NICSim: Nuclear Instrumentation and Control Simulation for Modeling Cyber-Attacks

Mohamed S. El-Genk, Timothy M. Schriener
Institute for Space and Nuclear Power Studies and Nuclear Engineering Department, University of New Mexico, 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: 07-01-2018 to 09-30-2022

Report No. DOE-UNM-15055
Institute for Space and Nuclear Power Studies, The University of New Mexico, Albuquerque, NM, USA, http://isnps.unm.edu/reports/

September 30, 2022

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

NICSim: Nuclear Instrumentation and Control Simulation for Evaluating Response to Cyber-Attacks

OVERVIEW

Purpose: Develop a novel and effective platform to emulate nuclear power plant control systems that integrate physics models of sensor instruments and nuclear reactor dynamics for end-to-end simulation of the responses of the plant I&C system to cyber-attacks.

Objectives:

- Use, DOE SCEPTRE emulation framework to simulate digital I&C systems in nuclear plants
- Develop and couple physics-based simulation models of nuclear plant components and sensors to SCEPTRE for direct feedback
- Identify and characterize reactor safety monitoring and control system
- Implement fully-emulated SCEPTRE model of safety system
- Test integrated NICSim model of safety monitoring system Programmable Logic Controllers (PLCs) under cyber-attack

IMPACT

Logical Path: Completion of the proposed research includes three major goals: (1) Port SCEPTRE framework into nuclear power plant domain by developing emulytics models of the plant's I&C components. (2) Tie this framework to dynamics physics-based Simulink models of a representative PWR plant and components to investigate potential cyber-attacks, (3) Bring the emulation capabilities provided by SCEPTRE and reactor dynamics models into an integrated platform & demonstrate capability by modeling a realistic response under a simulated cyber attack.

Outcomes: A successful outcome is a first-in-class emulytics platform that could be used to assess resilience and cybersecurity risks of different control system designs for a wide range of power plants. This platform would enable investigators to evaluate new I&C systems designs prior to deployment and evaluate their response under simulated cyber-attacks.

DETAILs

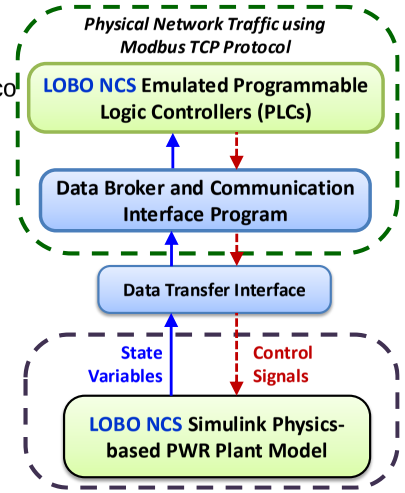
Principal Investigator:
Mohamed S. El-Genk
Institution: University of New Mexico
Collaborators: SNL
Duration: 3 years
Total Funding Level:
$799,945

TPOC: John Yankeelov

Federal Manager:
Jihad Alijayoushi

Workscope: NE-1

PICSNE Workpackage #:
18-15055



RESULTS / ACCOMPLISHMENTS

Results: Project team developed and validated: (a) the emulation methodologies of various PLCs in a representative PWR plant, (b) a data transfer interface program linking the PLCs to a dynamic physics-based model of PWR plant and various components, (c) The physics-based models of the PWR plant and components, (d) the emulated PLCs in the protection and safety monitoring and operation I&C systems, and (e) the ManiPIO program for simulating cybersecurity events on the PLCs.
Accomplishments: (1) successfully compared digital and physical signatures of an open-source architecture PLC and an emulated PLC, (2) developed and tested the data interface linking various PLCs to developed PWR plant model, (3) developed and integrated emulated PLCs in representative PWR I&C systems architectures, (4) developed and tested integrated model of a representative PWR plant, (5) developed and demonstrated the developed ManiPIO program for simulating complex sequences of cybersecurity events on both emulated and commercial hardware PLCs, (6) characterized and improved performance of OpenPLC used in emulated PLCs, and (7) published results in nine conference papers, three refereed journal publication, and a book chapter.

Table of Contents

EXECUTIVE SUMMARY 5
LIST OF PUBLICATIONS 7
LIST OF FIGURES 10
ABBREVIATIONS 13
1. INTRODUCTION 15
2. DIGITAL I&C SYSTEMS IN A PRESSURIZED WATER REACTOR PLANT 18
2.1 Digital Instrumentation and Control 19
2.1.1. PWR Digital Safety I&C System 19
2.1.2. PWR Digital Operation I&C System 21
2.1.3. Overview of Components within Digital ICS 22
2.2. Cybersecurity in Commercial Nuclear Power Plants 26
2.2.1. Cybersecurity Threats Faced by Nuclear Power Plants 27
2.2.2. Cybersecurity Controls and Mitigation Strategies in Nuclear Power Plants 28
2.3 Summary 30
3. CYBERSECURITY INVESTIGATION CAPABILITIES AND THE LOBO NUCLEAR CYBERSECURITY PLATFORM 32
3.1 IAEA Asherah Nuclear Power Plant Simulator (ANS) 34
3.1.1 ANS Dynamic Model of a Pressurized Water Reactor Plant 35
3.1.2. Representative PWR Plant I&C System 37
3.1.3. ANS Communication Interface and Configuration and Attack Terminal 37
3.1.4. ANS Nuclear Cybersecurity Investigations 37
3.2 LOBO Nuclear CyberSecurity (LOBO NCS) Platform 38
3.2.1 Data Transfer Interface 40
3.2.2. Data Broker and Communication Interface 41
3.2.3. Graphical User Interface 42
3.2.4. ManiPIO Framework 42
3.2.5. A Representative PWR Plant Model 44
3.2.6. Emulated PLCs of I&C System in a Representative PWR 47
3.2.6.1. Protection and Safety Monitoring I&C System in a PWR Plant 47
3.2.6.1.1. The Core Protection Calculator PLC 47
3.2.6.1.2. Engineered Safety Features Actuation System PLC 50

3.2.6.1.3. Coincidence Logic Processor PLC 51
3.2.6.2. Plant Operation I&C System in a Representative PWR Plant 52
3.2.6.2.1. Reactor Power Regulation PLC 53
3.2.6.2.2. Pressure PLC 54
3.2.6.2.3. Pressurizer's Water Level PLC 56
3.2.6.2.4. Feedwater PLCs 57
3.2.6.2.5. Reactor Coolant Pump PLC 58
3.3. Summary 59
4. LOBO NCS CYBERSECURITY INVESTIGATIONS FOR A REPRESENTATIVE PRESSURIZED WATER REACTOR PLANT 61
4.1 Steam Generator Nominal Operation and when Targeted by an FDIA 62
4.1.1 Response of Representative PWR SG Model with a Simulated FDIA 64
4.2 Simulated Nominal Startup Transient of Representative PWR Plant 64
4.3. Simulated Startup with an FDIA Targeting Pressure PLC 70
4.4. Simulated Startup with an FDIA Targeting Core Protection Calculator PLC 72
4.5. Summary 75
5. AUTONOMOUS REMOTE CONTROL AND CYBERSECURITY INVESTIGATIONS OF SPACE REACTOR POWER SYSTEMS 77
5.1 Digital Twin Concept 77
5.2. Description of CBC Space Reactor Power System 79
5.3. Dynamic Model of S^4 CBC Space Reactor Power System 83
5.4. DynMo-CBC Model and Emulated PLCs 84
5.5. Applications to Cybersecurity Investigations 87
5.5.1 Nominal Startup of DynMo-CBC Power System without an FDIA 88
5.5.2. Response to Simulated Cyberattack on Drum PLC 92
5.6. Summary 93
6. SUMMARY AND CONCLUSIONS 94
7. ACKNOWLEDGEMENTS 96
8. REFERENCES 97

EXECUTIVE SUMMARY

Digital Instrumentation and Control (I&C) systems are effective in achieving high operation efficiency and reliability in industrial installations. However, digital Industrial Control Systems (ICS) and Operation Technology (OT) networks in all sectors of the economy have been of late the targets of an ever-growing number of cyberattacks. Examples are industrial facilities, food processing and packaging plants, defense facilities, water treatment plants, oil refineries, transportation, and other infrastructures. The OT networks in industrial installations, including nuclear power plants are primarily designed for efficiency, safety, and operation reliability but not to same cybersecurity scrutiny of the enterprise Information Technology (IT) systems. Reported cyberattacks targeted the Programmable Logic Controllers (PLCs) for control and operation. Digital I&C systems have markedly improved the operation, reliability, and safety of nuclear reactor plants, significantly increased their load factors, and supported power up rates and operation life extensions. Despite operating within fully isolated networks, potential cyber-vulnerabilities of I&C systems in nuclear power plants need to be investigated. This prompted efforts to develop high-fidelity cybersecurity platforms for research, education, and training.

The Nuclear Instrumentation & Control Simulation (NICSim) development effort 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 2018 DOE NEUP award, is the subject of this report, address some of these needs. As part of this effort the LOBO Nuclear CyberSecurity (LOBO NCS) platform links emulated PLCs in the I&C systems of a representative Pressurized Water Reactor (PWR) plant to Matlab Simulink physics-based, dynamic models of the integrated plant and components. The efficient data transfer interface and broker in the LOBO NCS platform manage and coordinate communication between the emulated PLCs and the Simulink physics-based models. The Manipulate Process I/O (ManiPIO) cybersecurity testing and evaluation program in the LOBO NCS platform simulates cybersecurity events targeting emulated and hardware PLCs in I&C systems. The modular and highly flexible elements in the platform support applications to different I&C systems and nuclear power plant designs.

The linked component models into that of a representative PWR plant include: (a) a reactor dynamic thermal-hydraulics coupled to 6-groups point kinetics; (b) thermal-hydraulics of the primary and secondary loops linking the reactor to a 3-region Pressurizer Model and a simplified Steam Generator Model, and (c) reactor primary coolant pumps. The Simulink physics-based models integrated into that of the plant solve the overall mass, momentum, and energy balance equations for coolant flow rate and temperatures throughout the primary side of the plant. The emulated PLCs in the LOBO NCS for the PWR plant's protection and safety monitoring system can autonomously trip the reactor and actuate the engineered safety systems when monitored plant conditions exceed programed safety setpoints. The PLCs in the Plant Operation I&C system regulate the reactor power, the system pressure, the water level in the pressurizer, the feedwater flow for adjusting the water level in the steam generator, and the shaft rotation speed of the reactor primary coolant pumps.

In this report, simulated cyber-attacks of a representative PWR plant and components and of a space nuclear reactor power system with multiple CBC loops are conducted using the LOBO NCS platform. Results of simulated nominal operation transients are compared to those when an

emulated PLC is subject to a Modbus TCP False Data Injection Attack (FDIA). In these investigations a representative PWR steam generator model is coupled to an emulated Feedwater PLC following a simulated 10% increase in stream demand. Nominally, the Feedwater PLC maintains the water level in the SG close to its preprogramed setpoint. A simulated FDIA using the ManiPIO program succeeded in manipulating this PLC to maintain a constant feedwater injection during the simulated transient, causing a rapid decline in the water level in the SG.

The LOBO NCS platform also investigated the effect of a Modbus TCP FDIA on the Pressure PLC during a simulated reactor startup transient. The applied FDIA manipulated the PLC by writing a low system pressure to its memory register to turn on the submerged proportional and backup heaters and raise the system pressure. The increase in the flash evaporation rate by the submerged heaters in the pressurizer rapidly increased the system pressure. The pressure peaked at 18.238 MPa, which is 2.553 MPa higher than nominal value. The LOBO NCS platform also investigated a simulated FDIA on the Core Protection Calculator PLC in the plant safety I&C system. This FDIA manipulated the PLC to vote to trip the reactor by overwriting a false high value of the reactor inlet temperature.

To demonstrate versatility the LOBO NCS platform is also used to simulate a startup of the S^4 CBC space reactor power system for nominal operation and when the PLC for the control drums within the radial reflector are targeted by a simulated FDIA. The simulated FDIA wrote a false higher rotation rate of the control drums to the PLC's memory register. This increased the external reactivity insertion raising the reactor thermal power and hence, the core and coolant temperatures throughout the power system. Although, the calculated temperatures during this simulation remained below the melting points for the fuel and structural materials, the rapid increase in temperature could induce undesirable thermal stresses within the reactor and the CBC energy conversion loops.

The LOBO NCS Platform developed as part of the NICSim effort provides capabilities to aid in the development of cyber-secure digital I&C systems for current and advanced nuclear power plants. This platform can help investigate cyber-vulnerabilities of current and proposed I&C system architectures and analyze potential effects of upgrades and modifications. It could also help researchers evaluate different defensive measures and cybersecurity monitoring programs to detect and stop potential threats and train professionals and students on detecting signs of a potential cyber-compromise within the plant. ***The results of this effort have been documented and disseminated widely in the publications listed in the next subsection***

LIST OF PUBLICATIONS

The results of the conducted research are documented in technical reports and refereed journal and conference proceeding and Transactions publications. See complete list below:

Technical Reports

El-Genk, Mohamed S., Timothy Schriener, Christopher Lamb, Raymond Fasano, Andrew Hahn, 2019, Implementation and Validation of PLC Emulation and Data Transfer. **Progress Report UNM-ISNPS-02-2019**, Institute for Space and Nuclear Power Studies (ISNPS), University of New Mexico, July 2019.

