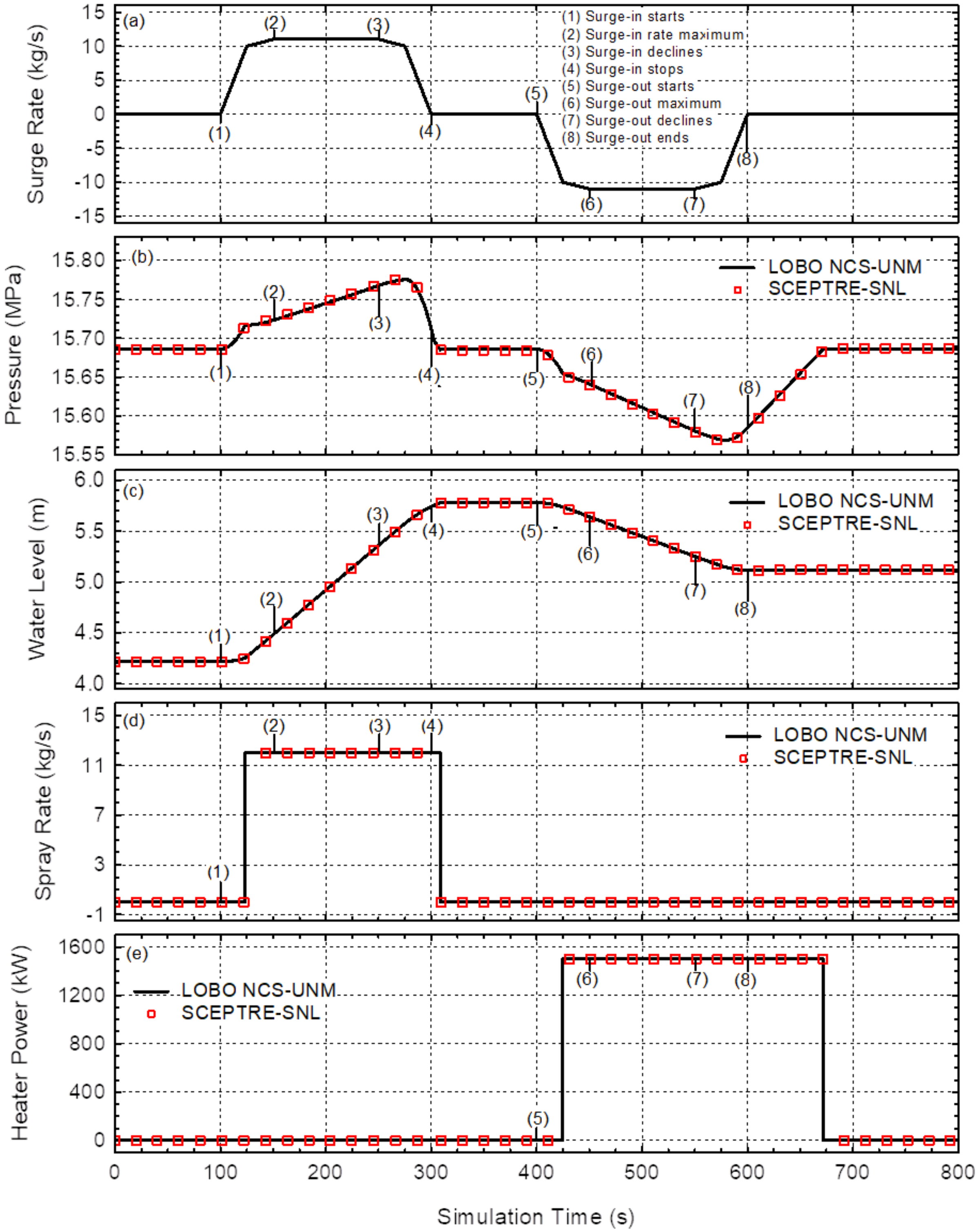


Fig. 2.10: Comparison of simulation results of pressurizer model linked to emulated PLCs in sequential surge-in and surge-out event using LOBO NCS and SCEPTRE.

2.3.2. Simulated Transient

This subsection compares the obtained results using the LOBO NCS platform and the SNL SCEPTRE framework (Fig. 2.10). These results are a simulated transient operation of the pressurizer's Simulink model and the pressure PLC. A simplified program of the emulated PLC regulates the system pressure during the simulated transients. These are comprised of a surge-in of water from the hot leg of a representative PWR plant into the pressurizer followed by a surge-out of water from the pressurizer to the hot leg. The pressure PLC controls the electrical power to the immersed heaters and the opening of the water spray nozzle in the pressurizer to maintain the pressure within programed setpoints (Fig. 2.4b). The electrical power to the immersed heaters increases the rate of flash evaporation into the top saturated vapor region of the pressurizer (Fig. 2.11). In the simulated transients the side heat losses from the pressurizer wall to the environment are neglected. On the other hand, the spray of tiny subcooled water droplets into the vapor region of the pressurizer helps reduce the system pressure by stimulating condensation onto the surface of droplets (Fig. 2.11). For this test. the pressure PLC is configured with the power to the immersed heaters and the opening of the water spray nozzle operating in a binary state; either fully off or fully on.

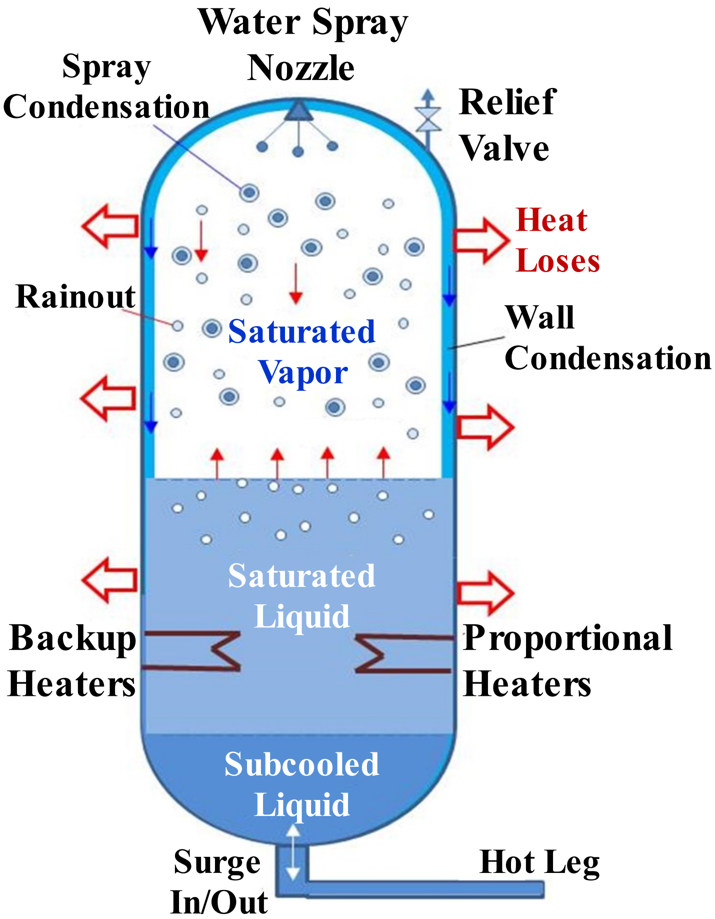


Fig. 2.11. A sketch of the Simulink pressurizer model showing various regions and the physics processes taken place (El-Genk, Altamimi, and Schriener 2021).

The water spray switches on when the pressure increases above a setpoint of 15.716 MPa. The PLC maintains the water spray rate of 12 kg/s until the pressure reaches or decreases below a lower setpoint of 15.686 MPa, at which the water spray into the pressurizer ceases. When the pressure decreases below a pressure setpoint of 15.656 MPa the pressure PLC switches the immersed heaters on at 1.5 MW. This power level is maintained until the system pressure increases due to flash evaporation into the top saturated vapor region of the pressurizer. When the pressure reaches a setpoint of 15.686 MPa the PLC shuts off the power to the immersed electrical heaters. This PLC control scheme with sharp transitions for activating and deactivating the power to the immersed heaters and the spray of water droplets is employed in simulations carried out using both the LOBO NCS platform and the DOE SCEPTRE framework

The obtained values of the electrical power to the heaters, the water spray rate, the system pressure, and the water level in the pressurizer are compared to detect any differences in the magnitudes and timings. The control program for the pressure PLC is written in the IEC 61131-3 standard structured text language and compiled and run using the OpenPLC runtime (Alves, et al. 2014). On the LOBO NCS platform the emulated PLC running OpenPLC uses a virtual machine with VMWare software. On the SCEPTRE platform the OpenPLC runs within a VM orchestrated by MiniMega (Fig. 8).

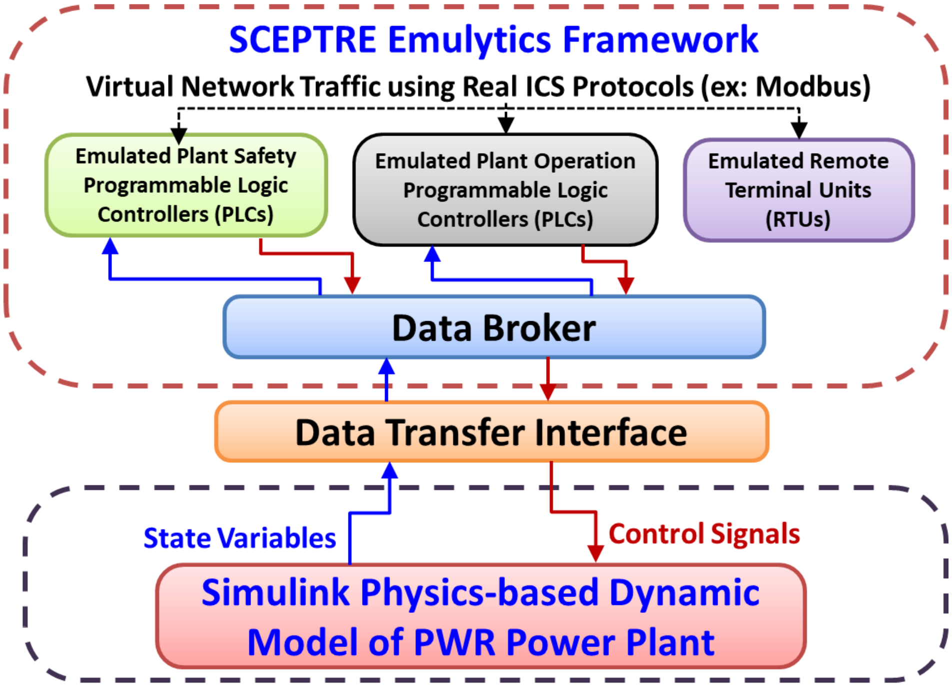

SCEPTRE Emulytics Framework
Virtual Network Traffic using Real ICS Protocols (ex: Modbus)
Emulated Plant Safety Programmable Logic Controllers (PLCs)
Emulated Plant Operation Programmable Logic Controllers (PLCs)
Emulated Remote Terminal Units (RTUs)
Data Broker
Data Transfer Interface
State Variables
Control Signals
Simulink Physics-based Dynamic Model of PWR Power Plant

Fig. 2.12. A layout for testing the pressurizer model linked to emulated and hardware PLCs using the DOE SCEPTRE Framework at SNL.

The simulated transient involving a surge-in of water from the hot leg into the pressurizer followed by a surge-out of water into the hot leg (Fig. 2.10) starts from nominal steady state conditions. These are of a system pressure of 15.686 MPa, water level in the pressurizer of 4.216 m, and hot leg water temperature of 564.8 K. After 100 s into the simulated transient (point 1 in Fig. 2.10a) water from the hot leg surges into the pressurizer at a linear rate and reaches 10.0 kg/s within 25s (or t = 125 s). During the subsequent 25s, water surge-in rate continues to increase slowly to 11.0 kg/s at t = 150 s (point 2 in Fig. 2.10a). The surge-in rate is maintained steady at this level for 100 s (t = 250 s at point 3 in Fig. 2.10a). At such time, the water surge-in rate decreases linearly to 10.0 kg/s at t = 275 s, and then to zero at t = 300 s (point 4 in Fig. 2.10a). This point marks the end of the surge-in part of the simulated transient of the pressurizer. During the next 100 s, there is no surge-in or surge-out of water from the pressurizer from and to the hot leg, respectively.

The sequential surge-out phase of the simulated transient starts at t = 400 s (point 5 in Fig. 2.10a). During that phase, the surge-out rate of water from the pressurizer to the hot leg decreases linearly to 10.0 kg/s with 25 s (or at t = 425 s). It continues to decrease linearly but at a slower rate to reach 11.0 kg/s within 25 s (or t = 450 s at point 6 in Fig. 2.10a). The surge-out rate is kept constant at this rate for 100 s to t = 550 s (point 7 in Fig. 2.10a). It then decreased linearly to 10.0 kg/s and to zero at t = 575 s and 600 s, respectively (point 8 in Fig. 2.10a). Beyond this point the pressurizer operation returns to its nominal steady state conditions.

