Cyber Security Modeling of Non-Critical Nuclear Power Plant Digital Instrumentation

Trevor Maclean, Robert Borrelli, Michael Haney

Chapter 5

CYBER SECURITY MODELING OF NON-CRITICAL NUCLEAR POWER PLANT DIGITAL INSTRUMENTATION

Trevor MacLean, Robert Borrelli and Michael Haney

Abstract This chapter examines potential attack vectors that exist in a nuclear power plant and correlates the likelihood of an attack from each vector. The focus is on the boron monitoring system, which directly affects the reactivity in the core; cyber attacks on this system can lead to increased core wear, unsafe reactivity levels and poor power performance. A mockup model is developed using open-source software and hardware, which is tested to evaluate the potential of cyber attacks. A man-in-the-middle attack is implemented to demonstrate a cyber attack and its potential effects. Additionally, a redundancy-based cyber attack mitigation method is implemented using a hardware device that compares the input/output values of multiple programmable logic controllers. The approach for modeling general attack and defense steps is applicable to industrial control systems in the energy sector.

Keywords: Nuclear power plants, digital instrumentation and control, security

1. Introduction

Cyber security vulnerabilities are an ever-present risk to industrial control systems. As nuclear power plants experience increased digitization of control systems, potential attack vectors will propagate. Critical systems in nuclear power plants have multilayered defenses to prevent malicious actors from causing catastrophic damage. A multilayered defensive approach to all plant operations maintains safety at an increased cost or risk of lost energy production. In the case of non-critical systems (i.e., systems that are not directly involved in the nuclear reactions in the core) and systems designed to be passively safe (e.g., natural convection cooling of a reactor during a power loss incident), lost production caused by an unnecessary shutdown of the power plant or tolerating the equipment deficiency with a less efficient contingency backup method can cause unintentional harm to humans and/or the environment. Non-critical and passively-safe systems are designed for continuous operation without direct human interactions. Although operations could be secured to accommodate all equipment deficiencies to maintain safety at all costs, the most efficient, but still safe, method is to operate a non-critical or passively-safe system with a fault detection program and perform automated or rapid repairs without operational impacts by utilizing concurrently-operating systems.

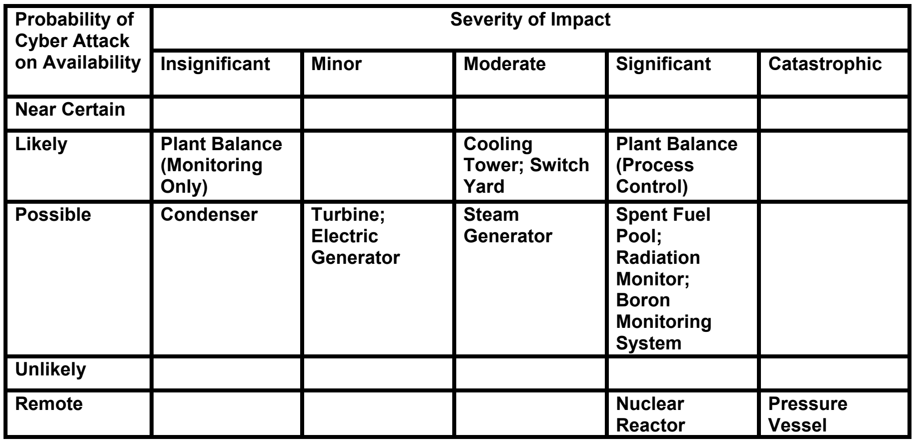
This chapter discusses how cyber attacks have interfered with nuclear power plants in the past. It reviews nuclear power plant components and attack paths. A mockup testbed is developed for a non-critical boron monitoring system against which a cyber attack is launched and an attack mitigation strategy involving failure detection and operator alerts is demonstrated. The modeling of general attack and defense steps is applicable to industrial control systems in nuclear power plants as well as in other types of power plants in the energy sector.

2. Background and Literature Review

Cyber attacks focused on gaining or interrupting control of industrial control systems are becoming increasingly prevalent. Kim [11] discusses cyber attacks that compromised plant operations at Ohio's Davis-Besse Nuclear Power Plant in 2003, Browns Ferry Nuclear Power Plant in 2006 and Iran's Natanz uranium hexafluoride centrifuge facility in 2010. Each of these compromised plants had one or more previously-unidentified vulnerabilities – "zero-day" vulnerabilities [11] – that were exploited to result in a security breach or cause equipment damage. The Ohio Davis-Besse Nuclear Plant's network server was infected by the Microsoft SQL Slammer worm that disabled a safety monitoring system. Excessive network traffic caused by a failing programmable logic controller caused the variable frequency drives of recirculation pumps in the Browns Ferry Nuclear Power Plant to be disabled. A man-in-the-middle attack by the Stuxnet worm on Iran's Natanz facility allowed the centrifuges to operate normally, except under specific conditions when critical system values were modified while reporting normal conditions to operators via the human-machine interfaces (HMIs).