El-Genk, Mohamed S., Timothy Schriener, Christopher Lamb, Raymond Fasano, Andrew Hahn, 2019, Identification and Characterization of Safety Monitoring and Control Systems. **Progress Report UNM-ISNPS-03-2019**, Institute for Space and Nuclear Power Studies (ISNPS), University of New Mexico, August 2019.

El-Genk, Mohamed S., Timothy Schriener, Andrew Hahn, Ragai Altamimi, 2020, A Physics based, Dynamic Model of a Pressurized Water Reactor Plant with Programmable Logic Controllers for Cybersecurity Applications. **Progress Report UNM-ISNPS-02-2020**, Institute for Space and Nuclear Power Studies (ISNPS), University of New Mexico, July 2020.

El-Genk, Mohamed S., Timothy Schriener, Andrew Hahn, Ragai Altamimi, Raymond Fasano, Christopher Lamb, 2020, Emulated Programmable Logic Controllers for the Protection and Safety Monitoring and Operation I&C Systems in a Representative PWR Plant for Cybersecurity Applications. **Progress Report UNM-ISNPS-03-2020,** Institute for Space and Nuclear Power Studies (ISNPS), University of New Mexico, October 2020.

El-Genk, Mohamed S., Timothy Schriener, Andrew S. Hahn, Raymond E. Fasano, Christopher Lamb, 2021, Validation of LOBO Nuclear CyberSecurity (LOBO NCS) Platform and Demonstration of Manipulate Process I/O (ManiPIO) Framework for Cybersecurity Testing and Evaluation. **Technical Report ISNPS-UNM-01-2021,** Institute for Space and Nuclear

El-Genk, Mohamed S., Timothy Schriener, Andrew S. Hahn, Asmaa Salem, 2022, Integration and Characterization Testing of the LOBO Nuclear CyberSecurity (LOBO NCS) Platform and OpenPLC. **Technical Report ISNPS-UNM-01-2022**, Institute for Space and Nuclear Power Studies (ISNPS), University of New Mexico, July 2022.

Peer Reviewed Journal Papers

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

El-Genk, M.S., T.M. Schriener, "A Cybersecurity Platform for Simulating Transient Responses of Emulated Programmable Logic Controllers in Instrumentation and Control Systems for a PWR plant," ***J. Cyber Security Technology,*** 6:1-2 (2021) 65 - 90.

Schriener, T.M., M.S. El-Genk, "Simulated False Data Injection Attacks on Emulated and Hardware Programmable Logic Controllers of the Pressurizer in a Representative Pressurized Water Reactor Plant," ***J. Cyber Security Technology,*** in press (2022).

Book Chapter

El-Genk, M. S., and T. M. Schriener, *Modeling and Simulation Capabilities for Nuclear Cybersecurity Investigations of a Representative PWR Plant and Space Reactor Power Systems*, **in Nuclear Power Plants: Recent Progress and Future Directions**, John K. Campton, Editor, Nova Science Publishers, Inc., Chapter, 1, 2022.

Conference full Papers

Hahn, A., T. Schriener, M.S. El-Genk, "Selection and Validation of Fast and Synchronous Interface to the Controller of a Space Nuclear Reactor Power System," *Proc. 28th International Conference on Nuclear Engineering (ICONE28),* ICONE28-POWER2020-16237, Anaheim, CA, USA, 2-6 August 2020.

El-Genk, M.S., T. Schriener, R. Altamimi, A. Hahn, C. Lamb, R. Fasano, "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.

Fasano, R, C. Lamb, M.S. El-Genk, T. Schriener, A. Hahn, "Simulation Methodology of Programmable Logic Controllers for Cybersecurity Applications," *Proc. 28th International Conference on Nuclear Engineering (ICONE28),* ICONE28-POWER2020-11150, Anaheim, CA, USA, 2-6 August 2020.

Schriener, T.M., M. S. El-Genk, "Response of Programmable Logic Controllers of the Pressurizer in a Representative PWR Plant Following a False Data Injection," ***ANS 12th Nuclear Plant Instrumentation, control and Human-Machine Interface Technologies,*** Paper No. 34539, Providence, RI, 13-17 June 2021, 1361 - 1371.

El-Genk, M.S., T. Schriener, A. Hahn, R. Fasano, C. Lamb, "LOBO Nuclear Reactor Plants CyberSecurity (LOBO-NCS) Platform," ***ANS 12th Nuclear Plant Instrumentation, control and Human-Machine Interface Technologies,*** Paper No. 34512 , Providence, RI, 13-17 June 2021, 1417 – 1426.

Conference Transactions Summaries

Hahn, A., M.S. El-Genk, T.M. Schriener, "Programmable Logic Controller of a Pressurized Water Reactor Core Protection Calculator, ***Trans. Am. Nucl. Soc. Virtual Meeting.*** *Technical Session:* Cybersecurity for Nuclear Installation-II, 8-11June 2020, p. 135,

El-Genk, M.S., T.M. Schriener, C.C. Lamb, "Nuclear Instrumentation and Control Simulation (VICSim) Platform for Investigating Cybersecurity Risks," ***Trans. Am. Nucl. Soc Virtual Meeting.*** *Technical Session:* Cybersecurity for Nuclear Installation-II, 8-11June 2020, p. 133,

Altamimi, R.M., M.S. El-Genk, T.M. Schriener, "Pressurizer Model and PLCs for Investigation of Cybersecurity of PWR Plants," ***Trans. Am. Nucl. Soc. Virtual Meeting.*** *Technical Session:* Cybersecurity for Nuclear Installation-II, 8-11June 2020, p. 137,

Schriener, T.M., M.S. El-Genk, "Steam Generator Model and controller for Cybersecurity Analyses of Digital I&C Systems in PWR Plants," ***Trans. Am. Nucl. Soc. Virtual Meeting.*** *Technical Session:* Cybersecurity for Nuclear Installation-II, 8-11June 2020, p. 139.

Workshop presentations / Summary

El-Genk, MS, NICSim: Nuclear Instrumentation and Control Simulation for Evaluating Response to Cyber-attack," Sandia National Laboratories' Research Spotlight Forum- Cyber Security, Albuquerque, NM, 6 August 2019. https://digitalops.sandia.gov/Mediasite/Play/d54f41efcc0241afbce2c027403e6ab41d.

List of Figures

Fig. 2.1. A layout of the reactor trip protection I&C systems with associated sensors in a representative PWR plant (El-Genk, et al. 2020). 20
Fig. 2.2. Control hierarchy used within digital industrial control systems (El-Genk and Schriener 2022). 21
Fig. 2.3. Westinghouse Core Protection Calculator rack mounted PLC with signal input/output modules (images from US NRC). 23
Fig. 2.4. Digital I&C systems with sensor measurements and actuator signals communicated directly to PLC or indirectly through plant internal network (El-Genk and Schriener 2022). 26
Fig. 3.1. A block diagram of the ANS platform for nuclear plant cybersecurity investigations (adapted from Busquim e Silva, et al. 2021). 34
Fig. 3.2. A block diagram of a representative PWR plant and I&C system in ANS (Busquim e Silva, et al. 2021). 35
Fig. 3.3. A block diagrams of the LOBO NCS platform for a representative PWR plant and the emulated PLCs in the I&C systems (El-Genk, et al. 2021). 40
Fig. 3.4. A schematic of the structure of ManiPIO framework in LOBO NCS (El-Genk, et al. 2021). 42
Fig. 3.5. Developed physics-based components model of a representative PWR plant in LOBO NCS platform (El-Genk et al. 2020). 44
Fig. 3.6. A layout of the digital I&C systems of a representative PWR plant in the LOBO NCS Platform: (a) Reactor safety I&C system, (b) Plant operation I&C system (El-Genk, et al., 2021). 45
Fig. 3.7. A schematic of the instrumentation's layout in a representative PWR (El-Genk and Schriener 2022). 48
Fig. 3.8. A layout of the instrumentation sensors for the coolant in the I&C systems of a representative two loop PWR plant (El-Genk and Schriener 2022). 49
Fig. 3.9. Determination of CHFR, the temperature margin of the coolant exiting the reactor core, and the shaft rotation speed of the reactor pumps, for actuating the CPC safety functions (El-Genk and Schriener 2022). 50
Fig. 3.10. A block diagram of the Engineered Safety Features Actuation System functions in PLC for a representative PWR plant (El-Genk and Schriener 2022). 51
Fig. 3.11. Block diagram of control program of the reactor power regulation PLC in LOBO NCS (El-Genk and Schriener 2022). 52
Fig. 3.12. An illustration of the measurement's sensors of the pressurizer in a representative PWR plant (El-Genk and Schriener 2022). 53
Fig. 3.13. A block diagram of the control program of the Pressure PLC in the LOBO NCS platform (El-Genk and Schriener 2022). 54
Fig. 3.14. A control program for a representative pressurizer Water Level PLC (El-Genk and Schriener 2022). 55
Fig. 3.15. Instrumentation arrangements in SG of a representative PWR plant in LOBO NCS platform (El-Genk and Schriener 2022). 56
Fig. 3.16. Block diagram of control program of SG's Feedwater PLCs in the LOBO NCS platform (El-Genk and Schriener 2022). 58

Fig. 3.17. Block diagram of a PI controller program logic for PLCs of reactor primary coolant pumps in LOBO NCS platform (El-Genk and Schriener 2022). 59
Fig. 4.1. Linked SG model to secondary loop in a representative PWR plant (El-Genk, et al. 2021). 61
Fig. 4.2. Results of simulated transient of SG linked to the Feedwater PLC following a 10% increase in steam demand during of nominal operation and when the PLC is a target to a simulated FDIA by ManiPIO program in the LOBO NCS Platform (El-Genk, et al. 2021). 63
Fig. 4.3. Calculated state variables of a representative PWR plant using the reactor Simulink model during simulated startups without and with a FDIA (El-Genk and Schriener 2022). 65
Fig. 4.4. Calculated state variables of a representative PWR plant using the pressurizer Simulink model linked to the Pressure PLC during a simulated startup without and with an FDIA (El-Genk and Schriener 2022). 66
Fig. 4.5. Calculated state variables of a representative PWR plant using the primary loop Simulink model linked to the pressurizer Water Level PLC during a simulated startup without and with an FDIA (El-Genk and Schriener 2022). 67
Fig. 4.6. Calculated state variables of a representative PWR plant using the SG Simulink model linked to Feedwater PLC during a simulated startup without and with an FDIA (El-Genk and Schriener 2022). 68
Fig. 4.7. Calculated state variables of a representative PWR plant using the linked Simulink model of the reactor coolant pump to the pumps PLCs during a simulated startup without and with an FDIA (El-Genk and Schriener 2022). 70
Fig. 4.8. Calculated state variables of a representative PWR plant using the primary loop Simulink model linked to the pressurizer Water Level PLC during a simulated startup without and with an FDIA targeting one of the four Core Protection Calculator PLCs (El-Genk and Schriener 2022). 73
Fig. 4.9. Calculated CHFR and trip voting signals for emulated Core Protection Calculator during simulated startup without and with an FDIA targeting the PLC (El-Genk and Schriener 2022). 74
Fig. 5.1. A generic space nuclear reactor power system for electric thrusters and for science payload (PHTS: primary heat transport system). 78
Fig. 5.2. Radial cross views of the S^4 reactor core and fuel stacks – coolant channels unit cell (El-Genk, Tournier, Gallo 2010). 80
Fig. 5.3. A layout of the DynMo-CBC integrated space reactor power system (El-Genk, Tournier, Gallo 2010). 81
Fig. 5.4. Cutaway and isometric views of single-shaft UNM-BRU-1 unit (Gallo and El-Genk 2009). 82
Fig. 5.5. A schematic of the fully deployed S^4 CBC space reactor power system (El-Genk, Tournier, Gallo 2010). 83
Fig. 5.6. A block diagram of the implemented DynMo-CBC space reactor power system model and emulated PLCs in the LOBO NCS platform. 85
Fig. 5.7. Changes in BOL hot-clean external reactivity insertion, ρ_{ex}, into the S^4 reactor core as a function of the rotation angle, θ, of the B4C/BeO rotating control drums in the BeO radial reflector (Hahn, Schriener, El-Genk 2020). 86

Fig. 5.8. Control variables of the DynMo-CBC space reactor power system during a simulated startup without and with a FDIA (El-Genk and Schriener 2022). 89
Fig. 5.9. Calculated S^4 reactor variables during the simulated startups without and with a FDIA (El-Genk and Schriener 2022). 90
Fig. 5.10. CBC space nuclear power system state variables in the CBC loops during the system startup nominally and with a FDIA (El-Genk and Schriener 2022). 91