2.3.3 Comparison of Simulation Results

The results of the simulated transient of the pressurizer in a representative PWR using the LOBO NCS platform (Fig. 2.9) are compared to those obtained for the same transient using the DOE SCEPTRE framework at SNL (Fig. 2.12). During the simulated transient described above the emulated pressure PLC controls both the water spray into the top vapor region of the pressurizer (Fig. 2.11) and the electric power to the immersed heaters in the middle region of saturated/subcooled water. The PLC receives the system pressure calculated by the compiled Simulink model of the pressurizer and returns the control signals to turn on or off the water spray and/or the immersed heaters, back to the Simulink model. In the LOBO NCS platform the calculated pressure and the control signals are communicated directly to and from the PLC using the data broker and communication program (Fig. 2.9). In contrast, the topology in the SCEPTRE framework communicates the calculated state variables by the pressurizer Simulink model to the PLC from the sensors' VMs. The PLC control signals are then communicated to the control actuators' VMs before being passed through the SHIM to the Simulink model of the pressurizer (Figs. 2.7-2.8).

When the surge-in of water from the hot leg into the pressurizer starts (point 1 in Fig. 2.10) the inflow of water raises the water level in the pressurizer, which compresses the top vapor region, increasing the system pressure (Figs. 2.10b, c). When the rising pressure reaches the setpoint to turn on the water spray the PLC sends a control signal to open the spray nozzle. The injected subcooled water droplets at a rate of 12 kg/s into the top vapor region stimulates vapor condensation onto the surface of the droplets, which slows down the increase in pressure (Fig. 2.10d). The spray droplets and the vapor condensate eventually reach the middle region of the pressurizer and contribute to changing the water level in the pressurizer. In the LOBO NCS the pressure PLC turns on the water droplets spray at t = 123.14 s, compared t = 124.02 s when using SCEPTRE, a difference of only 0.88 s (Fig. 2.10d). The results in Figs. 10b and 10c show the system pressure peaks and begins to decrease before the surge-in phase of the simulated transient ends (Point 4 in Fig. 2.10b). It remains steady during the following 100s (to point 5 in Figure 2.10b). On the other hand, the water level in the pressurizer steadily increases through the end of the surg-in phase of the simulated transient and remains steady for the following 100 s (points 5 in Fig. 2.10c).

The pressure PLC switches the water spray off at t = 308.68 s in the LOBO NCS simulation, compared to t = 306.68 s (~2 s earlier) in the SCEPTRE simulation. Owing to this slight difference in timing, the predicted system pressure in the LOBO NCS platform peaks at 15.776 MPa, which is slightly lower than that predicted in SCEPTRE of 15.777 MPa (Fig. 2.10b). The in-surge of water into the pressurizer and injected water spray increases the water level in the pressurizer during the surge-in phase of the simulated transient, reaching a maximum of 5.781 m at the end of the surge-in phase, closing the water spray nozzle (Fig. 2.10c). This figure shows that the predictions of the maximum water levels at the end of the surge-in phase of the simulated transient in the LOBO NCS and the SCEPTRE are practically identical.

When the surge-out phase of the simulated transient starts (point 5 in Fig. 2.10), the resulting decrease in the water level in the pressurizer (Fig. 2.10c) expands the top vapor region in the pressurizer and decreases the system pressure (Figs. 2.10b and 2.11). When the decreasing pressure reaches or drops below the preprogramed setpoint, the pressure PLC sends a command signal to turn on the submerged electrical heaters. The dissipated power results in flash evaporation into the top vapor region of the pressurizer to help restore the system pressure (Figs. 2.10e, 2.11). The LOBO NCS platform switches the immersed electrical heaters at t = 424.64 s compared to t = 425.19 s using the SCEPTRE framework, a slight difference of only 0.55 s. The timing difference between the two platforms is larger when the PLC switches the immersed heaters off following the end of the surge-out phase of the simulated transient (beyond point 8 in Fig. 2.10e). In the LOBO NCS these heaters are switched off at t = 671.84 s, compared to t = 675.16 s in the SCEPTRE framework, a difference of 3.32 s. Despite these small timing differences for actuating of the immersed heaters and the water spray during the simulated surge-in and surge-out transients, the predicted lowest system pressure of 15.569 MPa using SCEPTRE is practically the same as that predicted using the LOBO NCS of 15.567 MPa (Fig. 2.10b).

Following the simulated sequential surge-in and surge-out events, the steady state water level in the pressurizer of 5.119 m is higher than its initial steady state value of 4.216 m (Fig. 2.10c) before the initiated transient. This difference in the water levels reflects the mass of the added water spray during the surge-in phase of the simulated transient. The excellent agreement of the results of the simulated transients using the LOBO NCS platform at UNM and the DOE SCEPTRE framework at SNL conforms the fidelity and validates the architecture of the LOBO NCS for cybersecurity investigations. Despite the vast differences the topologies of the networks in LOBO NCS and SCEPTRE (VLAN vs physical Ethernet), the predicted timing differences of communicating the control signals from the PLC to actuate the immersed heaters and spray are small with practically negligible effects on the pressurizer's state variables.

2.4.Summary

This section demonstrated some of the capabilities of the LOBO NCS platform with emulated PLCs for investigating cyber vulnerabilities. The LOBO NCS is being developed at the UNM-ISNPS in collaboration with SNL with open-source emulated PLCs to be used for academic research and education as well as professional training. The versatile and modular LOBO NCS platform links physics-based Simulink models of various components in a representative PWR plant to emulated or physical PLCs in the digital I&C systems. The user-friendly graphic interface provides real-time display of the calculated state variables during nominal operation and simulated transients and when the PLCs are under simulated cyberattacks. The simulated cybersecurity events affecting the PLCs are programed using the ManiPIO cybersecurity testing and evaluation framework developed at SNL in collaboration with the

UNM-ISNPS. The testing of the Simulink physics-based models of components in a representative PWR plant linked to the emulated PLCs can be done, both independently as stand-alone programs and as parted of the integrated plant model within the LOBO NCS platform.

The fidelity of the LOBO NCS platform is demonstrated by comparing the results of a simulated transient using a physics-based Simulink model of the pressurizer linked to an emulated pressure PLC to those obtained using the DOE SCEPTRE framework at SNL. The LOBO NCS platform is used to simulate an operation transient following a 10% increase in the steam load demand. The simulated scenarios are for nominal operation of the feedwater PLC and when attacked by a simulated FDIA. This FDIA targeting the memory registers is simulated using the ManiPIO program to manipulate the PLC to thinking that the water level in the SG remains constant at its nominal steady state value. The simulated FDIA caused a significant decrease in the water level in the SG to the point for activating the safety system for actuating the Auxiliary Feedwater System.

The soundness of the architecture implemented in the LOBO NCS framework is confirmed and validated by comparing the transient simulation results to those obtained using the DOE SEPTRE framework. The simulated transients are of sequential surge-in and surge-out of water into and from the pressurizer to the hot leg of a representative PWR plant. The calculated state variable values for the physics-based pressurizer model are practically identical, despite the differences in the network architectures in conjunction with the LOBO NCS and SCEPTRE. These differences only resulted in small differences in the timing for actuating the immersed electrical heaters and the subcooled water spray in the pressurizer during the simulated transient.

3. Simulated FDIAs on Emulated and Hardware PLC

False Data Injection Attacks (FDIA) are a category of potential cyber security events that could target the PLCs in ICS in nuclear power plants and industrial and energy infrastructures. During an FDIA, a malicious program sends false data to manipulate the PLCs input or output control signals. Zhang and Coble (2020) developed and employed a toolkit for cybersecurity analysis of the digital I&C systems and investigated the effects of launching an FDIA on altering the operation of SG feedwater control PLC in a Pressurized Water Reactor (PWR) plant. They linked a Siemens S7 PLC programmed as the feedwater controller to a PWR simulator as hardware-in-the-loop. Results demonstrated that the FDIA could falsify the PLC operation to reduce the feedwater injection rate into the SG.

Alves and Morris (2018) experimentally investigated the effect of using Modbus TCP FDIA on the operation and responses of a soft PLC, developed using the OpenPLC runtime, and commercial hardware PLCs by Siemens, Allen-Bradley, Schneider-Electric, and Omron. The soft and hardware PLCs were programed with the same controller logic to monitor and count pulses of repeating sawtooth input signals. The simulated FDIA attempted to overwrite the Modbus register to hold the internal counter of the signal pulses. The PLCs responded differently to the Modbus TCP FDIA. In some cases, the FDIA was able to consistently overwrite the value for the counter. In other cases, the counter repeatedly reverted between the true and false values as the PLC and simulated cyberattack continued writing to Modbus register.

The work in this section uses the LOBO NCS platform (Fig. 2.9) to investigate the response of the pressure PLC for the pressurizer in a representative PWR plant during nominal simulated transients and when under FDIAs. The validated Simulink physics-based model of the pressurizer is linked to both an emulated PLC, based on the open-source OpenPLC runtime (Alves, et al. 2014), and a commercial hardware Allen-Bradley Micrologix PLC (Allen-Bradley 2013). The physics-based Simulink model of the pressurizer simulates an operational transient of sequential surge-in and surge-out of water from and to the hot leg of the primary coolant loop in a representative PWR plant. The connected PLCs control the water spray and the proportional and backup heaters in the pressurizer.

The FDIAs are initiated by the ManiPIO cybersecurity event generation program in the LOBO NCS platform. In the first simulated FDIA, ManiPIO program sends a false low pressure state variable to the Modbus holding registers of the PLC. In the second simulated FDIA the ManiPIO program alters the holding register of the control signal for the water spray function to prevent activating the water spray. During the simulated transients with FDIAs the responses of the emulated and commercial hardware PLCs, linked to the physics-based model of the pressurizer, are compared. These investigations are among many planned to demonstrate the capabilities of the LOBO NCS platform for assessing and quantifying the effect of simulated cybersecurity events on the operation of the digital I&C systems in a representative PWR plant.

3.1. Pressurizer Model and Pressure PLC

The Simulink physics-based model of the pressurizer divides it into three regions: an upper region of saturated vapor, a middle region of saturated liquid, and a lower surge region of subcooled liquid (El-Genk, Altamimi, and Schriener 2021). It accounts for the different physical processes taking place within the pressurizer. These include rainout, surface condensation on the spray water droplets, wall condensation, and flash evaporation into the saturated vapor region

(Fig. 2.11). The lower region of the pressurizer accommodates the water that enters following a surge-in from the hot leg of the primary loops. Energy supplied by the immersed heaters raises the enthalpy of the subcooled liquid to saturation when merging into the middle region of the pressurizer. The pressurizer model assumes the same pressure in all three regions and solves the coupled mass and energy conservation equations in these regions to calculate the system pressure and the water level in the pressurizer during nominal and transient operations. The pressurizer model also accounts for the changes in the fluid properties in all three regions of the pressurizer as functions of pressure and temperature throughout the transient simulation (International Association for the Properties of Water and Steam 2012). More details on the formulation and validation of the pressurizer model (Fig. 2.11) can be found elsewhere (El-Genk, et al. 2020a; El-Genk, Altamimi, and Schriener 2021).

In simulated FDIAs, the pressurizer Simulink model runs as a stand-alone program and is decoupled from the integrated PWR plant model. The water temperatures in the hot and cold legs of the plant are specified in the input to the pressurizer model as functions of time. The thermophysical properties of the surge-in water into the pressure are evaluated at hot-leg temperature. The properties of the subcooled water to the spray nozzle at the top of the pressurizer (Fig. 2.11) are evaluated at the cold leg temperature. This nozzle sprays water droplets into the vapor region of the pressurizer when there is an increase in system pressure. The pressure relief valve opens intermittently to help restore the pressure when the system pressure continues to increase past a preprogramed setpoint, despite the water spray.

Table 3.1. Representative PWR pressurizer design and operating parameters in present analyses.