Industrial control systems are often controlled by programmable logic controllers due to their modular input/output (I/O) options and ability to operate in harsh environments. Programmable logic controllers typically have minimalized operating systems and often no security software, which render them vulnerable to cyber attacks, such as the Stuxnet computer worm or via the manipulation of controller I/O pins as described in [1]. Potential ways to influence I/O pin values are via configuration manipulation attacks, control-flow attacks and code manipulation attacks. The manipulation of I/O pins, called a pin control attack [1], involves reconfiguring pin assignments so that output pins are changed to input pins, and vice versa.

Programmable logic controller protocols such as Modbus Serial, Modbus TCP/IP and Distributed Network Protocol 3 (DNP3) are commonly used in



Probability of Cyber Attack on Availability	Severity of Impact				
	Insignificant	Minor	Moderate	Significant	Catastrophic
Near Certain					
Likely	Plant Balance (Monitoring Only)		Cooling Tower; Switch Yard	Plant Balance (Process Control)	
Possible	Condenser	Turbine; Electric Generator	Steam Generator	Spent Fuel Pool; Radiation Monitor; Boron Monitoring System	
Unlikely					
Remote				Nuclear Reactor	Pressure Vessel

Figure 1. Nuclear power plant cyber attack risk matrix.

the energy sector. These protocols are highly susceptible to cyber attacks, including numerous methods for intercepting, interrupting, modifying and fabricating data communications. These attack methods are described in detail in attack taxonomies for Modbus [9] and DNP3 [6], where each attack method has multiple sub-categories of attacks.

3. Risk-Informed Selection of Attack Paths

In 2012, the National Institute of Standards and Technology published a guide for conducting risk assessments [10]. This guide describes a process for performing risk assessments of information systems, which can be directly applied to various components of a nuclear power plant. Part of the process involves the review of threat sources, threat events, vulnerabilities, likelihoods and impacts. This research has identified the threat sources, threat events and vulnerabilities as nominal attack vectors at a nuclear power plant.

The major systems involved in plant operations were identified and placed in a risk matrix (Figure 1). Each system was assigned a probability of accessibility by a cyber attack and the severity of the attack impact on overall plant operations, plant employees, the public and/or the environment. The specific purpose of each system in the nuclear power plant was considered when assigning the accessibility probability and impact severity values in the risk matrix.

A nuclear power plant comprises safety-critical, important-to-safety and non-safety systems [14]. Safety-critical systems must operate to ensure the safety of plant employees, the public and the environment; a failure of a safety-critical system can cause serious injury to plant personnel and significant harm to the public and the environment. Important-to-safety systems impact the safety of plant personnel but would not have impacts as large as safety-critical systems. Non-safety systems are the remaining systems in a nuclear power plant that do not pose significant impacts to plant employees, the public and/or the environment.

This research examined the safety-critical and important-to-safety systems and the safety and security measures in place at a nuclear power plant. Safety-critical systems often have their risks mitigated through engineered controls, such as control rods that are physically unable to be retracted (which prevents the system from going critical rapidly). Therefore, these systems were determined to have lower likelihoods of successful cyber attacks. However, the consequences of successful attacks on safety-critical and important-to-safety systems would be severe because of the potential to affect the lives of plant personnel and the public, and the environment through contamination and radiation exposure. Figure 1 expresses such scenarios – the nuclear reactor and pressure vessel have remote cyber attack probabilities, but significant or catastrophic impact severity values.

Other non-safety-critical systems in the nuclear power plant would have lower severity levels in the risk matrix because cyber attacks on these systems would impact plant operational time, but would not cause significant hazards to plant employees, the public and the environment. The lower level of scrutiny placed on non-safety-critical systems can lead to an increase in cyber attack probability because these systems do not have the same level of protection as safety-critical systems.

The probabilities of cyber attacks listed are based on the accessibility of the control system to an attacker, either directly or via network access. For example, the switchyard has a high cyber attack probability because the power plant connections to external power utility lines cannot be air-gapped. The severity scale is based on the impact that the failed system would have on plant operations and employees, the public and the environment. Returning to the switchyard example, mitigating the consequences of an attack would require power from emergency backup generators. The use of emergency generators would not impact the public, but it would impact plant employees and plant operation; therefore, the switchyard is rated as having moderate severity.