ABBREVIATIONS

ADAPT	Analysis of Dynamic Accident Progression Trees
AFAS	Auxiliary Feedwater Actuation System
AI	Artificial Intelligence
ALIP	Annular Linear Induction Pump
ANS	Asherah Nuclear Power Plant Simulator
APNS	Asherah Pi Nuclear Simulation
BOL	Beginning-of-Life
BRU	Brayton Rotating Unit
CAT	Configuration and Attack Terminal
CBC	Closed Brayton Cycle
CEA	Control Element Assembly
CHFR	Critical Heat Flux Ratio
CIAS	Containment Isolation Actuation System
CMAC	Cerebellar Model Articulation Controller
CPC	Core Protection Calculator
CVCS	Chemical and Volume Control System
DCS	Distributed Control System
DET	Dynamic Event Tree
DOS	Denial of Service
DPT	Differential Pressure Transducers
DynMo-CBC	Dynamic Model – Closed Brayton Cycle
EC	Event Constructor
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FDD	Fault Detection Determination
FDIA	False Data Injection Attack
FPGA	Field Programmable Gate Array
GUI	Graphical User Interface
HDL	Hardware Description Language
HIL	Hardware-in-the-Loop
HMI	Human-Machine Interface
IAEA	International Atomic Energy Agency
IAPWS-IF97	International Association for the Properties of Water and Steam 1997 Formulation
I/O	Input/Output
ICS	Industrial Control System
I&C	Instrumentation and Control
IPC	Inter-Process Communication
IT	Information Technology
LOBO NCS	LOBO Nuclear CyberSecurity
LOCA	Loss of Coolant Accident
LSTM	Long Short-Term Memory
ManiPIO	Manipulate Process Input/Output
MitM	Man-in-the-Middle
ML	Machine Learning

M&M	Man-Machine
MSIS	Main Steam Isolation System
NAMAC	Nearly Autonomous Management and Control
NRC	Nuclear Regulatory Commission
NSGA-II	Non-dominated Sorting Genetic Algorithm II
OPC-UA	Open Platform Communications-Universal Architecture
OT	Operation Technology
PHTS	Primary Heat Transport System
PI	Proportional-Integral
PID	Proportional-Integral-Differential
PLC	Programmable Logic Controller
PMA	Permanent Magnet Alternator
PMS	Protection and Safety Monitoring System
PWR	Pressurized Water Reactor
RPM	pump rotational speed (RPM)
RPM_c	pump rotational speed from characteristics (rpm)
RTD	Resistance Temperature Detector
RTS	Reactor Trip System
RTU	Remote Terminal Unit
S^4	Submersion Subcritical Safe Space
SCADA	Supervisory Control and Data Acquisition
SCS	Supervisory Control System
SG	Steam Generator
SIAS	Safety Injection Actuation System
SMR	Small Modular Reactor
SNL	Sandia National Laboratories
SVM	Support Vector Machine
UNM-ISNPS	University of New Mexico's Institute for Space and Nuclear Power Studies
VM	Virtual Machine
WLAN	Wireless Local Area Network

1. INTRODUCTION

Digital Industrial Control Systems (ICSs) are in common use in critical industrial infrastructures for energy generation and transmission such as electrical power plants, smart transmission grids, transportation systems, factories, chemical and manufacturing plants, oil refineries, aerospace, transportation, and water treatment plants. They are versatile and facilitate higher performance than older analog control systems (National Research Council 1997; Korsah, et al. 2008). During the last four decades, replacing the analog with digital Instrumentation and Control (I&C) systems in existing commercial nuclear power plants in the USA and abroad, enhanced safety and reliability, supported power uprates, and increased availability or load factor by minimizing down times (National Research Council 1997; Korsah, et al. 2008; Gallier 2021). The load factor of nuclear reactor plants in the US is currently averaging > 92% compared to ~ 65% in late 1980s using analog control (Gallier 2021). The Generation II and III+ reactor plants currently in operation and under construction use partial or entirely digital I&C systems for autonomous control and to activate safety and protection systems (Korsah, et al. 2008).

In recent years, digital ICSs in industrial and energy infrastructures worldwide have been targets of multiple cyberattack campaigns. Notable examples are the Crashoverride and Blackenergy campaigns against the electrical transmission infrastructure in Ukraine, and the Stuxnet campaign against the Iranian uranium enrichment program (Dragos Inc. 2017; Karnouskos 2011). The Stuxnet campaign exploited cyber-vulnerabilities in the specialized digital Programmable Logic Controller (PLC) computers. Unlike enterprise Information Technology (IT) networks, Operation Technology (OT) networks in ICSs frequently do not have the same levels of safeguards and defensive technologies against potential cyberattacks. They have relied heavily on physical and network isolation to protect against cyberattacks. However, sophisticated cyber campaigns have proved capable of reaching even highly isolated systems. Therefore, it is imperative to assess and evaluate potential cyber-vulnerabilities of current and future I&C architectures in nuclear power plants (US Department of Homeland Security 2015; Nuclear Energy Institute 2010; National Research Council 1997).

Nuclear power plants typically employ separate I&C systems for semi-autonomous control and to conduct safety and protection functions. These systems comprise of a variety of digital ICS control devices including PLCs, Remote Terminal Units (RTUs), Field Programmable Gate Array (FPGA) devices, and Distributed Control Systems (DCSs). The autonomous safety systems provide the regulatory functions of initiating a reactor trip and/or actuating the Engineered Safety Features (ESF) (Korsah, et al. 2008). The digital I&C systems also assist the plant operators monitoring the plant operation and provide supervisory control capabilities. Currently, the regulator requires commercial nuclear power plants to develop cybersecurity plans for their I&C systems (Nuclear Energy Institute 2010).

The I&C systems operate either semi- or fully autonomous and send command signals to the plant's control systems mostly independent of the plant operators' actions. Therefore, a cyber-compromise of a digital I&C system within a nuclear power plant could potentially enable a hostile actor to alter the plant's operation and compromise safety. The expanding uses of digital I&C systems have placed an increased need for conducting high-fidelity cybersecurity research and training platforms capable of investigating potential vulnerabilities of these systems.

This report describes and documents the Nuclear Instrumentation and Control Simulation (NICSim) effort developed at the University of New Mexico's Institute for Space and Nuclear Power Studies (UNM-ISNPS) in collaboration with Sandia National Laboratories (SNL) (El-Genk et al., 2020a, 2020b, 2020c) under a 2018 award by the Department of Energy (DOE)

Nuclear Engineering University Program (NEUP). This effort also developed the LOBO NCS platform to investigate cyber-vulnerabilities of digital I&C systems in nuclear power plants. 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. The NICSim platform is modular and compatible with the DOE SCEPTRE cybersecurity framework at SNL (Camacho-Lopez 2016). It 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.

The LOBO Nuclear CyberSecurity (LOBO NCS) Platform developed based on the NICSim architecture (El-Genk, et al., 2021; El-Genk and Schriener 2022), links physics-based Simulink models of a representative PWR plant and components to emulated PLCs in the plant's I&C systems using a fast and reliable data transfer interface and broker program. It includes a user-friendly graphic interface with plotting capabilities for a real-time display of simulation results and incorporates the Manipulate Process Input/Output (ManiPIO) framework developed by SNL to simulate cybersecurity events on both emulated and hardware PLCs.

Section 2 - Digital I&C Systems in a Pressurized Water Reactor Plant reviews digital I&C systems in nuclear plants. This section describes the types and functions of several types of ICS devices used in digital I&C systems of a representative PWR plant and the types of cybersecurity protection measures implemented. This section discusses the different digital I&C systems assisting plant operator and providing semi-autonomous operation of the control systems, as well as those providing the autonomous safety functions. It also reviews types of cyber-threats which may target I&C systems and the cybersecurity protections and controls measures.

Section 3 - Cybersecurity Investigation Capabilities and the Lobo Nuclear CyberSecurity Platform reviews reported work on developing modeling and simulation platforms for conducting cybersecurity investigations of nuclear power plants and presents the LOBO NCS platform (El-Genk, et al., 2021; El-Genk and Schriener 2022). It describes the physics-based component models of a representative PWR plant, and the emulated PLCs developed for the plants Operation and Protection and Safety Monitoring I&C systems.

Section 4 - LOBO NCS Cybersecurity Investigations for a Representative Pressurized Water Reactor Plant presents the results of performed cybersecurity investigations using the LOBO NCS platform, linking developed Matlab Simulink physics-based models of a representative PWR plant and components to those of emulated PLCs in the I&C system. Results demonstrate the reliability and the fidelity of the emulated PLCs to control the PWR plant model during simulated nominal transient and of the same transient while the emulated PLCs are subject to simulated FDIAs. Presented results are of the steam generator model linked to an emulated Feedwater PLC during a nominal transient following an increase in steam demand. The simulated FDIA targeting the Feedwater PLC attempts to overwrite its Modbus input registers. Also presented are the results of simulating a startup of a representative PWR linked to the emulated PLCs in the I&C system.

Section 5 - Autonomous Remote Control and Cybersecurity Investigations of Space Reactor Power Systems describes the application of the LOBO NCS platform for cybersecurity investigations of a space nuclear reactor power system concept developed at UNM-ISNPS. It comprises a Submersion Subcritical Safe Space (S^4) gas cooled nuclear reactor with sectored core (King and El-Genk 2007) and three recuperated Closed Brayton Cycle (CBC) energy conversion loops, each with multiple water heat pipes heat rejection radiator panels (El-Genk, Tournier, Gallo 2010). The integrated S^4-CBC power system Matlab Simulink model linked to

the emulated PLCs controlling the reactor reactivity and the shaft rotation speed of the CBC turbomachine units. Presented results are of investigating the ability of the emulated PLCs during a power system startup scenario, both during nominal operation and while the controller is targeted by a cyberattack.

2. DIGITAL I&C SYSTEMS IN A PRESSURIZED WATER REACTOR PLANT

Generation II nuclear power plants had been mostly built with analog I&C systems. These plant I&C systems were comprised of analog calculators and logic circuits, which determined control outcomes based on the received sensors measurements in the plant. In accordance with the determined outcome of the logic circuit the system would then generate appropriate control signals to actuate related mechanisms in the plant's control and safety systems. In PWR plants, the analog logic circuits in the safety I&C systems used to actuate either a reactor trip or the ESF when the monitored state variables and the calculated parameters exceed preprogramed setpoints. Examples include the system pressure, the water levels in the pressurizer and the steam generator, the Critical Heat Flux Ratio (CHFR) in the nuclear reactor core, the shaft rotation speed for the main reactor coolant pumps, and the feedwater flow rate to the steam generator. When exceeding the preprogramed setpoints, an analog voltage or current signal is sent to the circuit bistables of the breakers to trip the reactor or to actuate the plant's ESF equipment.

During the 1970's and 1980's, the analog logic circuits in the safety I&C systems for operating nuclear plants in US were supplemented with digital PLCs to enhance safety and reduce incidents of operation transients with scram (Hung 2010; National Research Council 1997). These specialized computing systems introduced in the 1960's was already in widespread use in ICS in other industries. Combustion Engineering was an early pioneer in the use of PLCs in PWRs, developing digital Core Protection Calculators (CPCs) which performed the reactor trip protection safety function for the plant. The versatility of the CPCs enabled programming modifications of the control functions without requiring costly rewiring as is the case with analog systems (Hung 2010). This allowed plants to add additional safety monitoring and trip protection functions to the I&C systems using the same reactor trip circuits.

Digital I&C systems possess advantages over analog systems. Analog sensors and logic circuits can suffer drift that results in them losing their calibration over time. This can change the control system's response to operational transients which can result in unintended reactor trips shutting down the plant (National Research Council 1997). Digital logic controllers help eliminate the issue of controller drift and they can employ software to try to correct for expected sensor measurement drift. These computing systems also provide superior capabilities for self-diagnostics and fault detection to identify equipment malfunctions and aid plant maintenance (National Research Council 1997).

At present, the I&C systems in many of the operating nuclear plants in the US comprise a mixture of analog and digital components, although many plants include at least some digital systems (Korsah, et al. 2008). Early implementation of digital I&C systems has succeeded in reducing the frequency of unintended plant trips and decreased the maintenance burden on plant personnel (National Research Council 1997). This has contributed to very impressive average load factor values for the operating nuclear power plant fleet in the US, which has remained steady in the low to mid 90% to date (Gallier 2021). They have also supported power uprates as more precise operation of PLCs in safety I&C systems compared to analog systems helped existing plants recover safety margin for parameters like the CHFR (Hung 2010; Wierman et al. 2001). These have combined to allow the US fleet of 94 operating reactors in 2020 to generate 37% more electricity than the larger fleet of 112 reactors did 30 years earlier (Gallier 2021). Another factor that has helped drive adoption of digital I&C systems in the nuclear fleet is the lack of vendors supplying components for the older analog systems, making maintaining them

difficult and costly (National Research Council 1997).