Parameter	Value	Parameter	Value
Nominal pressure, MPa	15.5	Max. water spray rate, m^3/s	0.0443
Total internal volume, m^3	59.46	Proportional heaters power, kW_{th}	370
Nominal water fill, m^3	28.3	Backup heater power, kW_{th}	1,230
Wall inner diameter, m	2.54	Relief valve setpoint, MPa	17.237
Wall outer diameter, m	2.794	Spray upper setpoint, MPa	15.858
Overall height, m	12.776	Spray lower setpoint, MPa	15.686
Strait section height, m	9.98	Proportional heaters upper setpoint, MPa	15.686
End dome radius, m	1.397	Proportional heaters lower setpoint, MPa	15.340
Surge line length, m	25.39	Backup heater on setpoint, MPa	15.168
Surge line mean dia., m	0.4572	Backup heater off setpoint, MPa	15.340

The pressure PLC regulates the system pressure by controlling the rate of water spray, the electrical power to the immersed proportional and backup heaters (Fig. 2.11), and the opening and closing of the pressure relief valve. The PLC receives the system pressure calculated by the Simulink model of the pressurizer via the LOBO NCS data transfer and communication interfaces. It transmits back the control signals to adjust the various functions in the pressurizer. The calculated system pressure is compared within the PLC's logic to the preprogramed pressure setpoints for the various control functions (Fig. 3.1, Table 3.1). When the pressure increases past the preprogramed high setpoint of 15.686 MPa, the spray nozzle increases the rate of water spray into the vapor region of the pressurizer, commensurate with the increase in pressure. The water spray nozzle is fully open when the system pressure reaches 15.858 MPa. The rate of water spray in the pressurizer model reaches 0.0443 m^3/s when the spray valve is fully open. Conversely, when the pressure decreases below a setpoint of 15.686 MPa for the controllers of the proportional heaters, the PLC increases the electrical power to the heaters commensurate with the decrease in pressure until reaching 15.340 MPa (Table 3.1). The maximum power to the proportional heaters is set at 370 kW_{th}.

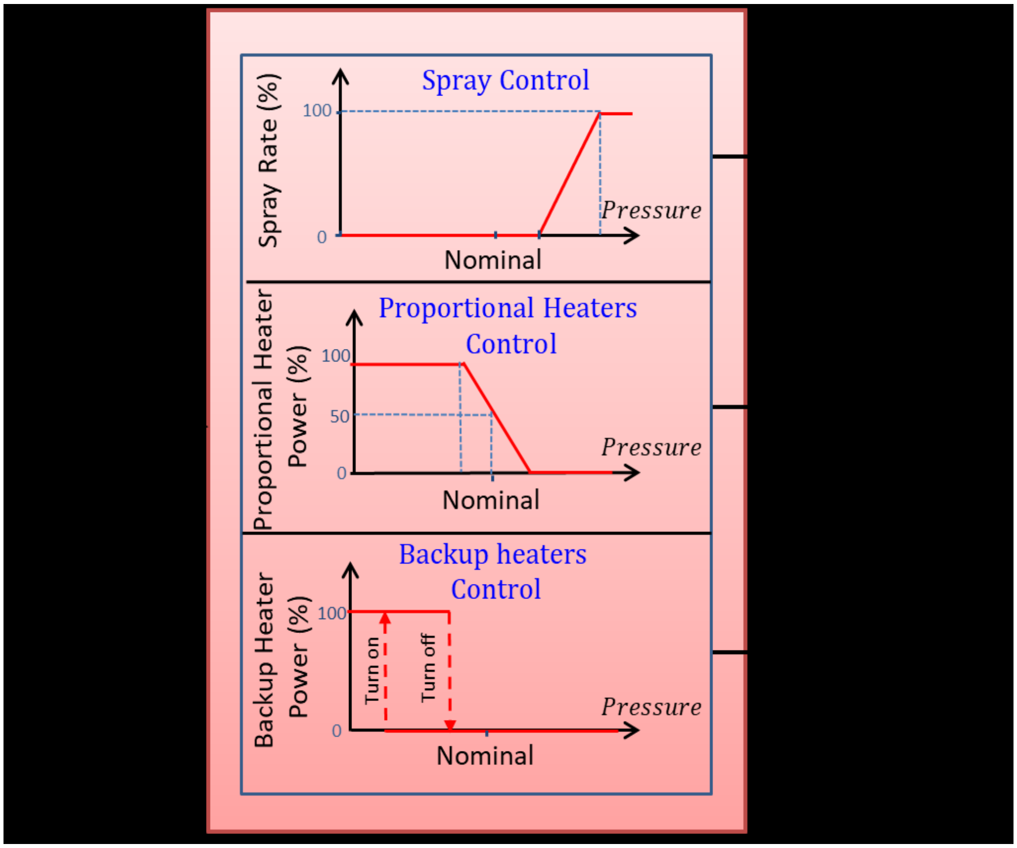


Fig. 3.1. Pressure PLC control of the spray nozzle, and proportional and backup heaters (El-Genk, et al. 2020a; El-Genk, Altamimi, and Schriener 2021).

When the system pressure continues to decrease below the low setpoint, the PLC turns on the backup heaters to increase flash operation into the top vapor region (Fig. 2.11) to help restore the system pressure. The backup heaters supply 1,230 $kW_{th,}$ and unlike the proportional heaters, operate binary either fully on or fully off. The backup heaters are programed to turn on when the system pressure reaches or decreases below a setpoint of 15.168 MPa and remains on until the pressure increases above an upper setpoint of 15.340 MPa (Table 3.1 and Fig. 3.1). The control logic of the pressure PLC in Fig. 3.2 is implemented for the emulated and commercial hardware PLCs investigated in the present analyses. Both PLCs are programed with identical logic.

The emulated PLC with an open-source architecture uses the OpenPLC runtime software

(Alves et al., 2014) within a Raspian OS virtual machine. It compiles and runs programs written in the IEC 61131-3 standard structured text PLC programming language. The virtual machine uses the VMWare virtualization software (VMware 2019) on a Windows 10 computer server. Communication with the OpenPLC runtime is accomplished using the Modbus TCP protocol. The other PLC implemented in the present simulations is a commercial Allen-Bradley (A-B) Micrologix L33ER PLC with ProSoft MVI69E-MBTCP module to support Modbus TCP communication (Allen-Bradley 2013). The ProSoft module interfaces with the Allen-Bradley's processor module through the PLCs backplane.

Both PLCs are configured with one Modbus holding register for the system pressure value, and four holding registers for the control signals for the various pressurizer functions (water droplets spray, proportional heaters, backup heaters, and relief valve). The data broker and the communication interface write the pressure state variable generated by the pressurizer Simulink model to the input register and returns the control signals in the four output registers back to the model from the PLCs (Fig. 2.9). The emulated PLC with OpenPLC and the Allen-Bradley physical PLC use a 2.0 ms scan time and the Simulink model of the pressurizer uses a simulation timestep of 10 ms. With the emulated PLC, the server running the virtual machine is connected to the testing network. The Allen-Bradley Micrologix is connected through the ProSoft module to the LOBO NCS network as hardware-in-the-loop.

3.2. Results and Discussion

This section compares the results of simulated transients of the physics-based Simulink model of the pressurizer linked to both emulated and physical hardware pressure PLCs. The simulated transients involving sequential surge-in and surge-out of water into and from the pressurizer into the hot leg of the primary loop of a representative PWR plant. The obtained results are of normal transient operation of the PLCs and when they are subject to simulated False Data Injection Attacks (FDIAs) generated by the ManiPIO program (Fig. 2.9). The next subsection presents the obtained results with the PLCs operating nominally.

3.2.1. Simulated Transient Results with Nominal Operating PLCs

The emulated and the commercial Allen-Bradley PLCs are first tested separately to determine their response during nominal operating conditions and when linked to the pressurizer's physics-based Simulink model in the LOBO NCS platform. The emulated PLC using the OpenPLC runtime in a virtual machine generates indistinguishable results from those of the commercial Allen-Bradley Micrologix PLC connected as hardware-in-the-loop (Schriener & El-Genk 2021). The simulated transient starts at t = 0 s with the pressurizer operating at steady state conditions of system pressure of 15.686 MPa, water level in the pressurizer of 4.22 m, and hot leg water temperature of 564.8 K. The surge-in of water from the hot leg into the pressurizer starts at t = 100 s (point 1 in Fig. 3.2) at the rate increase linearly to 25 kg/s (point 2 in Fig. 3.2) over a period of 50 s. The surge-in rate is then held steady at 25 kg/s for 100 s (point 3 in Fig. 3.2) before decreasing linearly to 0 kg/s over a period of 50 s (point 4 in Fig. 3.2).

The surge-in raises the water level in the pressurizer and compresses the vapor in the upper region (Fig. 2.11), which in turn increases the system pressure (Figs. 3.2b and 3.2c). In response to the increase in the system presure, the PLCs increase the spray rate of the water droplets into the upper vapor region of the pressurizer (Fig. 3.1). The ensuing vapor condensation onto the water droplets surface decreases the system pressure (Fig. 3.2c). During the progression of the surge-in event, the pressure PLC increases the spray rate of the water droplets to a peak value of 31 kg/s at t = 235 s. After that, the spray rate decreases to zero as the system pressure drops below the setpoint for opening the spray nozzle (Fig. 3.2c). The water level in the pressurizer increases due to the surge-in of water from the hot-leg and the injected water through the spray nozzle.

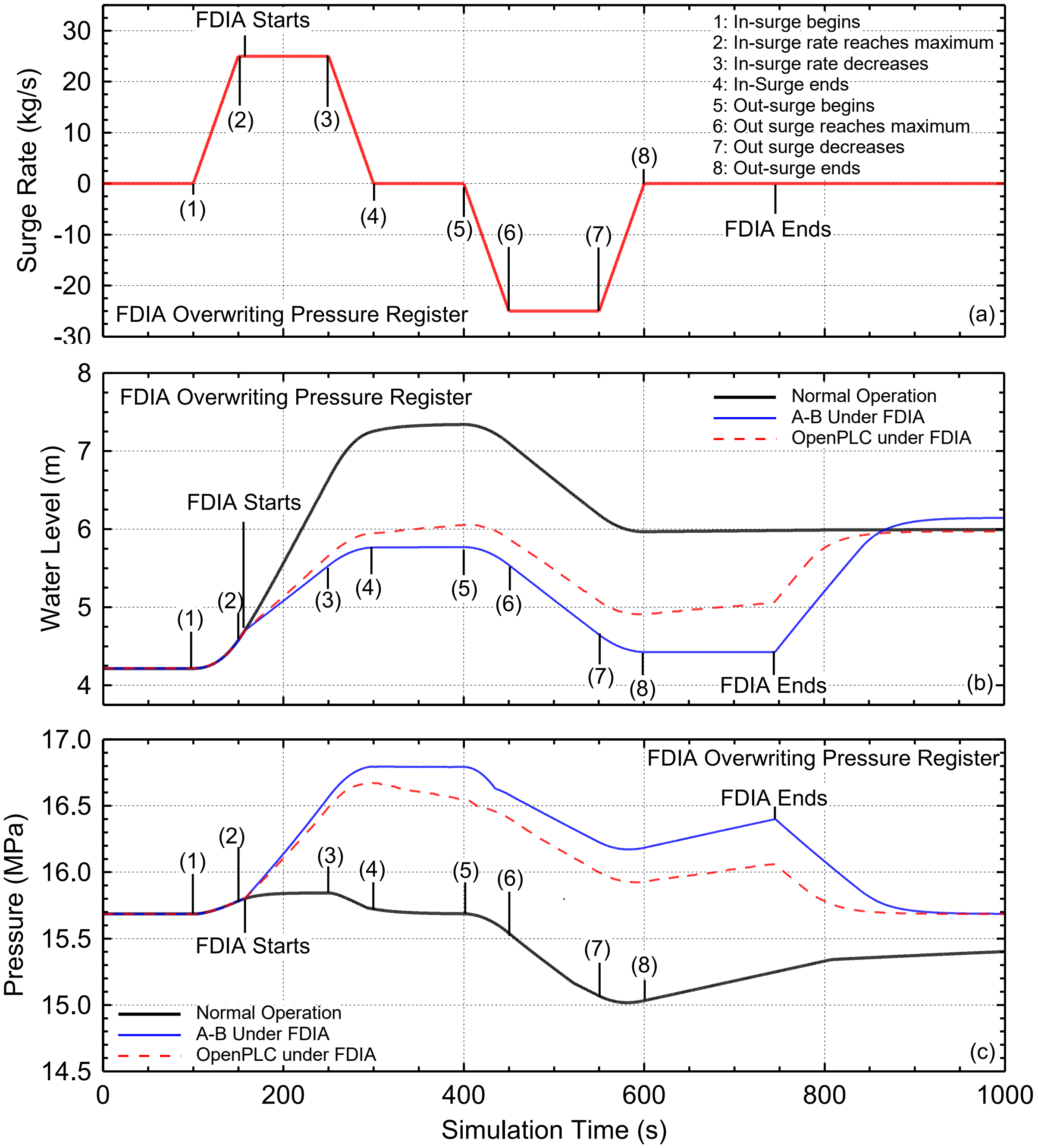


Fig. 3.2. Simulated transient results of sequential surge-in and surge-out during normal operation of the PLC and when targeted by simulated FDIA writing to the system pressure registers.

The sequential surge-out of water from the pressurizer into the hot leg begins at t = 400 s of the simulated transient (point 5 in Fig. 3.2). The surge-out rate increases linearly from 0 kg/s to 25 kg/s over a period of 50 s (point 6 in Fig. 3.2). It then remains steady at 25 kg/s for 100 s (point 7 in Fig. 3.2a), before decreasing linearly to 0 kg/s over a period of 50 s (point 8 in Fig. 3.2). The surge-out decreases the water level in the pressurizer (Fig. 3.2b), and the resulting expansion of the vapor in the top region of the pressurizer (Fig. 2.11) causes the system pressure to decrease (Fig. 3.2c).