Based on the data in Figure 1, the project scope was narrowed to focus on the spent fuel pool, switchyard, balance of plant systems and boron monitoring system, all of which are high risk systems because of their accessibility to external attacks (i.e., not air-gapped) and because of significant impact to plant operations if the cyber-physical systems were to be compromised. The spent fuel pool, switchyard and boron monitoring system have significant severity because failures could lead to unstable plant conditions or loss of plant control. The switchyard, although rated as having moderate severity, is a likely target of cyber attacks because of the accessibility of the switchyard by external entities and the inability to provide power to the plant without external sources after a successful attack.

Poresky et al. [12] describe cyber security strategies and vulnerability mitigation methods for advanced nuclear reactors. Research related to spent fuel pools, including patents such as [4], reveals that passive cooling is actively pursued to mitigate concerns about the failure of an active spent fuel pool cooling system. Based on the available information about passively-cooled spent fuel pools, the scope of this research was narrowed further to include only the switchyard, balance of plant systems and boron monitoring system.

Gergely et al. [8] describe risk mitigation methods for industrial control systems, including a fail-safe programmable logic controller that detects failures and places the system in a safe (non-operating) state. They also discuss fail-operate programmable logic controllers that detect failures and resort to backup systems for continuity of operations. However, the drawback of fail-operate systems is that they tend to degrade system performance.

Therefore, based on the analysis related to Figure 1 and previous research [4, 12], the boron monitoring system was selected as the system to model and analyze in this research. The boron monitoring system is rated as significant on the severity scale and possible on the accessibility scale. Modeling and analysis of the switchyard and balance of plant systems are topics for future research.

4. Boron Monitoring System

The boron monitoring system measures the boron levels in the reactor cooling loop. This system can directly affect the reactivity ("fissionability") or changes to the time-dependent neutron population in the core and cause undesirable operating conditions, leading to increased core wear, unsafe (high) reactivity levels and poor power performance. Using an outside vendor to design and implement a boron monitoring system introduces additional paths for cyber attacks compared with a boron monitoring system designed and implemented in-house. Therefore, the monitoring system is assigned a possible value on the cyber attack accessibility scale.

Multiple companies offer boron monitoring systems that incorporate programmable logic controllers. Examples include the Rolls-Royce Boronline and Mirion Technologies BM 501 Boron Meter. These products have similar components – a neutron emitting source and a neutron detector placed around an in-place pipe or in a storage tank in the nuclear power plant. The boron monitoring system is fail-safe because it is designed to place the reactor in a safe state if it were to fail.

4.1 Experimental Setup

This research demonstrates a cyber attack that compromises a programmable logic controller in a boron monitoring system and the mitigation of the attack. OpenPLC [2] and Raspberry Pis were selected to create a mock boron monitoring system. OpenPLC was selected because of its open-source software and hardware – its development platform is compliant with the IEC 61131-3 standard, supports SCADA protocols and interfaces with open-source human-machine interfaces and the ScadaBR SCADA simulator [3, 13]. Raspberry

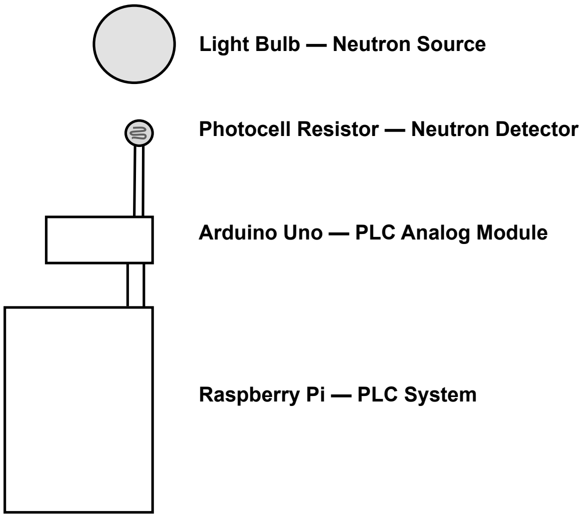

Light Bulb — Neutron Source
Photocell Resistor — Neutron Detector
Arduino Uno — PLC Analog Module
Raspberry Pi — PLC System

Figure 2. Conceptual model of the boron monitoring system.

Pis were employed because their I/O pins can be used to simulate the boron monitoring system.

Figure 2 shows a mockup of the boron monitoring system. It incorporates a Raspberry Pi with the OpenPLC software to emulate a programmable logic controller, an Arduino Uno to emulate a programmable logic controller analog module that feeds analog values to the Raspberry Pi, a photoresistor to represent a neutron detector and a light source to represent a neutron source. The neutron detector and neutron source are unique to the boron monitoring system whereas the programmable logic controller and analog module are commonly used in other industry sectors.