While digital I&C systems have provided considerable benefits to commercial nuclear power plants, they have also introduced potential cyber-vulnerabilities into these plants (Korsah, et al. 2008). While nuclear power plants are highly secure and resilient industrial facilities, a wide range of industrial facilities worldwide have been targets of cyberattack campaigns of increasing sophistication (Hemsley and Fisher 2018; Dragos Inc. 2017; Karnouskos 2011). These potential threats necessitate implementing cybersecurity controls and protection systems to guard against hostile actors both outside and inside the facility (Nuclear Energy Institute 2010). This section provides a brief review of digital I&C systems in commercial PWR plants including a discussion of the types of components commonly found in these systems. The section also discusses the cybersecurity controls and protections measures being implemented within the I&C systems in current nuclear power plant, including a discussion of postulated cyber threats.

2.1. Digital Instrumentation and Control

Digital I&C systems in nuclear power plants fall into two categories: the safety and protection I&C system which serves a regulatory safety function for the plant, and the non-safety or operation I&C system which assists the human operators in monitoring and controlling the normal operation of the plant. US NRC licensing requirements are mostly concerned with the former, safety related digital I&C systems with far fewer regulations governing the nature of the non-safety operational I&C systems in the plant (National Research Council 1997). The safety and operational control I&C systems rely on independent instrumentation, networking, and computer cabinets, and may utilize different computer hardware models for their digital components for added diversity (Schindhelm and Single 2010; Crew 2011). Such separation and diversity support the nuclear industry's defense-in-depth philosophy to plant safety, helping ensure that a failure in one will not cause a failure in the other (National Research Council 1997). This eliminates the risk that an isolated sensor failure or computer malfunction will compromise both systems. Equipment diversity also guards against common cause failures where a flaw in each device model does not compromise other plant's systems.

2.1.1. PWR Digital Safety I&C System

The safety I&C system within a nuclear plant is frequently referred to as the Plant Protection System or Protection and Safety Monitoring System (PMS). It consists of the Reactor Trip System (RTS) for the reactor autonomous trip function and the Engineered Safety Features Actuation System (ESFAS) autonomously activate the reactor's ESF (National Research Council 1997). The plant operator can also activate these systems manually, with the safety I&C system autonomously acting when indicated by its programming in the event the human operators do not act first. Both the RTS and ESFAS comprise sensor instruments and logic computers to monitor the conditions in the plant, and equipment to generate the analog and/or digital signals to trip the reactor and activate the ESF if the measured plant state variables reach their defined setpoints. They can also help alert the operators to take a corrective action when the monitored state variables and parameters approach trip and actuation setpoints.

The safety I&C system consists of four parallel safety measurement divisions or channels which are electrically and physically separate from one another. Fig. 2.1 shows a layout of a representative PWR plant and the reactor trip I&C system (El-Genk, et al. 2020). The figure shows the types of measurement sensors within each one of the four safety channels. The sensor measurements for the reactor include those of the vertical position of the control assemblies in the reactor core, and the ex-core reactor neutron flux detectors embedded in the shielding outside

the reactor vessel. The control rod position can be measured by electromagnetic position sensors that react to the movement of the control rod assembly drive shafts and/or by counting the electric pulses sent to the drive mechanisms. The ex-core nuclear instrumentation employs neutron flux detectors such as fission ion chambers and gas proportional counters which are calibrated to relate the level of the measured neutron flux to the reactor power. Plants may employ separate detectors which are tailored for low power operation during startup to supplement the power range neutron detectors used during normal operation.

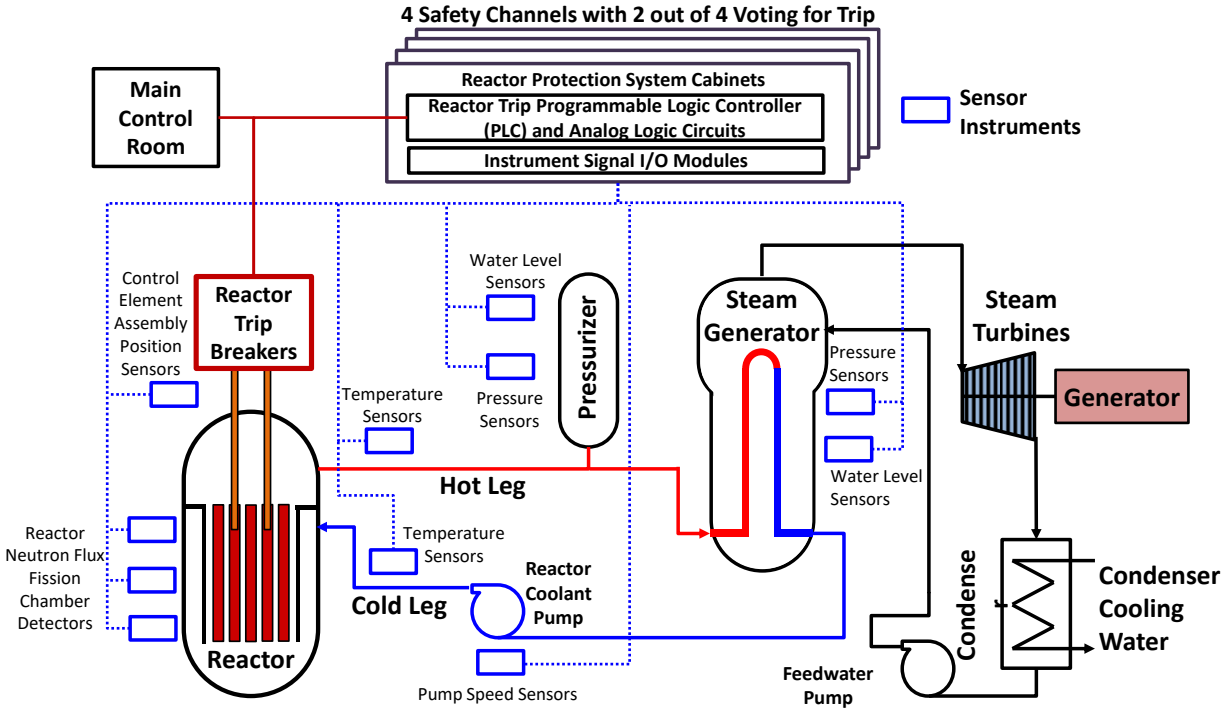


Fig. 2.1. A layout of the reactor trip protection I&C systems with associated sensors in a representative PWR plant (El-Genk, et al. 2020).

The reactor inlet and exit temperatures for the primary coolant loop are measured using Resistance Temperature Detector (RTD) platinum resistance thermometers placed in thermowells in the walls of the hot and cold leg ducts (Fig. 2.1). The sensors for the pressurizer and the steam generator indicate the system pressure and the water level. Pressure transducers indicate the system pressure in the pressurizer and steam generator. The water level in the pressurizer is calculated from the water static pressure head measured by Differential Pressure Transducers (DPTs). The rotation speed for the primary reactor coolant pumps is measured by magnetic speedometers. These sensors determine the speed from the frequency of an induced electric current created by the sensor intersecting the magnetic field lines produced by magnetic polls located on the teeth of a slotted metal disk mounted to the shaft.

The four channels or divisions of these measurements are communicated to separate PLCs in the reactor protection system of the plant (Fig. 2.1). The Input/Output (I/O) modules on the PLCs receive the analog and digital signals from each instrument and convert them to digital input values for use in the PLC's logic programming. The PLCs for the four parallel divisions each generate a separate voting signal on whether to initiate a reactor trip or actuate one or more of the plant's ESFs. The actuation logic for the reactor trip and ESF actuation normally uses 2/4 voting

coincidence. This means that any combination of at least two of the four divisions' PLCs must vote to act for the system to signal to either trip the reactor or activate one or more of the safety systems. This arrangement ensures that a false signal due to a single malfunctioned instrument or computer would not accidently trigger a shutdown or spurious ESF actuation. Non-essential safety functions for which the effect of an accidental actuation on plant operation is of lower consequence employ less stringent 1/2 voting coincidence.

2.1.2. PWR Digital Operation I&C System

The other category of digital I&C systems in commercial PWRs are the non-safety operation I&C systems which provide semi-autonomous control and monitoring of the plant operation (National Research Council 1997). The plant monitoring systems collect and display data on the different plant systems to assist the operators in maintaining the desired operation conditions of the plant. These systems can alarm the operators when the plant's operation condition approaches a reactor trip or safety system actuation setpoint so the operators can take preemptive corrective action. The computers in the plant monitoring system also record the plant's operational history for further analysis. This data can be used to monitor performance degradation and assist in planning preemptive maintenance.

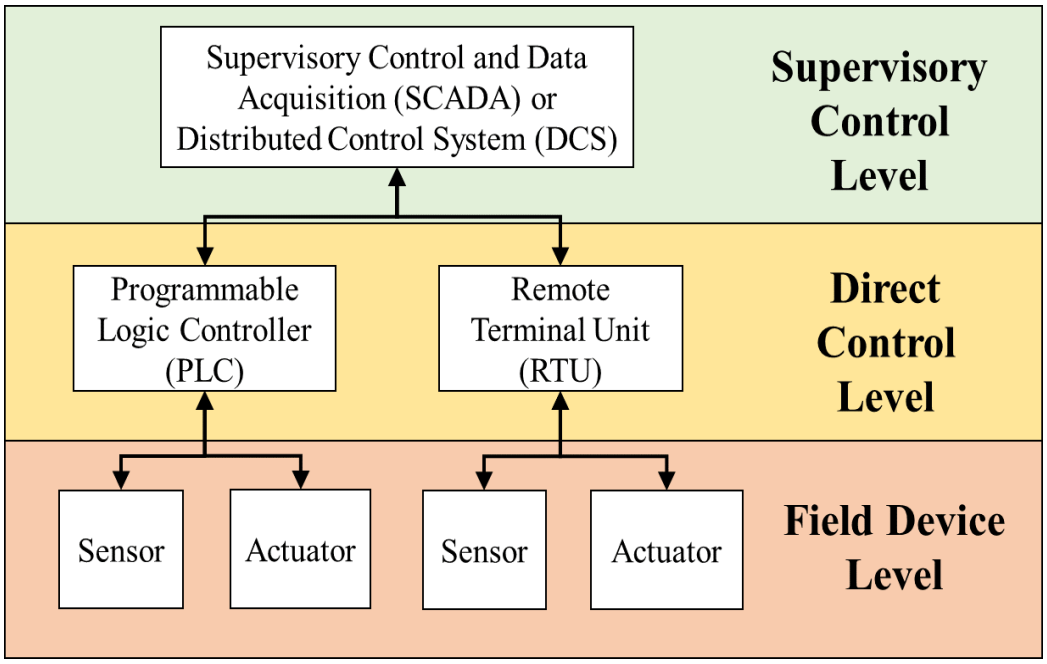


Fig. 2.2. Control hierarchy used within digital industrial control systems (El-Genk and Schriener 2022).

The semi-autonomous control systems aid the operators with controlling the plant's basic functions. They are the primary controls for startup, power operations, shutdown, and for plant transients, reducing opportunities for human error (National Research Council 1997). These I&C systems consist of a variety of different sensors and PLCs to regulate the operating state variables of the plant, such as the reactor power, primary loop system pressure, the water inventory in the pressurizer and on the shell side of the steam generators, rotation speed of the primary coolant pumps, the steam flow rate from the steam generator to the turbines, and the feedwater flow rate to the steam generator. These PLCs can be pre-programmed with operation

setpoints prior to startup or adjusted during operation by commands sent by the operators. The plant operation I&C systems typically use separate, independent sensors from those used within the safety I&C systems. This separation helps ensure that a malfunction or compromise of a component in one system does not threaten the performance of the plant's other I&C systems. These digital I&C system architectures contain a variety of different components to provide different control and orchestration duties. The next section provides a brief overview of the types of components which make up the digital I&C systems in ICS like in nuclear plants.

2.1.3. Overview of Components within Digital ICS

The OT devices in a digital ICS categorized into multiple tiered levels (Fig. 2.2). The lowest level includes what are termed field devices. These include the sensors which monitor the physical conditions within the plant and the physical control mechanisms which actuate the plant's components such as valves, pumps, and heaters. The next level up contains the direct control devices in the plant that receive the sensor's measurements and send command signals directly to the control mechanisms. These can take the form of PLCs and RTUs with digital and analog I/O modules for interfacing with the field devices below them. Above the direct control level is the supervisory control level. The devices at this level focus on coordinating and monitoring the control devices that provide the direct control functions. This supervision can involve human operators monitoring data collected by the various PLCs or a higher level autonomous or semi-autonomous computer decision making processes monitoring the control devices and sending commands to adjust their operation. ICS devices in the digital I&C systems at commercial nuclear power plants include:

- *Programmable Logic Controllers (PLCs)* are modular digital controllers first introduced in 1968 (Hung 2010). These control computers operate by scanning in data from its inputs, applying pre-programmed logic operations on the input data, and outputting a control value. The PLC performs this sequence in a periodic manner in repeated scan cycles. The inputs can take the form of analog voltage and current signals from sensor instruments which are converted to digital values using an analog to digital I/O module or digital input signals sent by another device.