When the pressure drops below the setpoint to turn on the proportional heaters, the PLC increases the electrical power to the heaters to increase the rate of flash evaporation into the top vapor region (Fig. 2.11) and hence increases the system pressure (Fig. 3.2c). However, the rapid surge-out of water from the pressurizer into the hot leg causes the pressure to continue to decrease even after the power of the immersed proportional heaters maxims at 370 kW_{th} (Table 3.1). The backup heaters switch on when the pressure reaches the on setpoint, supplying an additional 1,230 kW_{th} to increase flash evaporation into the vapor region of the pressurizer. The backup heaters stay on until the pressure reaches the setpoint to turn them off. In the meantime, the proportional heaters continue to support flash evaporation, slowly increasing the pressure until it reaches a new steady state level.

Following the end of the water surge-out phase of the simulated transient, the water level in the pressurizer reaches a steady state level higher than the initial value at the start of the simulated transient (Fig. 3.2b). During the simulated sequential surge-in and surge-out equivalent masses of water enters and leave the pressurizer, respectively. The difference in the steady state water levels before and after the simulated sequential surge-in and surge-out transient is due to the injected water spray during the surge-in phase.

3.2.2. Simulated Transient Results with PLCs under False Data Injection Attacks

The results presented in this subsection are of the responses of the pressurizer model with the emulated and commercial hardware PLCs are under a simulated False Data Injection Attack (FDIA) sending a false pressure value. The ManiPIO program in the LOBO NCS platform simulates a FDIA on the holding register of the PLCs by falsifying the input pressure state variable within the control logic. The FDIA is tested for both the pressure control program configured on both the Allen-Bradley (A-B) Micrologix PLC and the emulated PLC with OpenPLC. The Simulink pressurizer model is used to simulate the same sequential surge-in and surge-out transients described earlier (Fig. 3.2a).

The FDIA starts shortly after the surge-in rate reaches its highest value. It writes a false pressure of 15.0 MPa to the Modbus input holding register associated with the system pressure state variable. At this pressure, the logic programming of the PLCs would signal the proportional heaters to operate at maximum power and the backup heaters to turn on (Table 3.1). The FDIA continues to overwrite the register throughout the durations of the simulated surge-in and surge-out events (Fig. 3.2a). When the FDIA ends, the pressure PLC returns to normal operation state, receiving the correct pressure value, and attempts to restore the system pressure to the value defined by pre-programmed pressure setpoints (Table 3.1).

The simulation results in Figures 3.2 - 3.5 show that the FDIA successfully alters the response of the PLCs compared to nominal operation. Overwriting the pressure holding register causes the logic programing of the PLCs to change the control signals to both the water spray nozzle and the proportional and backup heaters. This in turn changes the water level and the system pressure. Prior to introducing the FDIA, the emulated and hardware PLCs produce identical responses to the water surge-in by increasing the rate of the spray water droplets into the vapor region of the pressurizer (Fig. 2.11) commensurate with the increase in the system pressure (Fig. 3.2c). The rates of the water surge-in and water droplets spray rate initially increase the water level in the pressurizer (Fig. 3.2b). When the FDIA starts injecting a false low-pressure value, the PLCs respond by prematurely closing the water spray nozzle (Fig. 3.3b-c), raising the electrical power to the proportional to their maximum, and turning on the backup heaters (Fig. 3.4a-c and 3.5a-c).

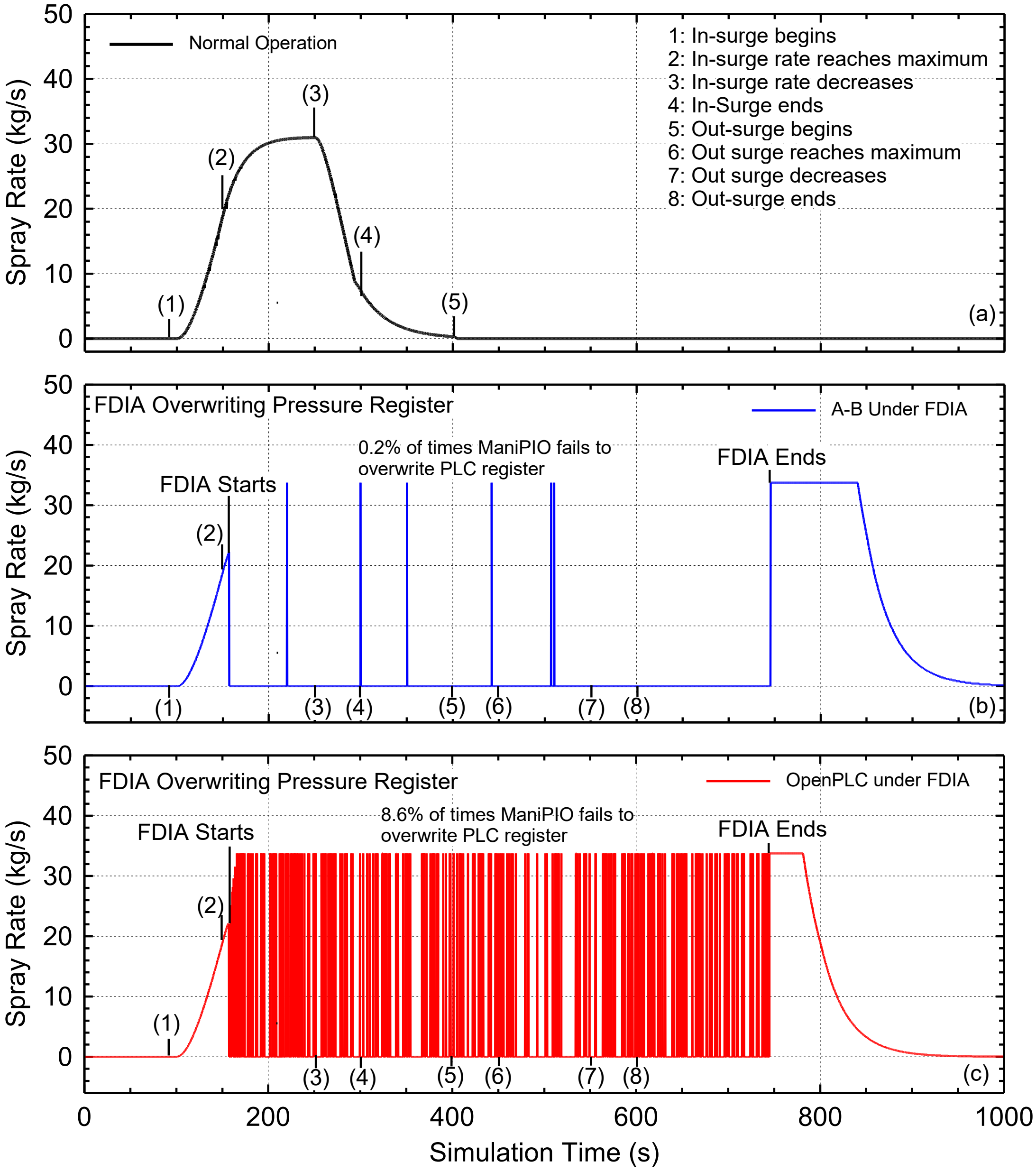


Fig. 3.3. Results of water spray function with Allen-Bradley hardware PLC and emulated PLC with OpenPLC during normal operation and when under FDIA targeting the system pressure registers.

The manipulation of the PLCs significantly increases the system pressure compared to its value during normal operation (Fig. 3.2c). The pressure peaks at 16.8 MPa with the Allen-Bradley PLC, and up to 16.7 MPa with the emulated PLC, compared to a maximum value of 15.8 MPa during nominal operation. The combination of increased pressure and reduced water droplets spray into the pressurizer when the PLCs are under a FDIA slows the increase in the water level in the pressurizer, compared to that during normal operation. During nominal operation, the water level in the pressurizer peaks at 7.34 m, compared to 5.94 m and 5.78 m when the Allen-Bradley and the emulated PLCs are subject to the simulated FDIA (Fig. 3.2b)

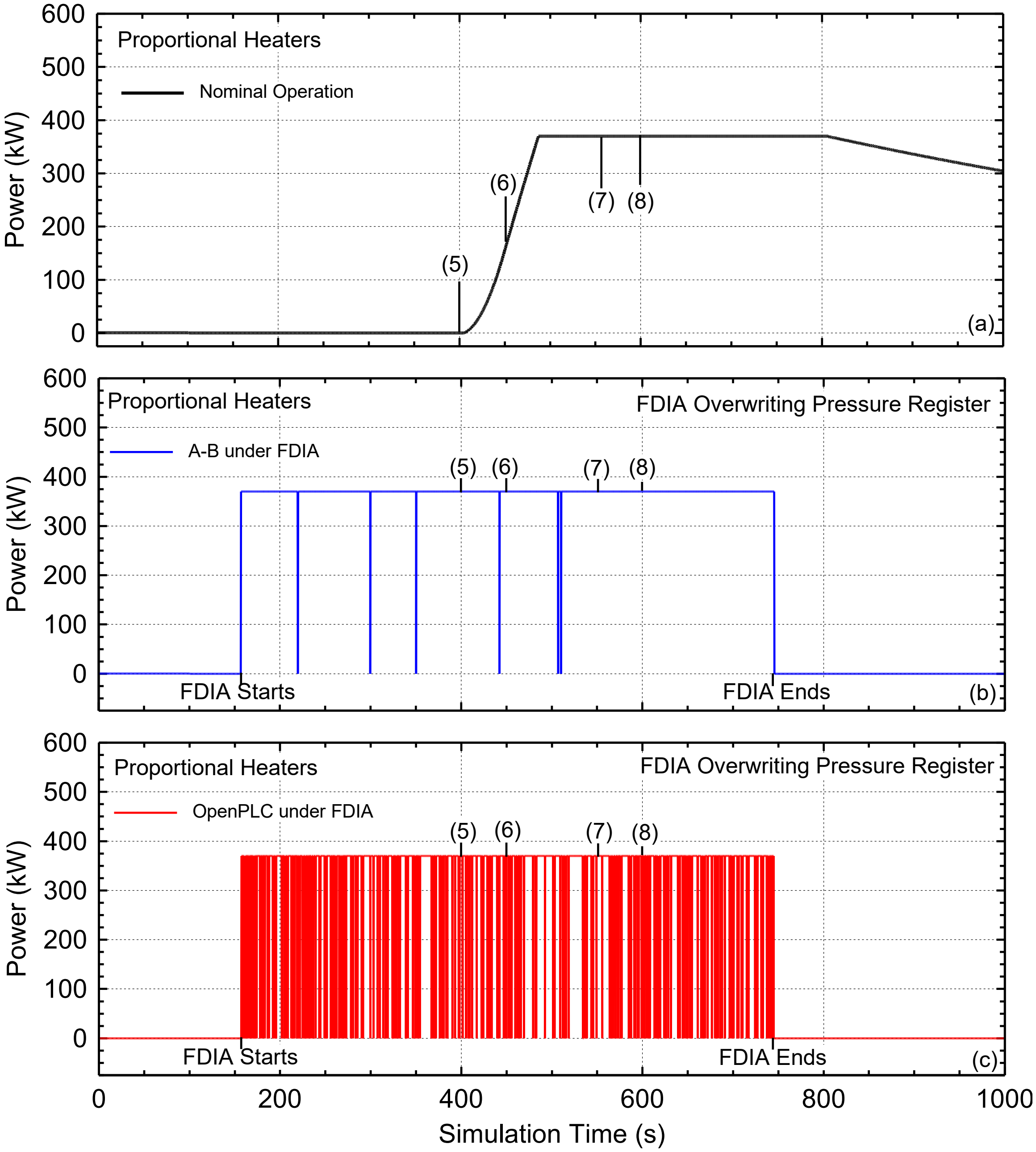


Fig. 3.4. Proportional heaters control functions for Allen-Bradley hardware and emulated PLC during normal operation and when under FDIA targeting the system pressure registers.