In order to launch and mitigate cyber attacks, three programmable logic controllers were set up in parallel using a 2-out-of-3 logic circuit arrangement to compare signals of interest. This method of risk mitigation [5] uses AND and OR integrated circuits to compare the signals received from the three programmable logic controllers and outputs the signal that matches at least two of the three inputs. The 2-out-of-3 circuit with three programmable logic controllers operating in parallel helps prevent performance loss and downtime if an individual programmable logic controller were to fail. By incorporating a method that identifies a compromised programmable logic controller in real-time and implementing a self-healing protocol [5] for continuity of operations, repairs can be performed and malicious software can be purged without interrupting the overall function of the boron monitoring system.

The 2-out-of-3 circuit compares the high and low photoresistor values for the three programmable logic controllers. The output of the 2-out-of-3 circuit is the majority value expressing the presence (high) or absence (low) of

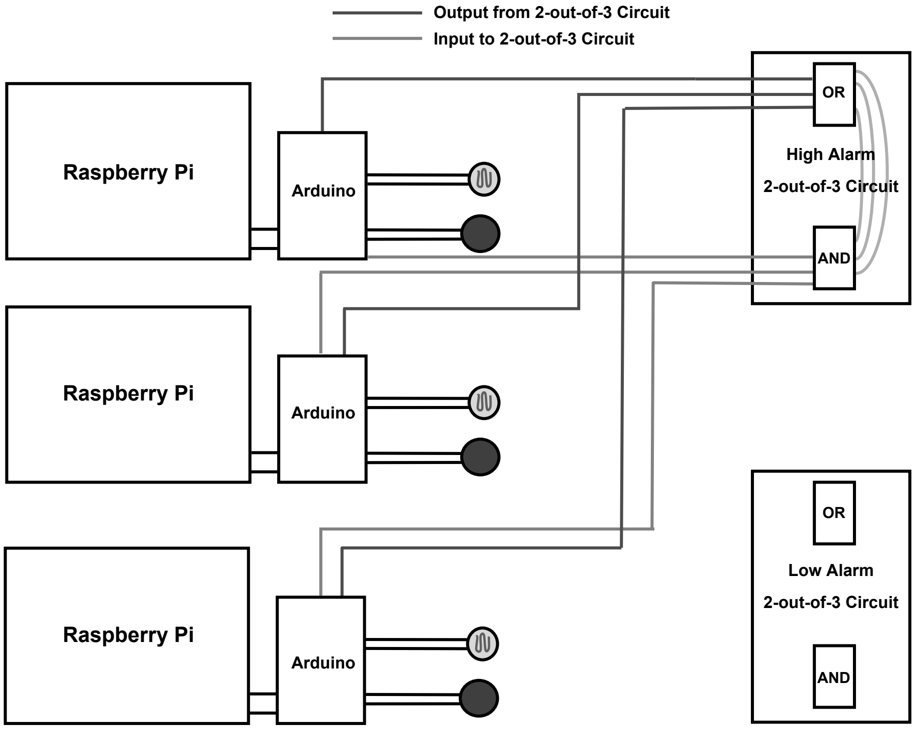


Figure 3. Schematic diagram of the boron monitoring system testbed.

neutrons reaching the detector. An alarm is sent to plant operators when a programmable logic controller has an anomalous output value.

Figure 3 shows a schematic diagram of the testbed with the implemented 2-out-of-3 circuit. The diagram shows the three programmable logic controllers, three Raspberry Pis and three Arduino Unos (analog system models), each with a photoresistor and cyber attack trigger. Each system outputs an alarm when a high or low level light is detected, corresponding to high or low boron levels, respectively. These alarm signals are wired to a 2-out-of-3 circuit to check for system continuity, which ultimately determines the overall system state of the light (boron) levels.

Figure 4 shows the cyber-physical testbed for analyzing cyber attack scenarios. Three different models of Raspberry Pi were incorporated in the testbed to ensure that performance differences would not produce differing results.