  Figure 2.3 shows an example of a PLC in a CPC system developed by Westinghouse for PWRs. It has multiple slots in a common rack-mounted backplane that accommodate different functional modules. The CPC PLC in Fig. 2.1 comprises two processor modules with microprocessors to perform logic programming, communication modules for handling data transfer between units, and analog and digital signal I/O modules to receive the sensors signals of the different state variables. Digital inputs can also be used, sent via a direct serial or parallel connection or by an Ethernet connection. The output modules of the PLC communicate the determined control value in the form of generated analog or digital signals either directly to the control actuators or with another connected PLC or RTU. PLCs can be programmed using several specialized languages such as ladder logic, function block diagram, and structured text as specified within the IEC-61131-3 standard. A PLC typically controls either a single control process or a few related processes within a plant as opposed to more sophisticated centralized digital control architectures. Thus, a plant digital I&C architecture will include many different PLCs performing specialized local control functions.
- *Field Programmable Gate Array (FPGA) Devices* are a form of integrated circuit consisting of thousands to millions of logic gates which can be programed or configured. They can offer greater simplicity compared to microprocessor-based computing systems with less reliance

on complex software such as the PLCs operating systems (McNelles and Lu 2013; EPRI 2011). FPGA devices use a low-level Hardware Description Language (HDL) to program the logic control functions into the logic gate array. Multiple parallel processes within the gate array can be programed to produce more complex control capabilities. Like a PLC, a FPGA controller includes analog and digital signal I/O modules for receiving sensor measurement signals and sending output control signals.

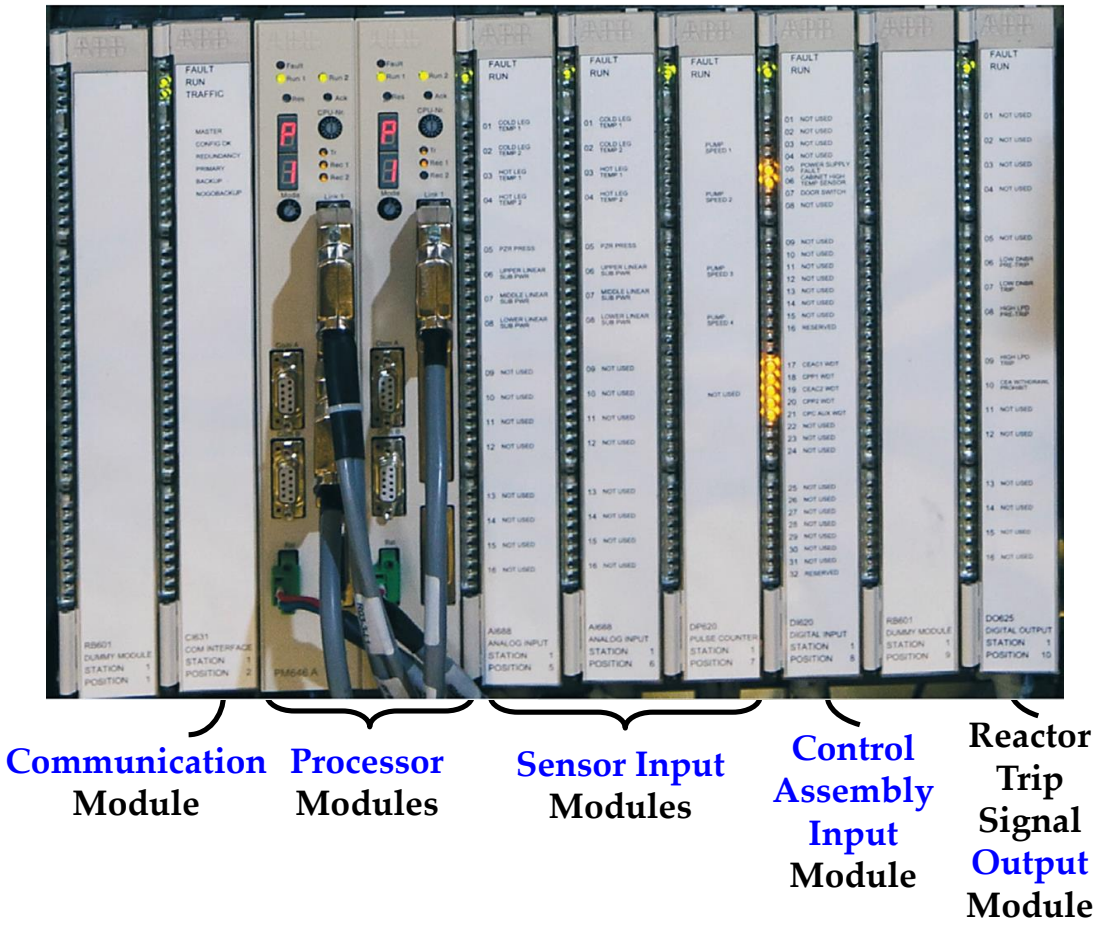


Fig. 2.3. Westinghouse Core Protection Calculator rack mounted PLC with signal input/output modules (images from US NRC).

FPGA devices are well suited for applications requiring fast response times as they often process their internal logic functions faster than comparable PLCs (She and Jiang 2011; EPRI 2011). Their lack of a typical operating system capable of running software programs as in microprocessor-based systems provides protection against certain classes of cyberattacks (McNelles and Lu 2013). In different plant I&C architectures the FPGA devices replace PLCs or work alongside them taking on the roles of RTUs or other lower-level devices. FPGA devices have been used in safety and non-safety I&C systems in nuclear plants worldwide since the late 1990's and are also being considered for next generation nuclear reactor plants and SMR designs (Lew, et al. 2019). The US NRC approved the first applications of FPGAs in a US nuclear power plant in 2009 (EPRI 2011). Another attractive feature is that FPGA devices are potentially easier to license than PLCs as they do not rely on

software in the same way PLCs do (EPRI 2011). Getting regulatory approval of the software in new or updated PLCs within safety I&C systems could expensive and time consuming.

- *Distributed Control Systems (DCSs)* are a broad category of digital ICS architectures that possesses capabilities beyond that of standardized PLCs. While a PLC may be in control of one to a few processes, DCSs can control, supervise, and orchestrate large numbers of different control processes within a plant. A DCS employs a centralized supervisory control function which monitors and sends commands to several distributed local control computers such as RTUs that directly interface with the plant's sensors and control actuators. These more sophisticated digital control systems have recently been supplementing and replacing traditional PLCs for some control functions within commercial nuclear power plants (Schindhelm and Single 2010). They can also utilize PLCs within the DCS's supervisory control functions alongside more directly controlled RTUs.
- *Supervisory Control and Data Acquisition (SCADA)* systems are another type of ICS architecture that provides means for operators to monitor and control network connected control devices like PLCs and RTUs within the plant. The SCADA system monitors the operating state of the PLCs and records and displays the data to the human operators. SCADA systems can share many functional similarities with DCSs, both serving as ways to orchestrate the operation of lower levels of more direct control devices. The primary difference between the two is in the focus on what is providing the supervisory control for the application. The emphasis of a SCADA system is providing data for human operators to aid decision making, while for a DCS the emphasis is more on autonomous computer supervisory control of lower-level systems.
- *Remote Terminal Units (RTUs)* are microprocessor-controlled devices which can connect sensors or actuators to a DCS, SCADA system, or a PLC. An RTU monitors the data from its connected devices and transmits it to the control systems higher up in the DCS or SCADA hierarchy. It can also receive and pass on control signals to connected actuation devices. Unlike a PLC, an RTU is not locally making the control logic decisions but implementing control decisions made by a connected PLC, FPGA, or DCS. Multiple RTUs connected to a single controller on a network to supply sensor data or carryout different control actions. Such arrangements used in large facilities where the RTUs collocated near their connected sensors or component actuators, while the actual control computers may be located distance away in the building. This simplifies the layout and eliminates the long cables for communicating analog signals between the sensors and both the actuators and control computers.
- *Human-Machine Interfaces (HMIs)* provide ways for human operators to access the PLCs and other computing devices within an I&C system. This provides an interface for updating the software, firmware, and control logic programming on the controllers. They check the health of the devices and change their operating status. HMIs comprise a touchscreen display or conventional display and keyboard, with a microprocessor-based computer to run the display and the programming software. Access to HMIs is restricted as a security measure to help protect the plant's control systems. For safety I&C systems in nuclear plants the HMIs used to update the PLCs' programming may be physically disconnected from the PLCs prior to startup to prevent individuals from altering their programming while the reactor is operating (Schindhelm and Single 2010).
- *Fieldbus Networks* can be used to connect the field devices and the PLCs and RTUs within a digital I&C system. They allow the different OT devices to communicate with each other

through serial or Ethernet-style connectors. A fieldbus communication setup can be simple involving two directly connected devices or sophisticated with large numbers of devices communication through network hubs and switches. The data communication through the fieldbus network commonly uses specialized ICS communication protocols such as Modbus, Profibus, DNP3, IEC-104, or preparatory vendor specific protocols like Siemens S7 and ABB Advant AF100.

The nuclear plant's PLCs connected to the sensor instruments and actuators in the I&C system using dedicated hard-wired cables or wired/wireless network connections (Fig. 2.4). Hard-wired connections link the instrument or actuator to the PLC for communicating analog signals, such as voltage and temperature, or digital signals using serial, parallel, or similar vendor proprietary connections. Direct connections are the most secure but may result in increased wiring complexity and cost. The I&C systems architectures digitally link networked sensors and actuation devices to PLCs and RTUs through the fieldbus or Ethernet network with the communications passing through routers and gateways. Such an arrangement provides flexibility in linking components and simplifies the sharing of the sensors' measured data with multiple systems, but at the cost of a potentially less secure system.

The wired connections could either be multidirectional or configured to utilize unidirectional configurations. Less critical systems in the plant can share information in multiple directions, allowing control elements to both send data to higher level supervisory and data monitoring and recording systems and receive commands over the network. For systems that require enhanced security, such as safety related I&C systems, network communications can be unidirectional. In these cases, the ethernet, serial, or parallel cables modified so that the wire leads for return data flow are physically disabled. For ethernet networks these are sometimes referred to as ethernet diodes. This can allow a secure PLC to communicate monitoring data on its operation state to the plant monitoring system while remaining isolated from receiving potentially malicious data from the overall network for enhanced security.

In recent years, some operators have incorporated secure wireless communication between instrumentation and control systems in their nuclear reactor plants (Derr and Becker 2021; Sabharwall, et al. 2021). Wireless networks can easily incorporate new sensors in large industrial facilities like nuclear power plants without a complicated and costly rewiring effort. These wireless systems can use widely used frequencies and protocols such as Wireless Local Area Network (WLAN) and Bluetooth, or more specialized portions of the wireless spectrum (Derr and Becker 2021). Internal wireless connections within a nuclear plant introduce additional cybersecurity risks beyond those of secure wired connections. A malicious actor does not need physical access to the secure hardware or communication lines in a wireless system, but merely being in range with a compatible wireless device inside the facility may be sufficient. Wireless communications thus need to be shielded to prevent them from propagating beyond the intended operation areas or receiving signals from outside. Real-time monitoring can also be used to scan for unauthorized wireless communication activities that are discovered and eliminated (Derr and Becker 2021).

2.2. Cybersecurity in Commercial Nuclear Power Plants

Nuclear power plants are highly secure facilities, with layers of physical protection and independent safety systems. The introduction of digital components and even all-digital I&C systems in nuclear power plants, however, has made cybersecurity protection an essential part of their security design and planning. The digital computing components in the plant's I&C systems

may possess vulnerabilities in their software, firmware, and hardware that could enable a hostile actor to maliciously alter their behavior. Hostile cyberattacks could aim to disrupt the operation of the plant and potentially attempt to cause damage to it. This could involve attempting to cause an unplanned reactor trip to shut down the plant, which could cause disruption to the electrical transmission grid and economic losses due to the plant being offline. A cyberattack campaign could also target multiple systems within the plant to try to bring it to an unsafe operating condition, while trying to send false monitoring data to the human operators to hide the attack in progress.