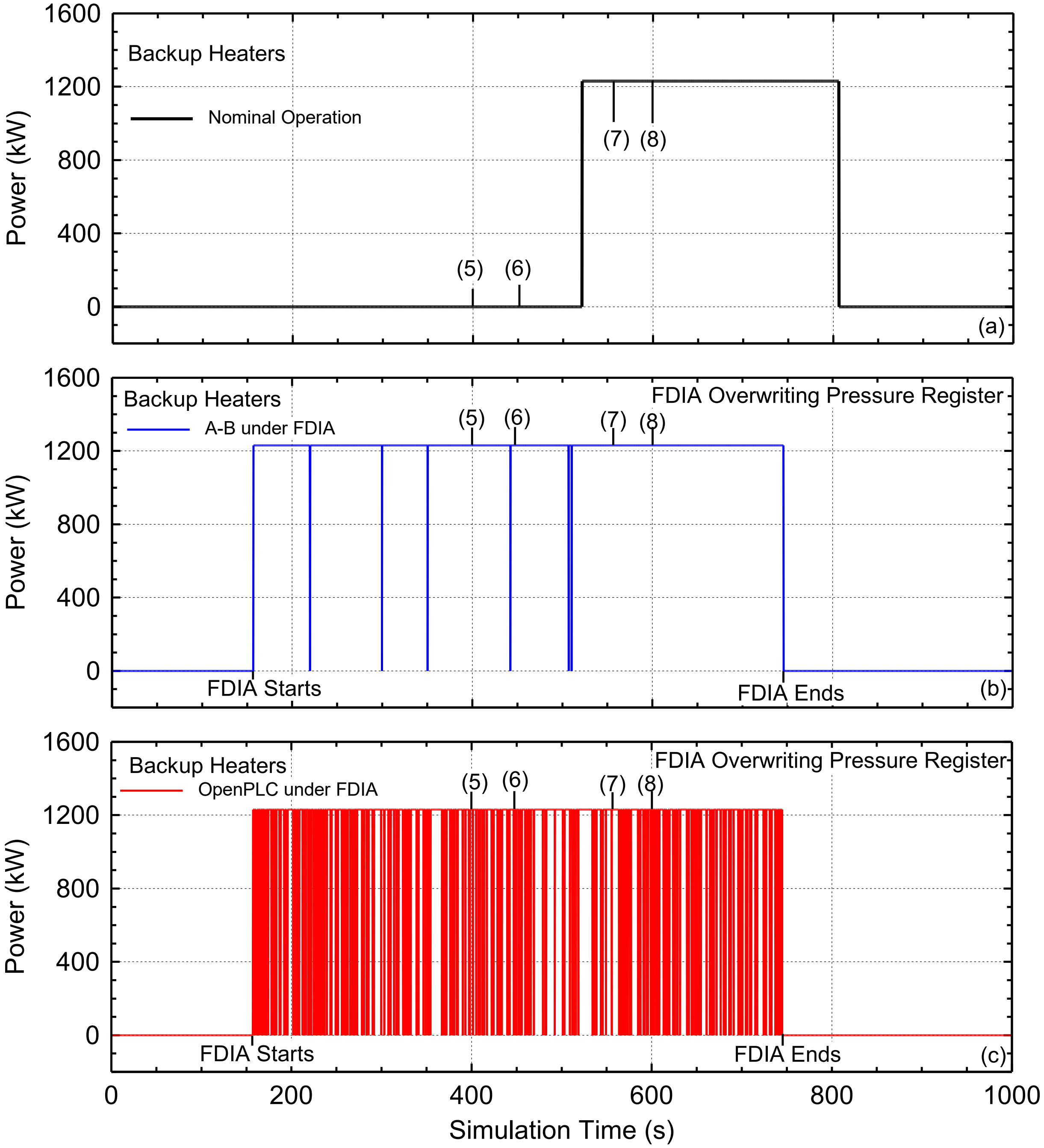


Fig. 3.5. The backup heater control function with Allen-Bradley hardware and the emulated PLCs during normal operation and when under FDIA targeting the system pressure registers.

During the FDIA, the ManiPIO program repeatedly overwrites the input register of the PLCs for the system pressure to force them to falsely operate the proportional heaters at their maximum power and turn on the backup heaters. This is while the LOBO NCS data broker and the communication program are competing to write the actual pressure value to the same Modbus holding register. At a few instances during the simulated FDIA, the PLCs manage to indicate the real pressure despite the attempts by the ManiPIO program to overwrite it. This response can be seen for the Allen-Bradley PLC in Figs. 3.3b, 3.4b, and 3.5b and for the emulated PLC with Open PLC in Figs. 3.3c, 3.4c, and 3.5c as series of vertical spikes. In response to the false high pressure the PLCs signals to turn off the immersed electrical heaters (Figs. 3.4b-c and 3.5b-c) and open the water droplets spray nozzle (Figs. 3.3b-c). When ManiPIO once again overwrites the register, the PLCs closes the water droplets spray nozzle and turns the proportional and backup heaters back on (Figs. 3.4b-c and 3.5b-c). The delineated spiking in these figures is like that observed by Alves, et al. (2018) in their experiments.

The simulated FDIA successfully overrides the pressure holding register of the Allen-Bradley PLC 99.8% of the time, with the true pressure value getting through only 0.2% of the simulation timesteps (Figs. 3.3b, 3.4b, 3.5b). The short duration of the spikes with the Allen-Bradley PLC causes little change in the system pressure and the water level in the pressurizer (Figs. 3.2b-c). The emulated PLC using OpenPLC shows more inconsistency in mitigating the ManiPIO program attempts to overwrite the Modbus input register for the system pressure (Figs. 3.3c, 3.4c, 3.5c). Unlike the Allen-Bradley PLC, the emulated PLC repeatedly turns the heaters and the water spray off and on while under the simulated FDIA. The holding registers of the emulated PLCs successfully overwritten the system pressure 91.4% of the time, with the true pressure value getting through more frequently ~ 8.6% of time (Figs. 3.3c, 3.4c, 3.5c). The greater number of successful actuations of the water droplets spray with the emulated PLC while under the simulated FDIA results in lower pressure and higher water level in the pressurizer than those with the pressurizer Simulink model linked to the Allen-Bradley PLC (Figs. 3.2b-c).

The differences in the responses of the two PLCs when under the simulated FDIA could be attributed to differences in the communication and timing protocols for the two PLCs. The emulated PLC with OpenPLC relies on an emulated network connection that passes through the network adapter of the server node running the virtual machines. The OpenPLC runtime has a software network communication module that handles the Modbus TCP communication on its open comm port (Alves, et al. 2014).

On the other hand, the Allen-Bradley PLC uses the attached ProSoft module to handle the Modbus TCP communication with the data broker and ManiPIO (Allen-Bradley 2013). This module passes the values of the written state variables and control signals to and from the processor module of the PLC across the backplane on regular scheduled intervals during the scan cycle (Allen-Bradley 2013). The more regular scheduled action of the commercial-grade hardware PLC to the Modbus TCP traffic would explain the relatively consistent response of the Allen-Bradley PLC under the FDIA initiated by the ManiPIO program.

When the FDIA ends at t = 747s in the simulated surge-in and surge-out transient, the pressure PLC returns to normal operation and the controller turns off the proportional and backup heaters (Figs. 3.4b-c and 3.5b-c). In response to the true high system pressure the PLC also increases the water droplets spray rate to reduce the pressure (Figs. 3.3b-c). The system pressure decreases slowly due to the condensation of vapor onto surface of the injected spray water droplets. It eventually levels off at a lower steady state value (Fig. 3.2c).

The presented results show that the simulated FDIA successfully alters the operation of both the emulated PLC and the commercial Allen-Bradley PLC during most of the attack period. The suppression of the emulated PLC with OpenPLC is less consistent than of the Allen-Bradley PLC (91.6% compared to 99.8%). However, it still sufficient to cause a significant increase in the system pressure during the simulated transient when the PLCs are under the simulated FDIA.

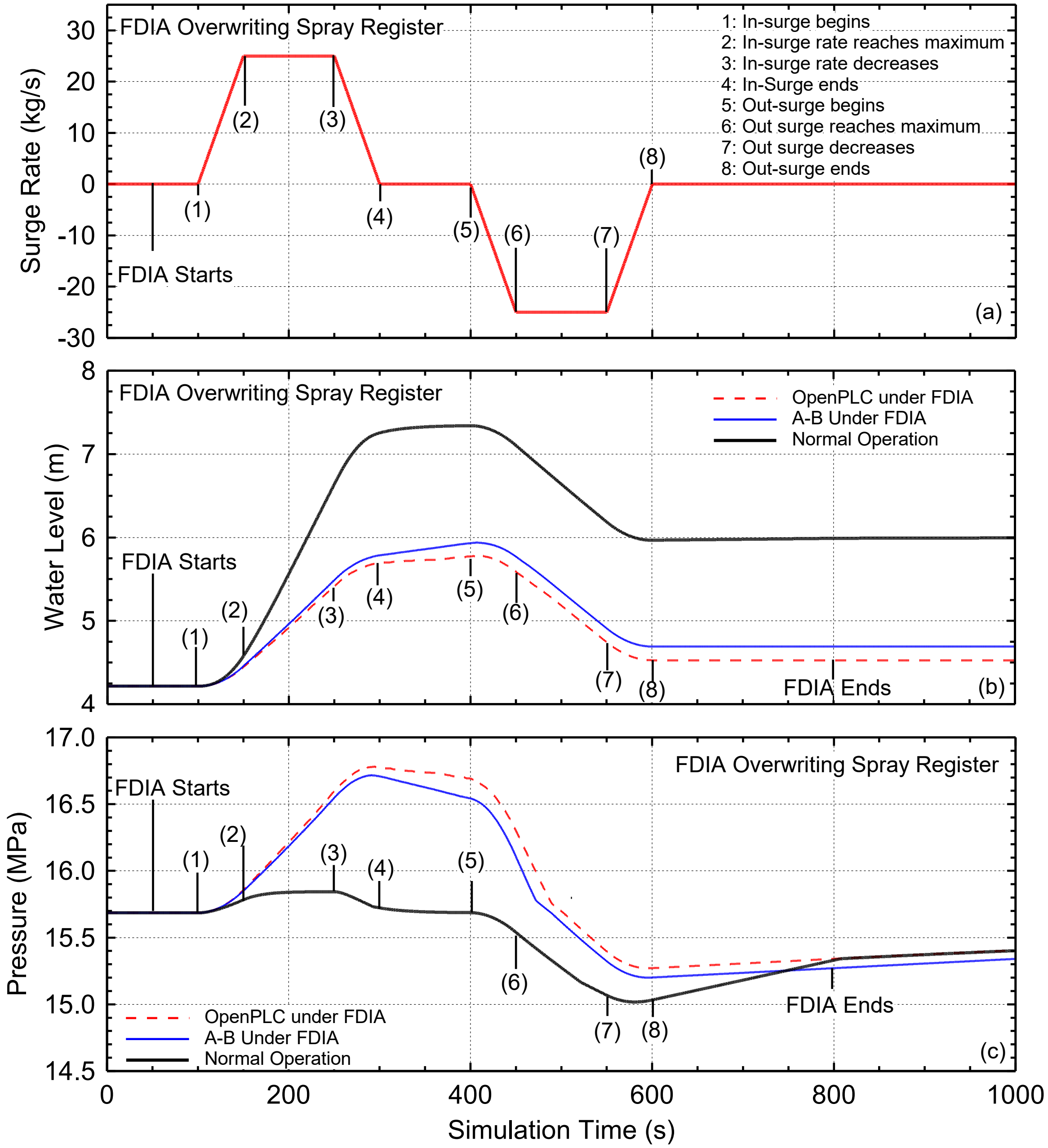


Fig. 3.6. Simulated transient of sequential surge-in and surge-out events during normal operation and when PLCs are under a FDIA targeting the water spray control function.

3.2.3. Responses of PLCs under a False Data Injection to Water Spray Holding Register

In the second FDIA investigated, the ManiPIO program overwrites the Modbus holding registers of the emulated and hardware PLCs to alter the control signal to the water spray nozzle in the pressurizer (Fig. 2.11). The presented results are of the Simulink model of the pressurizer during the same simulated transient of the sequential surge-in and surge-out, described earlier (Fig. 3.2a). The simulated FDIA to alter the control signal of the water spray nozzle starts at t =

50 s, before the surge-in event (Fig. 3.6a). The ManiPIO program writes zero water spray rate (0.0 kg/s) to force keeping the water spray nozzle closed. In so attempting, the FDIA causes the system pressure to increase rapidly during the simulated surge-in of water from the hot leg. The FDIA ends at t = 800 s of the simulated transient and the PLC returns to its normal operating state (Figs. 3.6a-c).