The testbed was programmed using the structured text programmable logic controller programming language via the OpenPLCEditor software [2]. The program checks the value read from each photoresistor and compares it against the predetermined high and low levels. When the photoresistor value is too high or too low an alarm signal is sent to the 2-out-of-3 circuit. The output of the 2-out-of-3 circuit is used as a system state alarm input to the programmable

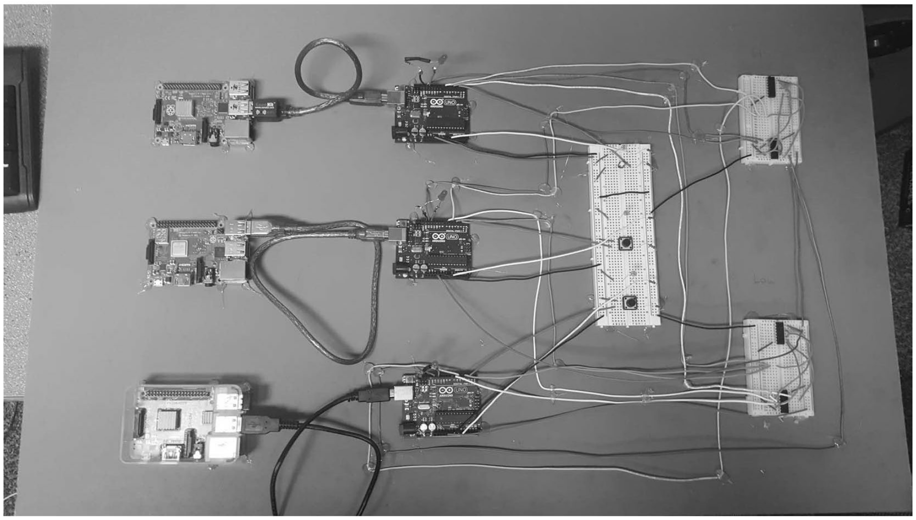


Figure 4. Cyber-physical testbed for analyzing cyber attack scenarios.

logic controller in question; it represents the actual boron value monitored by the programmable logic controller. The structured text program then compares the individual programmable logic controller high or low alarm to the system state alarm and triggers a programmable logic controller system alarm if a difference is detected.

```
IF Photoresistor < 21000 THEN
        LowAlarm := TRUE;
ELSIF Photoresistor > 37000 THEN
        HighAlarm := TRUE;
ELSIF Photoresistor > 21000 & Photoresistor < 37000 THEN
        LowAlarm := FALSE;
        HighAlarm := FALSE;
ENDIF;

IF OR((HighState <> HighAlarm),(LowState <> LowAlarm)) THEN
        SystemAlarm := TRUE;
ELSE SystemAlarm := FALSE;
ENDIF;
```

Figure 5. Structured text program.

Figure 5 shows the structured text program. The code has six declared variables. The `Photoresistor` variable stores the analog value provided by the photoresistor. `HighAlarm` and `LowAlarm` are programmable-logic-controller-specific output variables that denote whether the controller receives high or low light readings from the photoresistor. The `HighState` and `LowState` variables store the value received from the 2-out-of-3 circuit output and represent the value of at least two of the three programmable logic controllers. Finally, the `System Alarm` output variable holds the result of the comparisons of the `HighState` and `HighAlarm` variables and the `LowState` and `LowAlarm` variables.

4.2 Cyber Attack Simulation

In order to simulate an attack on the programmable logic controller, the source code of the slave device was modified to enable the photoresistor values to be changed before sending them to the controller. This corresponds to a man-in-the-middle attack on a Modbus communications system.

The testbed incorporates a pushbutton as a trigger for launching the attack; however, this could be any exploit on the programmable logic controller. When the pushbutton trigger is activated, the code functions identical to the default code, except when a value is assigned to the analog pin fed by the photoresistor. Specifically, the photoresistor analog pin value is set to a predetermined value of low, which corresponds to the system diluting the boron concentration to enable more neutrons to reach the detector from the neutron source. This attack results in an inadequate level of boron in the cooling system that could lead to an abnormal increase in the radiation levels and require the nuclear reactor to be tripped.

4.3 Experimental Results

Since the focus is on the cyber security vulnerability in a single programmable logic controller and the integrity of a system with multiple programmable logic controllers operating in parallel, the concern is not about the boron monitoring system state being high or low, but about the differences between the programmable logic controller alarm values. During normal operations, all the programmable logic controller states should match, reporting either low, high or no alarm.

Figure 6 shows the programmable logic controllers operating under normal conditions with matching low boron states. Since all the programmable logic controller values match, no programmable logic controller alarms are illuminated in the right-hand side of Figure 6.