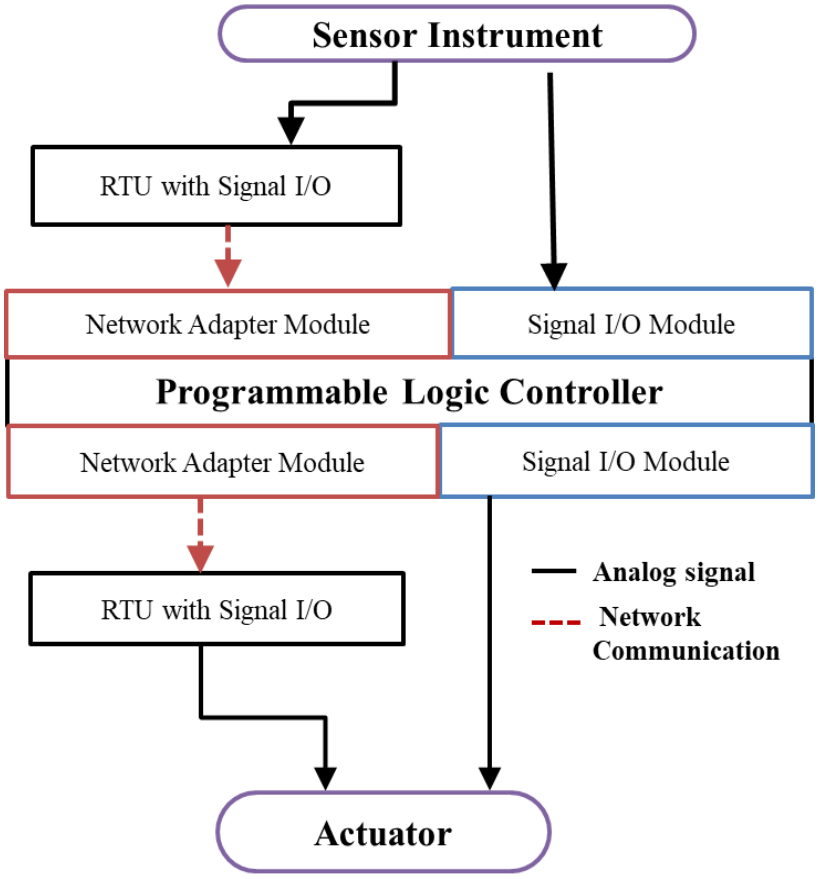


Fig. 2.4. Digital I&C systems with sensor measurements and actuator signals communicated directly to PLC or indirectly through plant internal network (El-Genk and Schriener 2022).

The US NRC requires all licensed nuclear plants to submit a cybersecurity plan as part of its physical protection program for review and approval (Nuclear Energy Institute 2010). Each plant is required to protect against cyberattacks on its systems serving regulatory safety related functions, security functions, and emergency preparedness functions, including offsite communication capabilities. Digital I&C systems within a commercial nuclear plant rely on a combination of physical and digital isolation, administrative controls, and computer security features for cybersecurity protection. The cybersecurity procedures and controls for the plant should both protect the digital I&C systems and networks against hostile cyberattacks without adversely affecting the reliability and robustness of the plant's monitoring and control functions (Garcia 2021). Cybersecurity measures developed in coordination with upgrades and changes to

the plant's digital I&C systems to ensure effectiveness without disrupting operation. Cybersecurity equipment and security procedures need evaluated to ensure the added benefits are worth the cost and the added system complexity. This is important as introducing new hardware and software may introduce additional failure modes which need investigated and accounted for (Garcia 2021).

2.2.1. Cybersecurity Threats Faced by Nuclear Power Plants

While the majority of historical cyberattacks have targeted IT infrastructure, OT and ICS systems like those used in nuclear plant I&C systems have become the target of a growing number of cyberattack campaigns in recent years (Hemsley and Fisher 2018). Cybersecurity threats can originate either from external sources outside the plant or internally emerging from within the plant boundary (Nuclear Energy Institute 2010). External cyber-threats can take the form of remote attacks on online components connected to outside computer networks. The digital I&C systems in nuclear plants are normally isolated from outside networks and they frequently utilize proprietary ICS communication protocols which can be more difficult to reverse engineer. This makes digital I&C systems in nuclear plants difficult or impossible to directly hack into from outside the plant.

The cyber-compromises which have occurred to date at commercial nuclear power plants have involved the enterprise IT business networks at the plants and not the networks for the plant control systems. This occurred in 2018 at the Wolf Creek Nuclear Power Plant where computers in the plant business network compromised by an email fishing scheme targeting the plant's employees (Perlroth 2019). However, increased standardization of I&C hardware models in the nuclear industry and the growing sophistications of state-level cyberattack campaigns make a hostile actor targeting nuclear plant control systems an increasing possibility in the future (Sabharwall, et al. 2021).

Supply chain attacks represent an alternative means for hostile actors to introduce malware from outside the plant. These attacks target the manufactures of digital I&C system components to create flaws or introduce malware within the hardware, firmware, or software at the factory. If undetected, the compromised devices or software installed within a plant and provide opportunities for the malicious programming to initiate cyberattacks at some future point. Supply chain attacks present a cybersecurity planning challenge as the manufacturing facilities are outside an operator's direct control. The global nature of modern manufacturing can make overseeing the parts which go into a plant's I&C system even more of a challenge. Securing against supply chain attacks requires extensive qualification and testing of hardware components before they accepted and installed to ensure they are free from introduced malicious programs.

Internal cybersecurity threats come from the accidental or intentional introduction of malicious programs by workers inside the plant (Nuclear Energy Institute 2010). During refueling outages and maintenance periods plant personal and outside contractors may legitimately access and update the programming on the PLCs and RTUs in the safety and plant operation I&C systems. There exists a potential for malware to exist on media such as laptops or flash drives used to update the ICS computers in the I&C system. This may be intentional as in an insider attack or unintentional where the malicious program transferred to the update media unbeknown to the employees who are performing the updates. When connected to the digital I&C hardware the malware could transfer across and compromise the system. This was the method used by the malware in the Stuxnet cyberattack campaign against the PLCs within Iran's uranium enrichment facilities (Karnouskos 2011). The malware crossed the air gap isolating the digital I&C system by hiding on flash memory update media. Institutional plant cybersecurity

testing is required to examine and scan all media brought into the plant to protect against such attacks.

Cyberattack campaigns on ICS have commonly targeted vulnerabilities in specific hardware and software models within the digital control system (Nuclear Energy Institute 2010). Malicious programs can have scanning functions which monitor the state of the computer they reside on and scan the attached network to identify potential target equipment. Sophisticated malware can then move from system to system to attempt to reach its intended target. Once there it can deploy its attack payload program and attempt to adversely affect the I&C system. While FPGA devices may not run malicious software, their inputs and outputs can still be targets of cyberattacks.

Cyberattacks on a reactor I&C system targeting the inputs and outputs may attempt to send or write false input data to the PLCs as in a FDIA. This could attempt to induce a PLC to act contrary to that indicated by the plant's current operating conditions. It could also send false operating data based on trends observed monitoring the plant's operation to try to hide an attempt to manipulate it towards a potentially damaging condition. Man-in-the-Middle (MitM) attacks intercept data at a network location in between the sender and receiver. This allows the malware to inspect the data to gather information on the plant's normal operation. Then when programed to act the attack could try to block the normal traffic and send false data or malicious commands in its place. Other types of cyberattacks target overwriting numerical values stored in the PLC's memory to change pre-programed setpoints and control values to alter its control functions. These can also exploit weaknesses in computers memory design and programs, for example allowing a program to alter stored values in the memory without accessing their locations.

2.2.2. Cybersecurity Controls and Mitigation Strategies in Nuclear Power Plants

A plant's cybersecurity protection should follow the same defense-in-depth protective strategy as employed in the design of its physical safety systems. Protecting against cyberattacks requires a combination of physical and digital security controls, protective hardware and software features, and secure network designs. These controls and systems aim to detect, delay, respond to, and recover from cyberattacks on its digital I&C systems (Nuclear Energy Institute 2010).

Commercial nuclear plants employ a combination of physical and digital boundaries to protect their digital I&C assets (Nuclear Energy Institute 2010). The level of security for a given device can be tailored to its importance to the safety of the nuclear power plant. The architecture of the I&C system establishes logical and physical boundaries to control the transfer of data between components of the I&C system. Networked components can be separated by digital security boundaries devices, such as firewalls and Ethernet diodes. Communication across these network boundaries can be monitored and restricted. The regulatory safety I&C systems are isolated to a greater degree within commercial nuclear plants than those for plant monitoring and operation control. Regulatory standards require that these systems have only limited contact with other I&C systems within the plant (Nuclear Energy Institute 2010). This accomplished using unidirectional Ethernet diodes at the boundaries of the safety I&C system to allow it to communicate its status to other plant I&C systems for monitoring purposes while preventing data or commands to be sent to the PLCs within the safety system. In addition to digital boundaries, physical barriers and controls are essential elements in the plant cybersecurity protection. Access to critical hardware restricted to authorized personnel with access privileges (Nuclear Energy Institute 2010).

The I&C computing hardware are secured in locked equipment cabinets to restrict physical access to the devices. This is supplemented by secure password protected account management

controls that further restrict unauthorized access to the computers. Access within the plant should be limited to the smallest number of users necessary to ensure the security of the digital I&C components (Nuclear Energy Institute 2010). Limiting the number of personnel that have access needs to be balanced against the security risk of any one individual having too much access to the plant's systems as a protection against insider threats. Security controls can enforce separation of the duties for personnel responsible for maintaining secure I&C system components to limit situations where a single individual has access to perform all service roles for a device (Nuclear Energy Institute 2010).

The hardware and software on the PLCs and other digital control devices can also be configured to reduce their potential cyber-vulnerabilities (Nuclear Energy Institute 2010). Modern digital I&C systems are much more powerful and versatile than the early generations of PLCs (Hung 2010). They can support a wider range of communication connections and software programming options. From a cybersecurity perspective unneeded ports and software capabilities represent additional attack surfaces for a malicious actor. The PLCs in the plant's I&C system configured to disable unneeded communication cable ports through software or by physically disconnecting them. Data ports such as USB can be disabled or removed on a device to prevent removable flash drives from being inserted. Similarly, software features can be removed or disabled if they are not required for the operation and maintenance of the device. Unnecessary device drivers and communication protocols can be uninstalled to restrict the PLC's ability to interact with unexpected devices covertly installed onto the I&C network. Software compilers for supporting programming languages not used by the PLC can also be removed to prevent malware from utilizing them in constructing cyberattacks.

A rigorous qualification process is needed to determine that the I&C systems' architecture and its components are suitable for use inside the nuclear power plant. Qualification requirements are plant and system specific, with each plant responsible for developing and enforcing its own standards to meet regulatory safety requirements (Garcia 2021). This is an essential cybersecurity component for defending against supply chain attacks. Components need to be evaluated on a dedicated testing platform prior to installation to validate their functional reliability and to try to detect potential vulnerabilities. These testing platforms can also be used to evaluate the effects of software updates prior to deploying them within the plant.

While security boundaries and cybersecurity precautions are intended to eliminate or limit the potential cyber-vulnerabilities in the plant's I&C system, it is still important to monitor the plant's digital systems for signs of cyber-compromise. Cyberattack detection is an active field of research in the nuclear industry (Garcia 2021). The plant's monitoring system typically records operating data for the components within the digital I&C system to monitor their health and track unexpected events which occur during operation. This system can help alert operators to certain classes of attacks by informing the operators of a PLC or RTU behaving in an unexpected manner. Security programs can monitor the network communications within the I&C systems' fieldbus and Ethernet networks for unexpected or unauthorized traffic. Unusual communication patterns could be a sign of malware or a software effort to compromise communications or scan the network for vulnerabilities. Similar network security monitoring is required for wireless systems within the plant. Secured wireless connection within the plant involves regular scans by security personnel to detect any unauthorized devices which may be planted by an insider.

Real-time malware protection programs can be deployed at security boundaries in the I&C network architecture, as well as on workstations, servers, and mobile computing devices on the plant's non-essential computing systems (Nuclear Energy Institute 2010). These programs act

like commercial antivirus and anti-malware software to detect and eradicate malware attempting to communicate data between systems or exploit vulnerabilities in the devices. These malware protection mechanisms can use signature definitions like IT antivirus programs to help detect known malicious programs. They can also proactively scan devices on the network to try to detect abnormal behavior which could indicate a compromise. If malware detected the infected programs must be prompted quarantined and removed. Protection software products from multiple vendors can be employed as part of a diverse defense-in-depth strategy to guard against limitations in any one vendors' software (Nuclear Energy Institute 2010).

2.3. Summary

Digital I&C systems have brought considerable economic and safety benefits to modern commercial nuclear power plants. They have contributed to a reduction in unanticipated reactor trips and supported power uprates that have enabled the reactors in the commercial nuclear fleet to generate more electricity to customers than ever before. Digital I&C systems have also greatly expanded the ability of operators to monitor and record plant data to assist in maintenance planning. Nuclear power plants use digital I&C systems to perform safety and protection functions as well as for non-safety operation control and monitoring. The safety I&C systems provide autonomous reactor trip protection and ESF actuation functions to shut down the plant or actuate its safety equipment when human operators fail to act first. The operational control I&C system assists the operators managing the plant during normal operation by regulating key operating parameters. These I&C systems comprise a series of different monitoring sensors and control actuators, PLCs, RTUs, FPGAs, and supervisory control systems. These systems are resilient against malfunctions and avoid common cause failures by design.