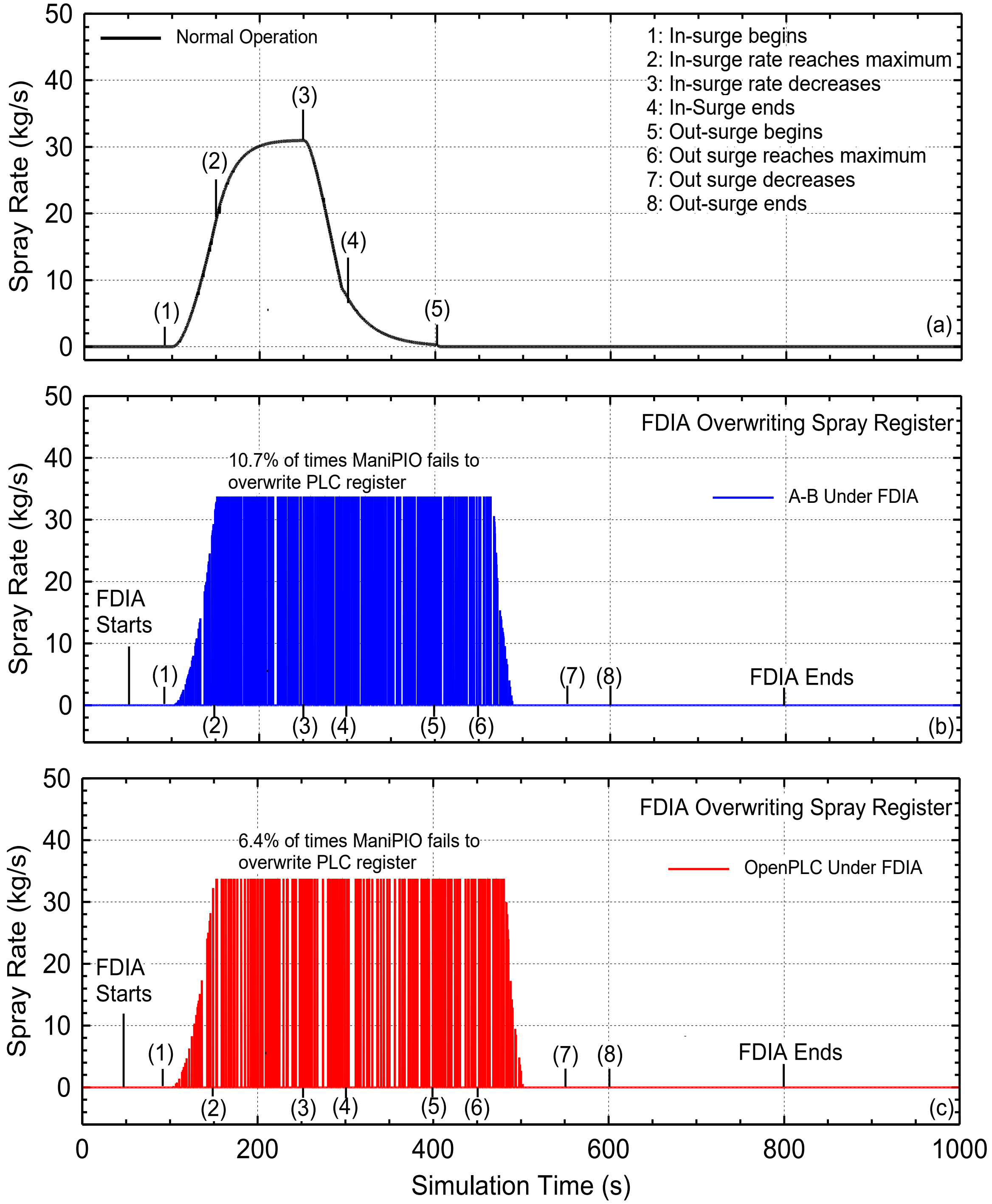


Fig. 3.7. Responses of the Allen-Bradley hardware PLC and the emulated PLC during normal operation and while under an FDIA targeting the water spray control function.

Figures 3.6 - 3.8 compare the responses of the emulated open PLC and the Allen-Bradley hardware PLC while under the simulated FDIA and during nominal operation. During the simulated surge-in transient the simulated FDIA disrupts the function of the water droplets spray, increasing the system pressure beyond the maximum value of 15.8 MPa (Table 3.1) when the PLCs are operating nominally (Figs. 3.6c). With the Allen-Bradley PLC under the simulated FDIA the pressure peaks at 16.7 MPa compared to 16.8 MPa with the emulated PLC. The suppressed water spray significantly reduces the water level in the pressurizer compared to that during nominal operation of the PLCs (Fig. 3.6b). With the Allen Bradley PLC the water level peaks at 5.94 m, compared to 5.78 m with the emulated PLC, and 7.34 m when both PLCs are operating normally.

The PLCs continue to normally control the proportional and backup heaters throughout the simulated transient. This is because the simulated FDIA only targets the holding register for the water spray into the pressurizer (Fig. 2.11). With nominal operation of the PLCs, they increase the power to the proportional at the start of the surge-out from the pressurizer to the hot leg, t = 400 s (Fig. 3.8a). When the PLCs are under the simulated FDIA (Fig. 3.6c), the resulting higher system pressure at the start of the surge-out event delays activating the proportional heaters (Figs. 3.8b and c). In addition, the system pressure does not decrease to the setpoint for turning on the backup heaters (Fig. 3.8d and Table 3.1).

The differences in the responses of the Allen-Bradley hardware and the emulated PLCs during the simulated FDIA targeting the water spray function (Figs. 3.5 - 3.8) are relatively smaller than those during the simulated FDIA targeting the system pressure (Fig. 3.2). Results presented in Fig. 3.7a-c show that for the Allen-Bradley PLC the simulated FDIA prevents actuating the water spray function 89.3% of the time. The control signal determined by the logic programming of this PLC reaches the true output 10.7 % of the time (Fig. 3.7b). For the emulated open PLC, the simulated successfully prevented the actuation of the water spray 93.6 % of the time during the surge-out phase of the simulated transient (Fig. 3.7c).

Consequently, with the Allen Bradley PLC under the simulated FDIA the system pressure increases beyond that for nominal operation to 16.7 MPa and to 16.8 MPa with the emulated open PLC. Disabling the water spray function decreases the water level in the pressurizer compared to nominal by 1.40 m and 1.65 m with the Allen-Bradley PLC and the emulated open PLC under attach, respectively. The simulated FDIAs targeting the output control signal of the water spray function with both the Allen-Bradley and emulated open PLC are relatively less disrupting of the operation of the PLCs, compared that the FDIAs falsifying the input state variables. The holding registers for the state variables are updated once every simulation timestep. However, holding registers for the output control signals are updated more frequently, once every 2 ms scan cycle. Frequent updates are more challenging because they cause a race condition between the ManiPIO program and the PLCs, which decreases the percentage of times the Modbus holding register is successfully altered.

The presented and discussed simulation results in this section demonstrate the capability of LOBO NCS platform to investigate the effects of cyber-compromises on the response of the PLCs of the pressurizer in a representative PWR plant. The developed and implemented ManiPIO program simulate FDIAs that successfully manipulate the response of both the Allen-Bradley hardware and the emulated open PLCs. The simulated FDIAs target the system pressure and the water spray function. They either change the input state variables to the Modbus holding registers or overwrite the registers for the output control signals. Additional FDIAs simulations are planned, which would target PLCs for the SG, the primary pumps, and the reactor control.

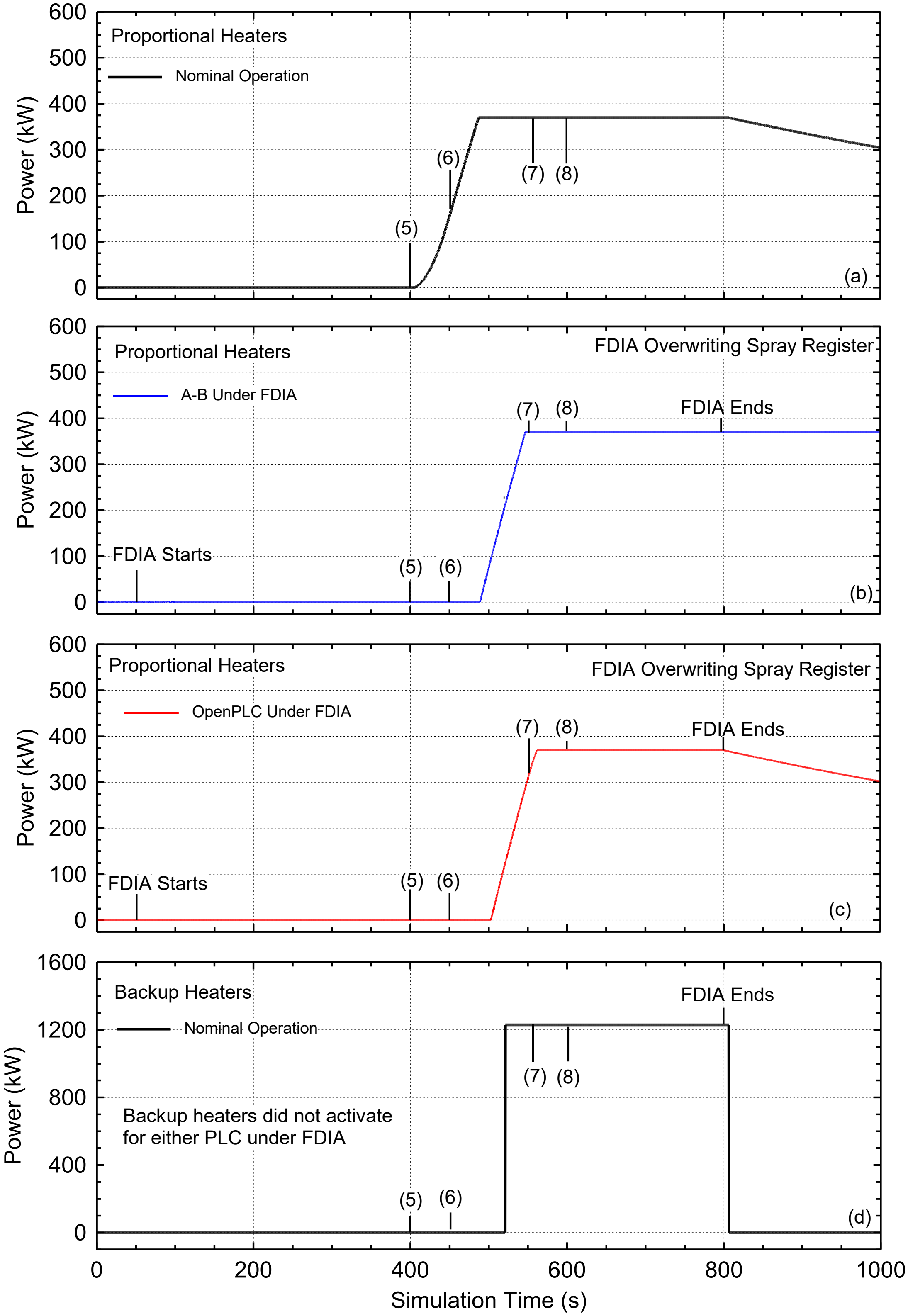


Fig. 3.8. Functions of the heaters controlled by the Allen-Bradley hardware PLC and emulated OpenPLC during normal operation and under an FDIA targeting the water spray control function.

Results show that the simulated FDIA overwriting the holding register for the system pressure PLCs successful forces them to shut off the water spray, increase the power to the proportional heaters and turn on the backup heaters. The initiated FDIA overwrites the holding register for the pressure 99.8% of the time with the Allen-Bradly PLC and 94.1% of the time with the emulated open PLC. Consequently, the system pressure increased by ~ 1 MPa to 16.8 MPa with the Allen-Bradley PLC and to 16.7 MPa with the emulated open PLC, compared to only 15.8 MPa during normal operation.

The simulated FDIA to overwrite the holding register for the water spray control signal successfully disabled the water spray into the pressurizer during the simulated surge-in and surge-out transient. The water spray function disabled 89.3 % of the time with the Allen-Bradley and 93.6 % of the time with the emulated open PLC. This caused the system pressure to increase beyond that for nominal operation to 16.7 MPa with the Allen Bradley PLC and 16.8 MPa with the emulated open PLC. The differences in the frequencies of the PLCs to update their output control values likely account for the relatively lower overwrite successes for the second FDIA scenario targeting the water spray function compared to the first targeting the system pressure.

4. Summary and Conclusions

This report details the work performed for Technical Task 6 to develop and demonstrate a cybersecurity testing and evaluation framework as part of the Nuclear Instrumentation & Control Simulation (NICSim) platform project. This platform is being developed at the University of New Mexico, in collaboration with Sandia National Laboratory under a DOE NEUP 2018 award. It describes and demonstrates the capabilities of the LOBO Nuclear CyberSecurity (LOBO NCS) platform and Manipulate Process I/O (ManiPIO) cybersecurity testing and evaluation program. The versatile and modular LOBO NCS platform is based on the NICSim architecture with open access capabilities for academic education and professional training. Both platforms link physics-based Simulink models of various of a representative PWR plant and components to the corresponding emulated and/or physical PLCs in the digital I&C systems. The user-friendly graphic interface in LOBO NCS provides real-time display of the calculated state variables during simulated transient operations and when the PLCs are the target of simulated cyber-attacks. Simulated cybersecurity events affecting the PLCs are programed using the ManiPIO cybersecurity testing and evaluation program developed at SNL. This report presents results demonstrating the fidelity of the LOBO NCS platform during a simulated FDIA on the system pressure PLC. The obtained results of the simulated transient of sequential surge-in and surge-out events using the physics-based Simulink model of the pressurizer and the emulated pressure PLC are in good agreement with those obtained using the DOE SCEPTRE framework at SNL.