Figure 7 shows the programmable logic controllers operating under normal conditions with matching high boron states. During normal operations, the boron measuring system would ideally have the correct amount of boron in the cooling loop. Therefore, the low, high and programmable logic controller alarms would not be illuminated. However, in Figure 7, although the high system state alarms are illuminated for all the programmable logic controllers, the boron monitoring system is considered to be operating properly and should be able to correct the high boron alarms. Since all the programmable logic controller

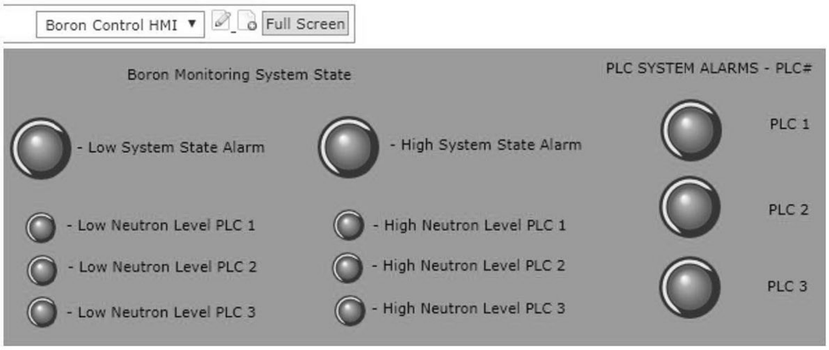

Boron Control HMI ▼
Full Screen
Boron Monitoring System State
PLC SYSTEM ALARMS - PLC#
- Low System State Alarm
- High System State Alarm
PLC 1
PLC 2
PLC 3
- Low Neutron Level PLC 1
- Low Neutron Level PLC 2
- Low Neutron Level PLC 3
- High Neutron Level PLC 1
- High Neutron Level PLC 2
- High Neutron Level PLC 3

Figure 6. Human-machine interface with no alarm.

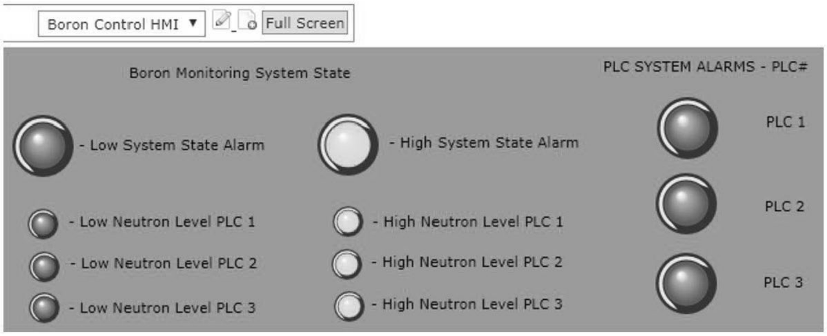

Boron Control HMI ▼
Full Screen
Boron Monitoring System State
PLC SYSTEM ALARMS - PLC#
- Low System State Alarm
- High System State Alarm
PLC 1
PLC 2
PLC 3
- Low Neutron Level PLC 1
- Low Neutron Level PLC 2
- Low Neutron Level PLC 3
- High Neutron Level PLC 1
- High Neutron Level PLC 2
- High Neutron Level PLC 3

Figure 7. Human-machine interface with a high alarm.

values match, no programmable logic controller alarms are illuminated in the right-hand side of Figure 7.

In order to validate the operation of the 2-out-of-3 circuit, light was blocked from the photoresistors associated with two programmable logic controllers (PLC 2 and PLC 3), causing them to have low values. Since the PLC 1 value does not match the low PLC 2 and PLC 3 values, the alarm of the non-conforming PLC 1 is triggered (Figure 8).

On the other hand, in Figure 9, extra light was provided to the two photoresistors associated with PLC 1 and PLC 2, causing them to have high values. Since the PLC 3 value does not match the high PLC 1 and PLC 2 values, the alarm of the non-conforming PLC 3 is triggered.

With the testbed operating as expected under normal conditions, a simulated cyber attack was executed to see if the testbed could identify that a programmable logic controller was reading an incorrect value compared with the remaining programming logic controllers. This was accomplished by installing

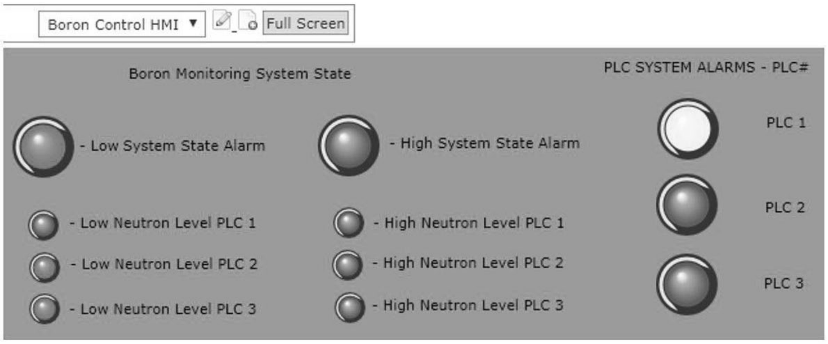

Boron Control HMI ▼
Full Screen
Boron Monitoring System State
PLC SYSTEM ALARMS - PLC#
- Low System State Alarm
- High System State Alarm
PLC 1
PLC 2
PLC 3
- Low Neutron Level PLC 1
- Low Neutron Level PLC 2
- Low Neutron Level PLC 3
- High Neutron Level PLC 1
- High Neutron Level PLC 2
- High Neutron Level PLC 3

Figure 8. Human-machine interface with two low alarms.