Although digital I&C systems have been a great benefit to the nuclear industry, they have introduced new cybersecurity concerns within commercial power plants. The US NRC requires all licensed nuclear plants submit cybersecurity protection plans on the controls and protective systems used to secure the critical digital assents in the I&C systems. These plans aim to defend against a variety of different cyber-threats originating from both outside and inside the plant. These threats could attempt to introduce malware into the plants digital control computers by the actions of employees within the plant or at their manufacturing facilities. Plants defend against these threats with extensive testing and evaluation procedures for introducing and updating computers in their digital I&C systems. This is in addition to a combination of administrative controls and protective systems employed within the plant.

Developing an effective cybersecurity plan for a nuclear power plant requires evaluating the effects of potential cyberattacks on the digital I&C assets and the resulting consequences on the operation of the plant. Cybersecurity evaluation and testing can help identify the level of protection needed for different components to meet the plant's safety requirements. Nuclear plant cybersecurity modeling and testing platforms are being developed to support evaluating the cybersecurity posture of existing nuclear power plants, investigating the effects of I&C upgrades, and assist in the development of next generation I&C systems for advanced reactors. The next section reviews the types of nuclear cybersecurity simulation and testing platforms currently being investigated and details the LOBO NCS platform.

3. CYBERSECURITY INVESTIGATION CAPABILITIES AND THE LOBO NUCLEAR CYBERSECURITY PLATFORM

With increased concerns over cybersecurity there is a need to develop simulation and testing platforms to investigate the effects of simulated cyberattacks on and cyber-vulnerabilities of the digital I&C system architectures in nuclear power plants. Nuclear cybersecurity simulation platforms are being developed to help investigate the cybersecurity for the current nuclear fleet. In addition, these platforms could help develop next generation I&C systems for advanced, SMRs and microreactors plants and used for education and professional training (Sabharwall, et al. 2021; El-Genk et al. 2020, 2021). The nuclear cybersecurity simulation platforms pursue different forms to investigate various aspects of cybersecurity protection and threats. Some nuclear cybersecurity simulation and analysis platforms utilize probabilistic methods to examine potential consequences of a successful cyber-compromise on nuclear power plants operation and safety. Wheeler, et al. (2017) have developed a methodology for predicting potential effects of a cyber-intrusion on the nuclear plant operation while the attack progresses through the digital I&C system. They used computer models to simulate the I&C system and investigate the progression of a cyberattack as it moves from one component to another within the I&C network. Their methodology employed the Analysis of Dynamic Accident Progression Trees (ADAPT) Dynamic Event Tree (DET) software to generate potential consequence scenarios which can be investigated using the MELCOR severe accident analysis code (Gauntt, et al. 2000).

Shin, et al. (2015) have developed a cybersecurity risk model for nuclear plant I&C systems. The model couples an activity-quality analysis and an architecture analysis to examine the system's vulnerabilities. The activity-quality analysis investigates different scenarios for levels of compliance to security regulations by the plant's personnel. The architecture analysis evaluates potential vulnerabilities due to the actions of the plant personnel and evaluates the effectiveness of mitigation strategies.

Chae, et al. (2022) recently developed a methodology to identify potential paths of a cyberattack on a nuclear power plant's digital I&C system architecture. It determines the paths to reach the target component in the shortest time with maximum impact on the plant operation and safety. The methodology uses a page rank algorithm to evaluate different paths within a network nodal model of the nuclear plant I&C system. Determining the optimal path from the perspective of the attacker can help identify the areas where cyber defenses should be concentrated or changed to reduce the cyber-vulnerabilities of the I&C system.

The above references focused on developing methods for identifying and tracking potential cyberattacks. A second category of cybersecurity simulation and modeling platforms directly investigate the effects of simulated cyberattacks on the plant's operation and safety. These platforms link simulated, emulated, and physical hardware components of the digital I&C system to real-time physics-based simulation models of the fully integrated nuclear power plant and various plant components. They provide broader and more comprehensive capabilities to investigate the consequences of how cyberattacks interact with the controllers in the I&C system. Such platforms previously developed for cybersecurity investigations of ICSs for critical energy infrastructure. An example is the DOE SCEPTRE framework (Camacho-Lopez 2016) originally developed for cybersecurity investigations of electrical transmission grid architectures. The nuclear plant cybersecurity platforms under development used to investigate the dynamic interaction between the developed simulation model of the plant and the digital controllers both

during normal steady state operation and various operation transients. Some platforms link networked I&C devices using real ICS communication protocols to closely represent the actual systems.

In these cybersecurity platforms, the digital I&C devices can be simulated, emulated, or integrated as HIL. Each of these options have their own advantages and disadvantages. Simulated components use simple computer programming to replicate the basic function of the device, such as a PLC or a switch. These simulated models are typically lightweight and fast running and can easily be incorporated into the physics-based plant model. While these models may replicate the nominal programed responses of the simulated devices, they do not include their software, firmware, or hardware. This makes simulated I&C component models of limited use in cybersecurity investigations because many types of cyberattacks cannot interact with them as they would with a real system. Functional simulation models can still be of used to represent I&C devices not directly involved in a simulated cybersecurity event.

Emulated devices use computer programs called Virtual Machines (VMs) to represent the firmware and/or hardware. The VM can run actual computer operating system images and software to provide increased fidelity compared to simulated models of I&C devices. Depending on the VM, the firmware and hardware can also be fully emulated. More commonly, however, the VM serves as a translation layer between the operating system running within it and the operating system and firmware of the host computer running the VM. The emulated digital I&C devices in a cybersecurity investigation platform can be configured to run the same operating system and software as a real system for a realistic evaluation of the effects of different cyberattacks. The VM emulation approach, however, comes at the expense of increased complexity and resource requirements compared to functional simulation models.

The HIL approach provides the highest possible degree of fidelity in a digital cybersecurity testing platform, where the actual physical PLC, RTU, switch, or other devices in the I&C systems are coupled to an integrated plant model. While this is a practical option for investigating the effects of postulated cyberattacks, commercial-grade ICS devices are costly and difficult to scale up to fully represent complex I&C architectures. In addition, setting up and configuring large numbers of devices for laboratory testing can be time consuming. By contrast, orchestration programs can start up and connect large numbers of VMs based on developed images of emulated I&C devices on affordable computational server hardware. Furthermore, investigators can just as easily tear down and reset the experiment without needing to flash and restore the programming on each physical device targeted by the simulated cyberattack scenario.

Several research projects have been initiated to meet this need for high fidelity digital platforms for investigating the cybersecurity of nuclear plant I&C systems and the effect of potential cyberattacks on the operation of the plant. These include (a) the Asherah Nuclear Plant Simulator (ANS) developed in conjunction with the IAEA, and (b) the LOBO Nuclear CyberSecurity (LOBO NCS) platform developed at the University of New Mexico in collaboration with Sandia National Laboratories. While the ANS and LOBO NCS platform are both developed to provide means to link emulated and physical hardware PLCs to transient models of a representative nuclear power plant, these two cybersecurity testing platforms provide different capabilities to researchers. Section 3.1 summarizes the capabilities of the IAEA developed ANS, with Section 3.2 presenting the LOBO NCS platform developed as part of the present DOE NEUP NICSim project.

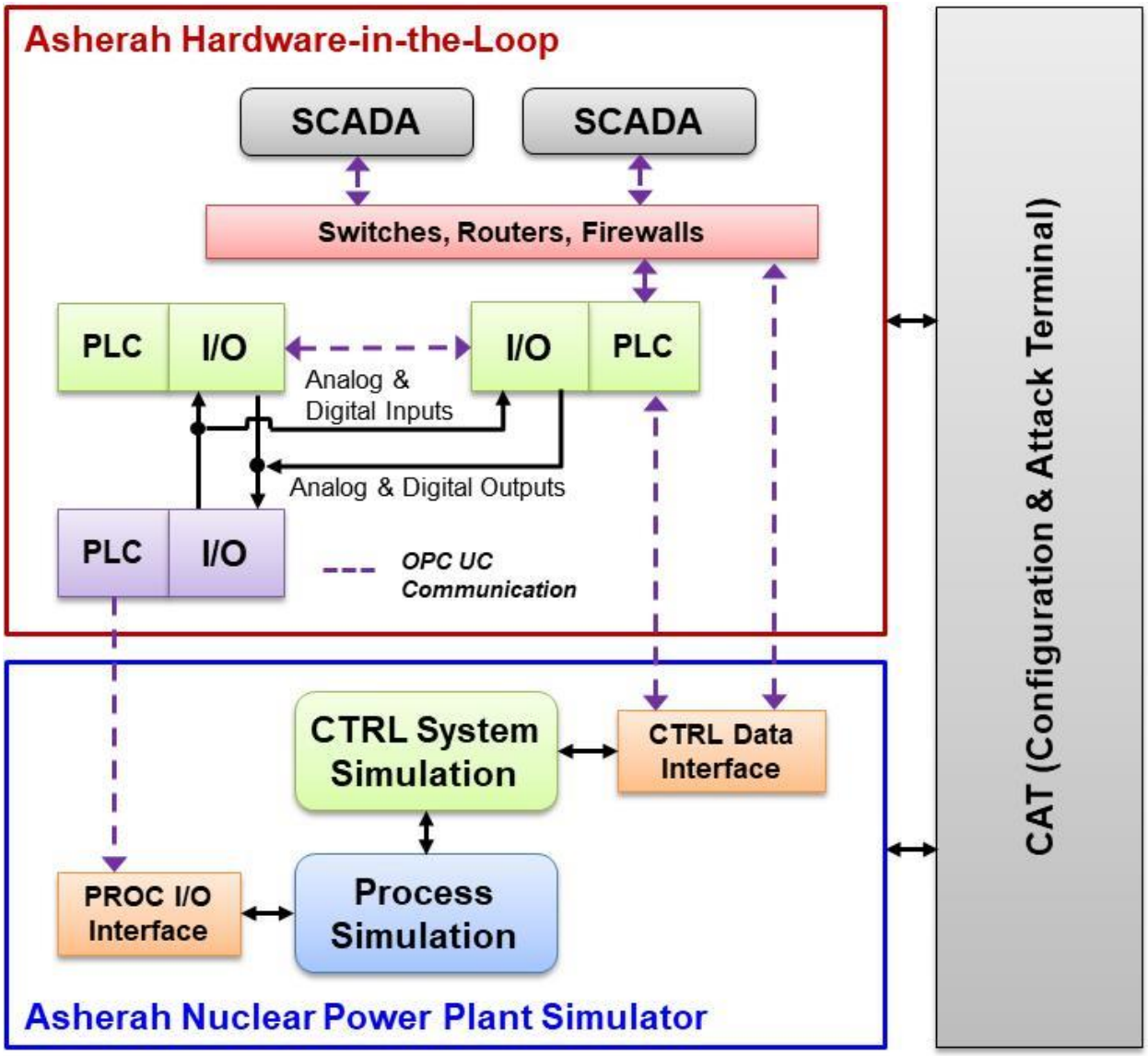


Fig. 3.1. A block diagram of the ANS platform for nuclear plant cybersecurity investigations (adapted from Busquim e Silva, et al. 2021).

3.1. IAEA Asherah Nuclear Power Plant Simulator (ANS)

The ANS has been developed as part of a 2016 IAEA Coordinated Research Project entitled Enhancing Computer Security Incident Response Analysis at Nuclear Facilities (Busquim e Silva, et al. 2021). This multi-disciplinary project involved participants from 17 research institutions in 13 countries. The goal was to develop capabilities to assess the impact of cybersecurity events on the digital I&C systems in nuclear power plants. The ANS simulator is designed to evaluate the consequences of malicious cyberattacks on the operation of the plant and I&C system and to help identify systems and equipment that require additional protection against cyberattacks. The simulator couples a dynamic model of a representative PWR plant with simulated, emulated, or physical hardware I&C components integrated as HIL. It is used to evaluate the impacts of cyberattacks targeting specific digital devices in the plants' I&C system.

The simulated PWR plant and I&C system are intentionally designed to be generic and not represent any specific real designs. (Busquim e Silva, et al. 2021).

This section describes the elements of the ANS and I&C cybersecurity testing platform (Figure 3.1), and the developed physics-based dynamic model of a representative PWR plant using the Matlab Simulink platform. Also described are: (a) the communication interfaces for among the simulated and hardware PLCs in a representative I&C system, and (b) the Configuration and Attack Terminal (CAT) used to set up and run the cybersecurity experiments. In addition, a series of HIL implementations by separate groups using the IAEA ANS platform are reviewed.