The transient results of simulating sequential surge-in and surge-out events of the pressurizer using the DOE SEPTRE framework confirm the accuracy and validate the soundness of the architecture implemented in the LOBO NCS platform. The transient values of the water level in the pressurizer and of the system pressure are practically identical. The differences in the network architectures used in conjunction with the LOBO NCS and SEPTRE result in small differences in the timing for actuating the immersed electrical heaters and subcooled water spray in the pressurizer during the simulated transient. Such differences, however, are inconsequential to the transient response and operation of the pressurizer.

A series of simulated cybersecurity events on the PLCs coupled to the developed physics-based Simulink models of a PWR plant components are investigated. The results successfully demonstrated the capabilities of the LOBO NCS platform and ManiPIO program. The first simulated transient is of the Simulink steam generator model linked to an emulated feedwater PLC following a 10% increase in steam load demand. Obtained results are for nominal operation of the PLC and when it is under a simulated FDIA are compared. The simulated FDIA on the memory registers of the PLC attempts to manipulate it into thinking that the water level in the downcomer of the SG remained falsely constant. During nominal transient operation of the emulated feedwater PLC, the water level remains to within 0.9% of its initial steady state by adjusting the feedwater rate commensurate with the steam load demand. When under a simulated FDIA, the emulated PLC could not maintain the feedwater commensurate with the increase in the steam load demand. Consequently, the water level in SG decreased to the point to activate the Auxiliary Feedwater Actuation System.

The LOBO NCS platform is also used to investigate a simulated transient involving sequential surge-in and surge-out of water into the pressurizer from and to the hog leg. The calculated responses are compared of an emulated PLC using OpenPLC and a commercial hardware PLC both configured to function as the pressure PLC. The ManIPIO program is used to simulate FDIAs targeting the holding registers of the system pressure and the water spray. The first simulated FDIA overwrites the value of the system pressure to the holding registers of the PLCs forcing them to falsely increase the power to the immersed proportional heaters to the peak value and turn on the backup heaters. The simulated FDIA by the ManiPIO program overwrites the holding register for the pressure 99.8% of the time with the Allen-Bradly PLC and 94.1% of the time with the emulated PLC. This FDIA increases the system pressure to 16.8 MPa with the Allen-Bradley PLC and to 16.7 MPa with the emulated open PLC, compared to 15.8 MPa during normal operation. The FDIA shutting off the water spray caused the water level in the pressurizer with the Allen-Bradley PLC and the emulated PLC to be 1.55 m and 1.05 m lower than normal, respectively.

The second simulated FDIA overwrites the holding register for the water spray control signal to disable the water spray into the pressurizer during the simulated surge-in and surge-out transient. This FDIA successfully disabled the water spray 89.3 % of the time with the Allen-Bradley and 93.6 % of the time with the emulated PLC. Consequently, the system pressure increased beyond nominal to 16.7 MPa with the Allen Bradley PLC and 16.8 MPa with the emulated PLC. Disabling the water spray function also decreases the water level in the pressurizer compared to nominal by 1.40 m with the Allen-Bradley PLC and 1.56 m with the emulated PLC.

The simulated FDIA of holding the output control signal of the water spray function with both the Allen-Bradley and the emulated PLC is relatively less disrupting to the operation of the PLCs, compared to the FDIA targeting the input state variables. The holding registers for the state variables are updated once every simulation timestep, while the holding registers for the output control signals are updated more frequently, once every 2 ms scan cycle. The frequent updates are more challenging as they create a race condition between the ManiPIO program and the PLCs, which decreases the percentage of successfully altering the Modbus holding register.

The presented and discussed simulation results in this report demonstrate the capability of LOBO NCS platform simulating and investigating cyber compromises of the PLCs in a representative PWR plant. The developed and implemented ManiPIO program successfully manipulates the responses of the Allen-Bradley hardware PLC and the emulated PLC when are under simulated FDIAs. The capabilities on the LOBO NSC could support the development of next generation cybersecurity and autonomous control technology and methods for terrestrial nuclear reactor power plants and space nuclear power systems, and other energy systems. The LOBO NCS platform could be used for academic education and professional training of a new cadre of nuclear cybersecurity researchers and engineers. The LOBO NCS platform and ManiPIO cybersecurity simulation program will be used carry out additional simulations of simulated FDIA events. Planned simulations will investigate responses of PLCs for the pressurizer, steam generator, reactor power, and primary pumps in a representative PWR plant.

5. Acknowledgements

This research is funded by the DOE Office of Nuclear Energy's Nuclear Energy University Program under Contract No. Nu-18-NM-UNM-050101-01 to the University of New Mexico. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Energy. The views expressed in the report do not necessarily represent the views of the U.S. DOE or the United States Government.

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. DOE’s National Nuclear Security Administration under contract DE-NA-0003525.

We wish to thank Sandia National Laboratories for loaning the Allen-Bradley PLC used in performing the cybersecurity investigations using the LOBO NSC Platform, and whose results are documented and discussed in this report.

6. References

Allen-Bradley, 2013. *1769 CompactLogix Controllers User Manual*, Rockwell Automation Publication 1769-UM011I-EN-P - February 2013.

Alves, T.R., Buratto, MM, Mauricio de Souza, F., and Rodrigues, T.V., 2014. “OpenPLC: An open source alternative to automation,” in proceedings IEEE Global Humanitarian Technology Conference (GHTC 2014), San Jose, CA, USA, DOI: 10.1109/GHTC.2014.6970342

Alves, T., Morris, T., 2018. “OpenPLC: An IEC 61,113-3 compliant open source industrial controller for cyber security research,” *Computers & Security*, **78**, pp. 364-379.

Biondi, P., 2021. Scapy v2.4.5 Documentation, https://scapy.net/, accessed June 2021

Busquim E. Silva, R.A., et al. 2020. “Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment,” *Proc. IAEA International Conference on Nuclear Security 2020*, Vienna, Austria.

Camacho-Lopez, T.R., 2016, "SCEPTRE," Electricity Subsector Coordinating Council & Government Executives Meeting,” Albuquerque, NM, USA.

Cetiner, S., Ramuhalli, P., 2019. Transformational Challenge Reactor Autonomous Control System Framework and Key Enabling Technologies, Oak Ridge National Laboratory, Oak Ridge, TN, Technical report ORNL/SPR-2019/1178.

Crussell, J., Erickson, J., Fritz, D., Floren, J., 2015. minimega v. 3.0. Technical Report No. 004619MLTPL00 SCR #1592.2, Sandia National Laboratories, Albuquerque, NM.

Dragos, Inc., 2017a, "TRISIS-Hatman Malware Analysis of Safety Systems Targeted Malware," https://dragos.com/wp-content/uploads/TRISIS-01.pdf.

Dragos, Inc., 2017b. CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations version 2.20170613, www.DRAGOS.com.

El-Genk, M.S, Schriener, T.M., Lamb, C., Fasano, R., Hahn, A., 2019, Implementation and Validation of PLC Emulation and Data Transfer, Report No. UNM-ISNPS-02-2019, Institute for Space and Nuclear Power Studies, University of New Mexico, Albuquerque, NM, USA

El-Genk, M.S, Schriener, T.M., Hahn, A., Altamimi, R., Lamb, C., Fasano, R., 2020a, A Physics-based, Dynamic Model of a Pressurized Water Reactor Plant with Programmable Logic Controllers for Cybersecurity Applications, Report No. UNM-ISNPS-02-2020, Institute for Space and Nuclear Power Studies, The University of New Mexico, Albuquerque, NM, USA.

El-Genk, M.S., Schriener, T.M., Lamb, C.C., 2020b, “Nuclear Instrumentation and Control Simulation (NICSim) Platform for Investigating Cybersecurity Risks.” In Trans. ANS Annual Meeting, Phoenix, AZ, June 7-11, 2020.

El-Genk, M. S., T. Schriener, R. Altamimi, A. Hahn, C. Lamb, R. Fasano, 2020c, “NICSIM: Nuclear Instrumentation and Control Simulation for Evaluating Response to Cyber – Attacks,” Proc. 28th International Conference on Nuclear Engineering (ICONE28), ICONE28-POWER2020-16756, Anaheim, CA, USA, 2-6 August 2020.

El-Genk, M.S., Altamimi, R., Schriener, T.M., 2021, “Pressurizer Dynamic Model and Emulated Programmable Logic Controllers for Nuclear Power Plants Cybersecurity Investigations,” Annals of Nuclear Energy, 154, 108121.

El-Genk M.S., et al., 2021. “LOBO Nuclear Reactor Power Plants CyberSecurity (LOBO NCS) Platform,” in proceedings 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), paper No. 34512, virtual meeting, June 14-17 2021.

Falliere, N., Murchu, L., Chien, E., 2011, "W32 Stuxnet Dossier," Symantec, https://www.symantec.com/content /en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Hahn, A., Schriener, T.M., El-Genk, M.S., 2020b. "Selection and validation of fast and synchronous interface to the controller of a space nuclear reactor power system," Proceedings of the 2020 28th Conference on Nuclear Engineering Joint with the ASME 2020 Power Conference ICONE28-POWER2020, August 2-6, 2020, Anaheim, California, USA, paper ICONE28-POWER2020-16237

International Association for the Properties of Water and Steam, 2007, The International Association for the Properties of Water and Steam Revised Release on the IAPWS Industrial Formulation 1997 for the Thermodynamic Properties of Water and Steam, Lucerne, Switzerland, IAPWS R7-97(2012)

Karnouskos, S., 2011. "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," in proceedings IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, 7-10 November, 2011, DOI: 10.1109/IECON.2011.6120048.

Korsah, K., et al., 2008. Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update, US NRC Technical Report NUREG/CR-6992, Washington, DC.

Metzger, J.D., El-Genk, M.S., Parlos, A.G., 1991. "Model-Reference Adaptive Control with Selective State-Variable Weighting Applied to a Space Nuclear Power System," *J. Nuclear Science and Engineering*, **109**, pp. 171-187.

National Research Council, 1997. Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues, Final Rep., National Academy Press, Washington, D.C.

Nuclear Energy Institute, 2010, "Cyber Security Plan of Nuclear Power Reactors," NEI Technical Report NEI 08-09 [Rev.6].

Nuclear Energy Institute, 2021, "U.S. Nuclear Plant Actual and Expected Uprates by Plant," https://www.nei.org/resources/statistics/us-nuclear-plant-actual-and-expected-uprates, accessed July 2021.

MathWorks, 2020, "Matlab & Simulink R2020a," Natick, Massachusetts, United States, https://www.math works.com/

Phenix SCEPTRE Development Team, 2021. Phenix Documentation, phenix.sceptre.dev, Sandia National Laboratories, Albuquerque, NM.

Schriener, T., El-Genk, M.S., 2021. "Response of Programmable Logic Controllers of the Pressurizer in a Representative PWR Plant Following a False Data Injection," in proceedings 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), paper No. 34539, virtual meeting, June 14-17, 2021.

Trask, D., Jung, C., MacDonald, M., 2014. "Cybersecurity for Remote Monitoring and Control of Small Reactors," *Proc. 19th Pacific Basin Nuclear Conference (PBNC 2014)*, Vancouver, British Columbia, Canada, 24-28 Aug. 2014.

VMware, 2019. VMware Workstation 15 Pro.

Zhang, F., Coble, J.B., 2020. "Robust localized cyber-attack detection for key equipment in nuclear power plants," *Progress in Nuclear Energy*; **128**; 103446.

Appendix A: Manipulate Process Input/Output (ManiPIO) Framework

A high priority concern of industrial control systems is stopping the interference, influence, or manipulation of the operation of the Programmable Logic Controllers (PLCs). While methods of intrusion into networks are important to understand, the dynamics of interfering with process control systems are the mechanism by which actual damage occurs. The Manipulate Process Input/Output (ManiPIO) framework allows users to develop custom scripts to execute manipulations on PLCs to simulate cybersecurity events within ICS systems. The program is developed to be modular and easy to use. Currently ManiPIO can utilize the Modbus TCP communication protocol, but its modular programming structure can allow for other protocols to be quickly and easily implemented in the future. Additional functionality can easily be added to the ManiPIO source code to fit specific user needs. The input configuration instructions are in the form of human readable text files and allow the user to create complex series of control system manipulations which simulate sophisticated cybersecurity events.

The ManiPIO framework consists of the main ManiPIO program which handles the ICS manipulations as well as a standalone network capture and recording utility. The network capture utility captures Modbus packets transmitted along the connected network and decodes and records the system control commands and process data to a log file. The network data capture utility has a modular design to allow users to place it on any computer node in the simulated plant network. Since the ManiPIO program and the network capture and recording utility are intended to be distributed to research partners, it is important that they do not contain any cybersecurity risks. Thus, neither program contain malicious software. They are built using open source tools and common python libraries.