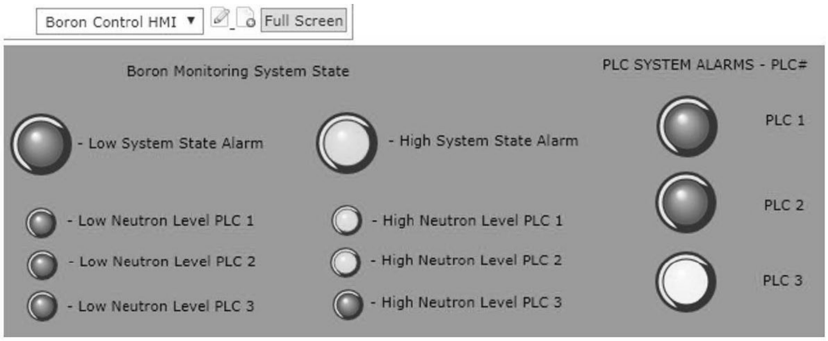

Boron Control HMI ▼
Full Screen
Boron Monitoring System State
PLC SYSTEM ALARMS - PLC#
- Low System State Alarm
- High System State Alarm
PLC 1
PLC 2
PLC 3
- Low Neutron Level PLC 1
- Low Neutron Level PLC 2
- Low Neutron Level PLC 3
- High Neutron Level PLC 1
- High Neutron Level PLC 2
- High Neutron Level PLC 3

Figure 9. Human-machine interface with two high alarms.

a pushbutton that overwrites the photoresistor value of a programmable logic controller with a significantly lower value.

Without the 2-out-of-3 circuit, the low neutron level alarm is activated for PLC 1, which tells the monitoring system to dilute the boron concentration. However, when the 2-out-of-3 circuit is operational during the cyber attack, the low alarm for PLC 1 is tripped and, because the PLC 1 value does not match the values of PLC 2 and PLC 3, the PLC 1 alarm is activated. With a proper contingency procedure in place, either the system operator would be notified or contingency recovery code would be executed to address the problem with PLC 1.

Figure 10 shows the situation when the pushbutton cyber attack trigger is activated for PLC 1 to overwrite the incoming photoresistor value with the low value. The cyber attack activates the low neutron level alarm for PLC 1. Due to the disparity between the PLC 1 value and the PLC 2 and PLC 3 values, instead of the monitoring system diluting the boron concentration, the PLC 1 alarm is triggered.

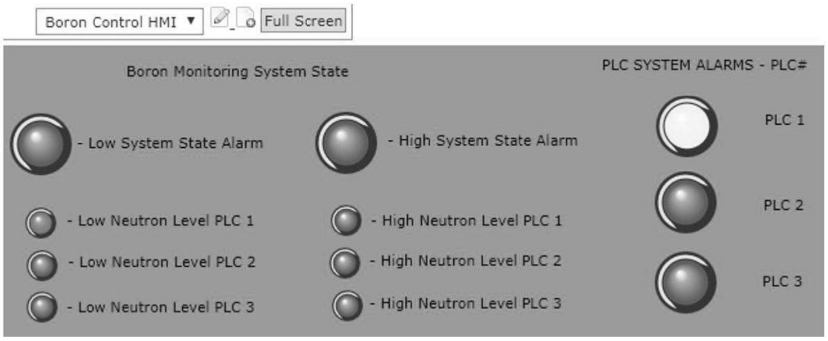

Boron Control HMI ▼
Full Screen
Boron Monitoring System State
PLC SYSTEM ALARMS - PLC#
- Low System State Alarm
- High System State Alarm
PLC 1
PLC 2
PLC 3
- Low Neutron Level PLC 1
- Low Neutron Level PLC 2
- Low Neutron Level PLC 3
- High Neutron Level PLC 1
- High Neutron Level PLC 2
- High Neutron Level PLC 3

Figure 10. Human-machine interface with active cyber attack alarms.

5. Scope of Study

The boron monitoring system testbed is constrained to identify cyber attacks and differentiate situations involving malfunctioning devices from those involving cyber attacks. Therefore, the testbed reports when a programmable logic controller value does not match the values of its two counterparts. In order to implement robust cyber security, a method should be implemented to differentiate between a cyber attack and a malfunctioning sensor.