A.1. Simulating Cybersecurity Events

The ManiPIO program is meant to safely simulate the interference of the PLCs by malicious actors. It simulates the potential effects of a successful cyber-intrusion of the ICS network by using established ICS network protocols to manipulate the values stored in the PLCs' memory registers. This allows ManiPIO to simulate how real cyber-events on the ICS would affect the processes being controlled. As cyber-events on ICS are continuously evolving, ManiPIO was designed to be highly modular, adaptable, and customizable. The python-based program is broken into separate classes with a main program section which reads the input scripts and constructs the timeline of the simulated cyber-event (Fig. A.1). The ICS Communication classes convert open-source python ICS protocol libraries into uniform structures for use within the Event classes. The Modbus TCP protocol is preconfigured into ManiPIO as the default Communication class, but separate classes can be established for each ICS protocol desired for the simulation. Each Event class can be configured to communicate using any of the implemented ICS protocol ICS Communication classes. This structure supports the simulation of complex cyber-events and allows for current and future protocols to be easily added to ManiPIO.

ManiPIO contains three major event types, a single value write, writing ramping values, and executing triggers (Fig. A.1). These Event classes rely on selected the ICS protocol Communication classes to communicate read and write actions with PLCs. The single value write event class allows the user to write single values to a PLC's memory registers either once as a single write event, or as a persistent event that periodically rewrites the same value to the PLC memory register. The ramp event class allows the user to write a value to the memory registers which changes over time. The user specifies a series of data values and the time period between these values. The program linearly interpolates between the input values over the specified time period and writes to the PLC memory with the appropriate value for that time. The trigger-on-event class reads the present values of the specified process variables on one of the PLCs on the network and triggers another event when the value or values it is monitoring satisfy the predetermined logic setpoints. This allows a user to simulate a cybersecurity event where a malicious program is monitoring the state variables to wait for the operating condition of the controlled process to reach a specific point before acting. All the different event classes allow the user to schedule each events' initiation using time delays, allowing the user to define a predesigned sequence of events.

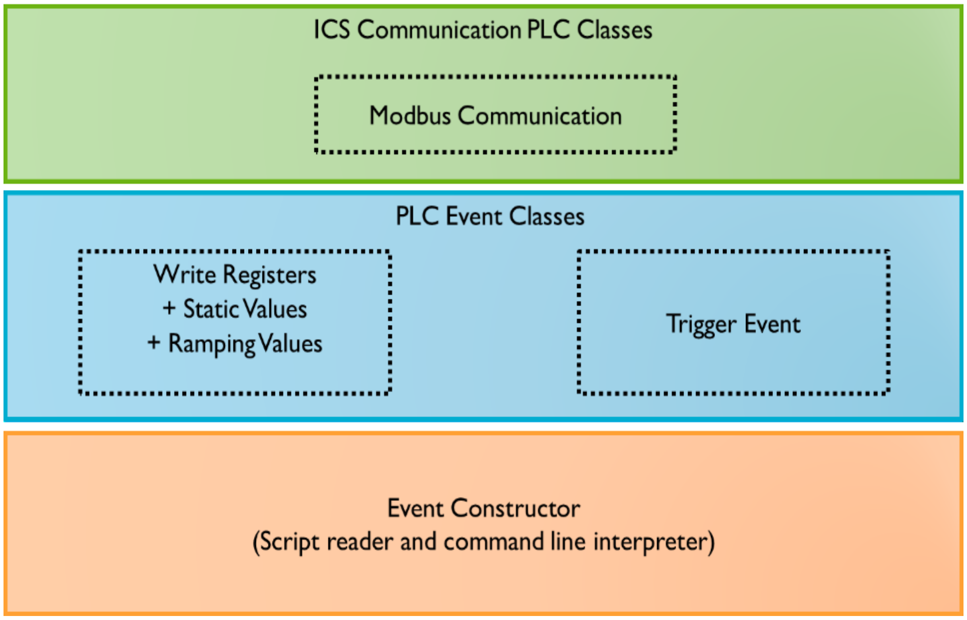


Fig. A.1: ManiPIO Internal code structure.

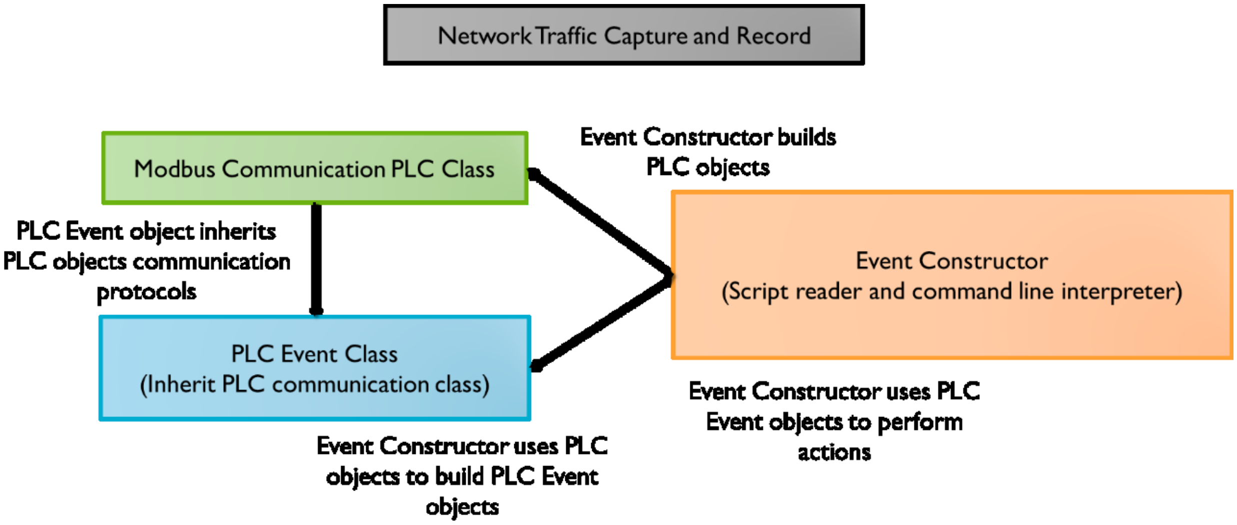

Network Traffic Capture and Record
Modbus Communication PLC Class
Event Constructor builds PLC objects
PLC Event object inherits PLC objects communication protocols
Event Constructor
(Script reader and command line interpreter)
PLC Event Class
(Inherit PLC communication class)
Event Constructor uses PLC Event objects to perform actions
Event Constructor uses PLC objects to build PLC Event objects

Fig. A.2: ManiPIO Component relationship diagram.

The ManiPIO Event Constructor coordinates the specified event classes in the user input script. The Event Constructor is used to coordinate the sequence of events by reading the user generated scripts and building the simulated ICS manipulations (Fig. A.2). The user writes a human readable script in the form of a text file which informs the constructor what communication protocols to use, the events, their variables, and the sequence at which they are started. The constructor then executes the events in individual threads and monitors them for safe completion. The modular design, adjustable execution schemes, and protocol flexibility combined in one package enables ManiPIO to simulate nearly any ICS control event.

A.2. Network Traffic Capture Utility

ManiPIO includes a standalone utility for capturing and recording network traffic during cybersecurity experiments. This utility performs deep inspection of Modbus TCP packets and is based on the open-source Scapy python library (Biondi 2021). The network utility is separate from the main ManiPIO program (Fig. A.2) to allow placement anywhere in the network. The utility monitors Modbus TCP packets passed between computers through the Ethernet network as well as packets sent between programs running on single computer in an internal loopback network. The captured packets are decoded, and the details are recorded to a log file. This log file can then be analyzed to provide data about the Modbus TCP communication to and from the PLCs during the simulated cyber-event and their transmitted control responses sent to the connected system model. The timing of the transmitted packets can be correlated with the simulation results to investigate the effects of the cyber event on the physics of the process in relation to the network traffic.

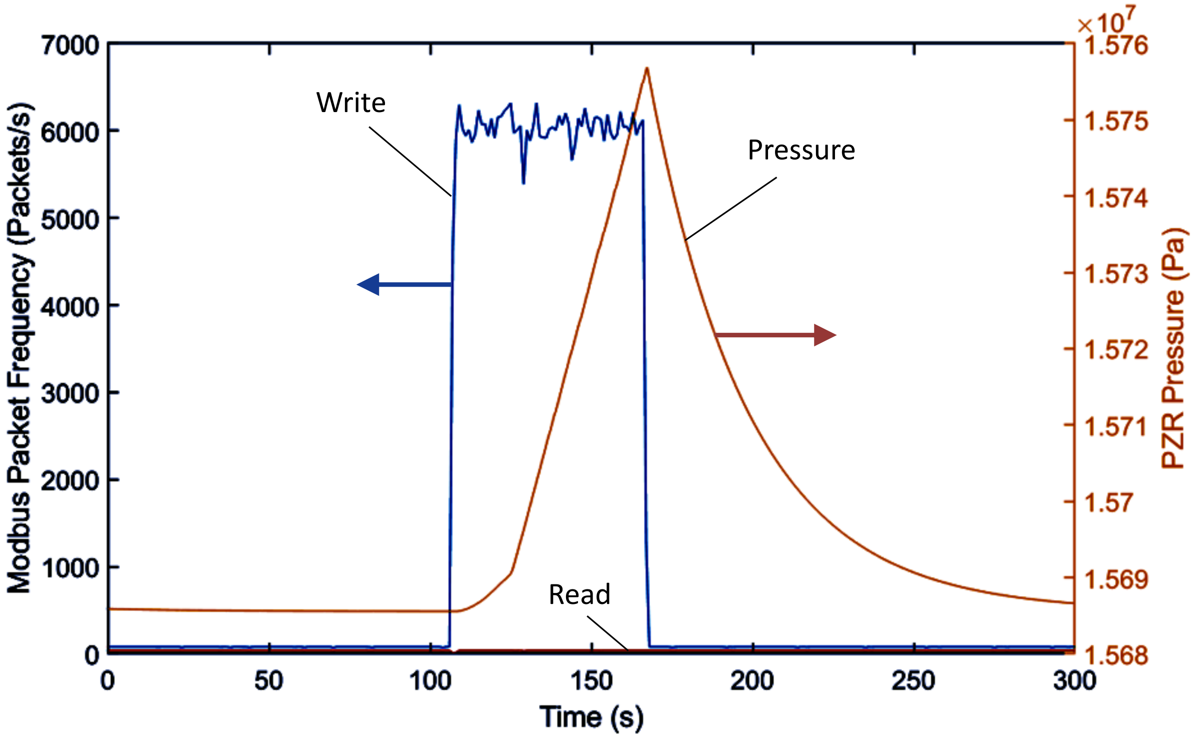


Fig. A.3: Network traffic of simulated cyber event with impact on physics.

Figure A.3 shows the results of Modbus TCP network traffic captured during a simulated transient using the NICSim pressurizer model and pressure PLC (El-Genk, Altamimi, and Schriener 2021). The Simulink pressurizer model, pressure PLC, and ManiPIO program were configured on the LOBO Nuclear CyberSecurity (NCS) platform at UNM-ISNPS. The Simulink simulation and data transfer interface were run on a Linus server computer. The network capture and record utility was connected to the ethernet switch and recorded the Modbus traffic on the network. The emulated PLC used the OpenPLC runtime (Alves, et al. 2014) and was run within a virtual machine on a Windows server using the VMWare software (VMWare 2019). The simulation starts with the pressurizer operating at steady state conditions. ManiPIO starts a simulated cyber event shortly after t = 100 seconds where the program repeatedly overwrites the Modbus holding register address on the controller that holds the input state variable for the pressure with a low pressure value (Fig. A.3). The start of the cyber-event is seen as the sharp increase in Modbus write packets, followed by the sharp decrease is the end of the simulated event. In response to the low pressure value written by ManiPIO, the pressurizer control PLC turns on the heaters, causing the actual system pressure to rise until the event is stopped (Fig. A.3). Following the end of the simulated cyber event the PLC actuates the water spray and returns the system pressure to the steady state value. These results demonstrate the ability of the ManiPIO program to manipulate the operation of the emulated PLC.

A.3. Summary

The developed ManiPIO program allows users to simulate cybersecurity events on ICS networks and record Modbus TCP traffic using an included network traffic capture utility. The ManiPIO program and accompanying network traffic capture utility support investigating the effects of varied and sophisticated simulated cyber-security events. The modular construction of this toolset enables new communication protocols and strategies to be easily integrated. Test results show that ManiPIO is capable of manipulating the values on the memory registers of PLCs alter the operation of a physics-based model of a PWR pressurizer. As research into the cybersecurity of ICS networks expands, the ManiPIO program will continue to provide a highly valuable and safe method to investigate cyber-security events and its effects on physical processes.