The current method for initiating and executing a man-in-the-middle attack does not cover up the malicious value passed to the human-machine interface. Indeed, not presenting the photoresistor value directly to the operator is a significant system vulnerability.

To create a more realistic and difficult-to-detect cyber attack, the man-in-the-middle attack should change the value of an output device (e.g., valve controlling a boron solution based on the control logic) while still reporting the output from the photoresistor as an acceptable, non-alarming value to the human-machine interface. In this way an operator would not receive an alarm despite the system operating in an alarmed state.

6. Conclusions

The review of nuclear power plant components and the subsequent assignment of qualitative risk measures to the components facilitated the identification of non-critical systems that pose significant safety and/or economic risks. The focus on the boron monitoring system is important because cyber attacks on this system can lead to increased core wear, unsafe reactivity levels and poor power performance. The mockup of the boron monitoring system using open-source software and inexpensive hardware components enabled the execution of a man-in-the-middle attack that demonstrated a system vulnerability and its mitigation using a mixed analog/digital solution. Similar methods can provide energy sector asset owners, operators and regulators insights into risk management and compliance regimes for securing industrial control system environments from evolving cyber threats.

A growing trend in the modernization of nuclear power plants is splitting digital and analog instrumentation and control [12]. Future research will investigate the cyber security implications of this modernization on non-critical nuclear power plant instrumentation, including the implementation of mitigation techniques involving field programmable gate arrays [7], fault-tolerant operations and self-repairing designs [12]. Additionally, future research will investigate other cyber attacks such as baseline response replay and direct slave control [9] to verify the effectiveness of the mitigation techniques. Creating testbeds for the switchyard and balance of plant systems, and incorporating split digital and analog instrumentation and control systems, would advance protection efforts for non-critical nuclear power plant instrumentation, helping identify potential vulnerabilities and mitigation approaches.

References

[1] A. Abbasi, M. Hashemi, E. Zambon and S. Etalle, Stealth low-level manipulation of programmable logic controller I/O by pin control exploitation, in *Critical Information Infrastructures Security*, G. Havarneanu, R. Setola, H. Nassopoulos and S. Wolthusen (Eds.), Springer, Cham, Switzerland, pp. 1–12, 2017.

[2] T. Alves, OpenPLC (`www.openplcproject.com`), 2019.

[3] T. Alves and T. Morris, OpenPLC: An IEC 61131-3 compliant open source industrial controller for cyber security research, *Computers and Security*, vol. 78, pp. 364–379, 2018.

[4] J. Dederer, W. Brown and F. Vereb, Alternate Passive Spent Fuel Pool Cooling Systems and Methods, U.S. Patent No. 9646726 B2, May 9, 2017.

[5] M. Denzel, M. Ryan and E. Ritter, A malware-tolerant, self-healing industrial control system framework, in *ICT Systems Security and Privacy Protection*, S. De Capitani di Vimercati and F. Martinelli (Eds.), Springer, Cham, Switzerland, pp. 46–60, 2017.

[6] S. East, J. Butts, M. Papa and S. Shenoi, A taxonomy of attacks on the DNP3 protocol, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Berlin Heidelberg, Germany, pp. 67–81, 2009.

[7] M. Elakrat and J. Jung, Development of a field programmable gate array based encryption module to mitigate man-in-the-middle attacks on nuclear power plant data communication networks, *Nuclear Engineering and Technology*, vol. 50(5), pp. 780–787, 2018.

[8] E. Gergely, D. Spoiala, V. Spoiala, H. Silaghi and Z. Nagy, Design framework for risk mitigation in industrial PLC control, *Proceedings of the IEEE International Conference on Automation, Quality and Testing, Robotics*, pp. 198–202, 2008.

[9] P. Huitsing, R. Chandia, M. Papa and S. Shenoi, Attack taxonomies for the Modbus protocols, *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 37–44, 2008.

[10] Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2012.

[11] D. Kim, Cyber security issues imposed on nuclear power plants, *Annals of Nuclear Energy*, vol. 65, pp. 141–143, 2014.

[12] C. Poresky, C. Andreades, J. Kendrick and P. Peterson, Cyber Security in Nuclear Power Plants: Insights for Advanced Nuclear Technologies, Technical Report UCBTH-17-004, Department of Nuclear Engineering, University of California, Berkeley, Berkeley, California, 2017.

[13] ScadaBR Project Team, ScadaBR (`sourceforge.net/p/scadabr/wiki/Home`), 2019.

[14] J. Song, J. Lee, C. Lee, K. Kwon and D. Lee, A cyber security risk assessment for the design of I&C systems in nuclear power plants, *Nuclear Engineering and Technology*, vol. 44(8), pp. 919–928, 2012.