3.1.1. ANS Dynamic Model of a Pressurized Water Reactor Plant

The ANS includes a dynamic model of a 2,772 MW_{th} two-loop PWR plant based in part on the Babcock and Wilcox design of the Three Mile Island Unit 1 (Fig. 3.2) (Busquim e Silva, et al. 2021). The model developed using the versatile Matlab Simulink platform (The MathWorks 2020). The plant model comprises simple physics-based sub models of the systems and equipment within the plant's primary, secondary, and tertiary loops. The water and steam thermodynamic properties in the ANS calculated using the 1997 formulation specified by the International Association for the Properties of Water and Steam (IAPWS-IF97) (International Association for the Properties of Water and Steam 2007). The dynamic plant model designed to simulate both operational transients as well as a limited set of abnormal transients such as a turbine trip (Busquim e Silva, et al. 2021). The ANS plant model does not include physics to simulate accidents such as a Loss of Coolant Accident (LOCA). As shown in Fig. 3.2, the ANS primary loop model comprises those of the reactor with coupled point kinetics and thermal hydraulics, a 3-region pressurizer, the reactor coolant pumps, the U-tube steam generator, and the primary loop volume control tank. The ANS plant model also includes a model of the Chemical and Volume Control System (CVCS) to regulate the water inventory in the primary loop and the dissolved boron concentration for reactivity control.

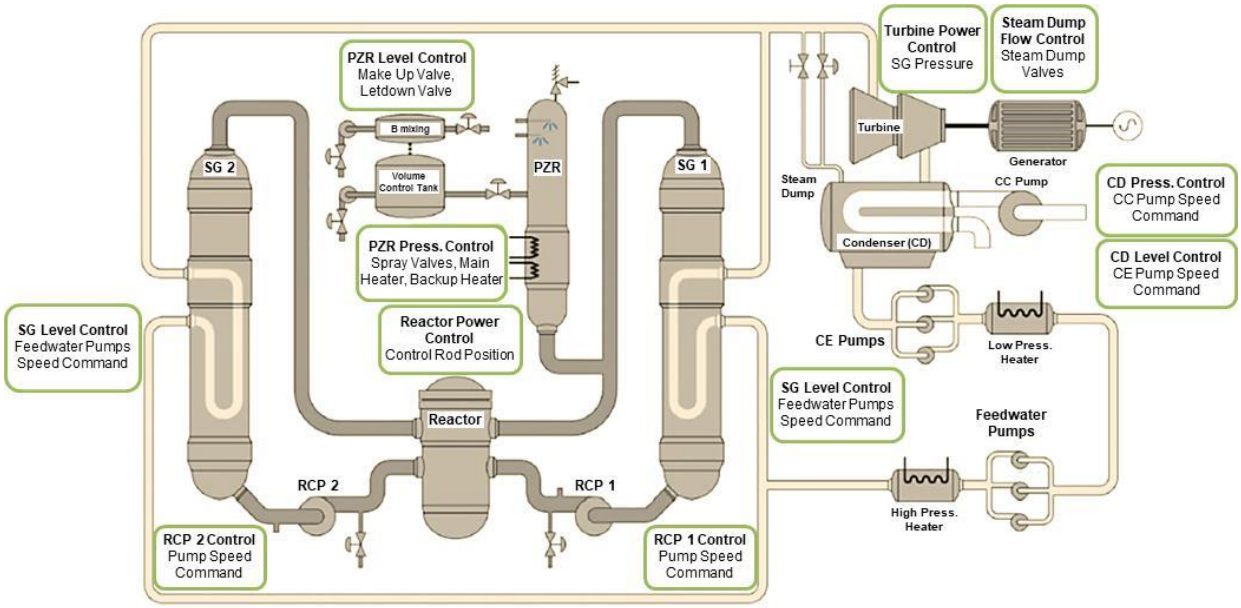


Fig. 3.2. A block diagram of a representative PWR plant and I&C system in ANS (Busquim e Silva, et al. 2021).

The reactor model uses a 6-group point kinetics model coupled to a transient thermal-hydraulics model (Busquim e Silva, et al. 2021). The parameters in the models are calibrated against calculated results calculated using a tool which couples the RELAP and PARCS codes (Busquim e Silva, et al. 2021). The implemented point kinetics assumes piecewise constant reactivity with an implicit solver to reduce the computational burden of the stiff differential equations. The reactor point kinetics model accounts for the temperature reactivity feedbacks for the fuel and coolant, represented as linear functions of temperature with constant coefficients. An additional term incorporated in the reactor kinetics model to account for the reactivity effect of the soluble boron concentration in the coolant.

The core thermal hydraulics represented using a simplified lumped approach with discretized axial nodes of the coolant and the fuel rods. The pressurizer model in the ANS comprises an upper vapor region and a lower liquid region, divided into two subregions. A saturated water subregion that contains the immersed proportional and backup heaters, and a subregion of either saturated or subcooled water that communicates with the water in the hot legs of the primary coolant loops. This subregion accommodates surge-in and out of subcooled water from and to one of the hot legs in the primary loop. The pressurizer model accounts for evaporation and condensation at the liquid-vapor interface, condensation of vapor along the wall of the upper vapor region and on the subcooled spray droplets injected at the top of the pressurizer into the vapor region. The rates of evaporation and condensation assumed to be proportional to the mass and steam quality in the vapor and that of water in liquid regions.

The ANS steam generator model uses a lumped approach to describe the flow of the water from the primary loop through the U-tubes of the steam generator to calculate the rate of heat transfer in terms of the mean water temperature. The secondary side of the steam generator is represented as two regions: a lower region with subcooled or saturated water and an upper vapor region with saturated steam. The model accounts for the evaporation from the lower water region but not for condensation in the vapor region. The water level in the steam generator is allowed to vary but the U-tube bundle is assumed always covered with water as during nominal operation (Busquim e Silva, et al. 2021).

The reactor coolant pumps model utilizes normalized characteristic curves for a reference pump design. The homologous curves normalized to the rated values for the pump head, flow rate, and rotation speed. It includes additional time constants in the governing equations to account for the pump dynamics during operation transients. The model of the feedwater pump in the secondary loop is a scaled down version of that the reactor coolant pump and uses the same normalized characteristic curves. The secondary loop model includes those of the steam turbine, electrical generator, condenser, feedwater system, steam reheaters, and the condensate extraction system (Fig. 3.2). The models for the turbine and the generator utilize generic non-proprietary performance curves with added equations for simulating dynamic responses. The turbine model includes correction factors to account for the effects of the outlet back pressure on the turbine operation. The generator model uses a simple performance curve with no additional dynamic terms. The two-region condenser model in ANS structured like that used for the secondary side of the steam generator. It assumes saturated steam and water in vapor region and in lower region, respectively. It is thermally coupled to tertiary heat rejection loop with simplified models of the condensate pumps and cooling tower.

3.1.2. Representative PWR Plant I&C System

The developed control systems within the ANS are based on well-known standard strategies used in commercial PWR power plants (Busquim e Silva, et al. 2021). They include control logic

programs for the Reactor Power, the Pressurizer's Pressure and Water Level, and Steam Generator's Feedwater, the Reactor Coolant Pumps, the Turbine Power, the Condenser's water Level and Pressure Control, and the Steam Dump within the primary and secondary loops in a PWR plant (Fig. 3.2). The simulated PLCs use simplified controller designs with Proportional-Integral-Differential (PID) and Proportional-Integral (PI) controllers to regulate their functions (Oka and Susuki 2013). The simulated I&C system architecture includes the safety functions in the I&C system for the reactor trip protection and the ESF. These functions are assumed isolated and protected within the plant and thus, I&C systems are not subjected to cyberattacks in ANS.

3.1.3. ANS Communication Interface and Configuration and Attack Terminal

The ANS links the physics-based model of a representative PWR plant to the simulated or HIL devices in the I&C systems for cybersecurity investigations (Busquim e Silva, et al. 2021). The CAT (Fig. 3.1) provides a graphical interface for the users to set up different cyberattack scenarios on the I&C network architecture. The ANS uses the Open Platform Communications-Universal Architecture (OPC-UA) as the preferred protocol for all types of communication. It also supports Modbus for hardware that does not support OPC-UA (Busquim e Silva, et al. 2021).

The ANS platform divides a representative PWR plant I&C system into four levels (Fig. 3.1). The first includes the simulated measurement sensors and actuators incorporated into the Simulink model. The second includes simulation models of field control devices such as RTUs or FPGAs. The third level includes the simulated PLCs for direct control in the I&C system as well as models for TCP/IP communication devices such as simulated routers and switches. The fourth level includes the configured supervisory control devices which can be integrated into the ANS as HIL.

The plant's Matlab Simulink model has two communication interface functions for connecting with external I&C components integrated as HIL (Busquim e Silva, et al. 2021). These include: (a) two communication channels for transferring data into or out of the Simulink model, and (b) a process I/O Interface for direct communication with the PLCs performing control functions in the I&C system. The interface sends the calculated state variables representing the simulated sensor signals to the PLCs and receives the returning controller actuator signals.

The Control Data Interface handles network communications with supervisory control level I&C system components, such as SCADA systems, to simulated PLCs in the I&C systems. This allows the SCADA or other supervisory control system to monitor parameters of simulated PLCs within ANS Simulink model. The data communication capabilities also include an HMI which functions as the main control room for the user running the simulation.

3.1.4. ANS Nuclear Cybersecurity Investigations

The ANS platform has been evaluated with a Siemens S7-1200 commercial PLC connected as HIL to the developed Simulink model of a representative PWR plant. The Siemens S7-1200 PLC has been evaluated in separate experiments representing the Steam Generator Feedwater PLC and the Pressurizer Pressure PLC. The PLC is connected to the OPC-UA network using a HIL interface device (Busquim e Silva, et al. 2021). The ANS platform was used to investigate the effects of simulated FDIAs attempting to alter the operation of the Siemens PLC by sending false values of the state variables to the PLC input registers. Results showed that the simulated FDIA successfully altered the operation of the PLCs and reduced the feedwater injection rate causing the water level in the steam generator to decrease.

Several research groups have adapted the ANS platform to develop custom cybersecurity testbeds with different HIL integration capabilities. Zhang, Payne, and Childress (2021) developed the Asherah Pi Nuclear Simulation (APNS) testbed that links the Asherah's PWR plant Simulink model with open-source PLCs based on the Raspberry Pi minicomputer with the OpenPLC runtime The OPC-UA communication channels in ANS communicates the calculated state variables by the Simulink model to the PLCs through an intermediate interface module and receives returning control signals

The interface module in the ANS platform uses a Prosys OPC-UA commercial ICS data server designed to help exchange data with various sources using the OPC-UA protocol. The Prosys server is used as an intermediary because the OpenPLC runtime does not support the OPC-UA communication protocol. The Softing dataFEED commercial software is used to oversee the communications between the OPC server and the Raspberry Pi PLC (Zhang, Payne, Childress 2021). The software uses the OPC-UA protocol to communicate with the Prosys OPC server and the Modbus protocol to communicate with OpenPLC. Several cyberattack scenarios of MitM, Denial of Service (DOS), and FDIAs conducted using this testing platform.

Recently, Hahn, et al. (2021) successfully coupled the ANS platform with the DOE SCEPTRE cybersecurity framework (Camacho-Lopez 2016). The SCEPTRE platform allows users to launch and coordinate large virtual I&C system architectures with a multitude of PLCs, switches, SCADA servers, and other I&C devices. Its capabilities support integrating large I&C architectures with as many as thousands of devices more easily than in the base ANS platform. Hahn, et al. (2021) used Siemens PLCSIM virtual PLC software to emulate Siemens S7-1500 PLCs within SCEPTRE.

The emulated PLCs run Siemens S7 control programs in a soft PLC environment on separate Windows 10 VMs. These VMs are connected using a virtual local area network with simulated switches and fieldbus devices that communicated using the Modbus TCP protocol. The Asherah Simulink model is modified to allow a Sandia developed shared memory inter-process communication interface to link it to the SCEPTRE platform. Hahn, et al. (2021) plan to scale up the system to perform cybersecurity investigations on large I&C architectures for nuclear power plants.

3.2. LOBO Nuclear CyberSecurity (LOBO NCS) Platform

The LOBO NCS platform developed at UNM-ISNPS in collaboration with Sandia National Laboratories (SNL) as part of the DOE NEUP NICSim project (El-Genk, et al. 2021; El-Genk and Schriener 2022) helps investigate cyber-vulnerabilities of nuclear plant digital I&C systems, supports academic education and research, and provides professional training. This modular platform links Matlab Simulink (The MathWorks 2020) physics-based models of a representative PWR plant with emulated and physical hardware PLCs in the digital I&C system. The LOBO NCS platform was designed to have greater modularity and flexibility than the IAEA's ANS. The initial development effort for LOBO NCS focused on linking the Simulink physics based PWR plant model and PLCs. However, the flexible of the modular platform allows it extended to other nuclear power plant types and I&C system architectures.

The modular LOBO NCS architecture allows users to swap out Simulink models, controllers, cybersecurity event generators, and graphical interfaces without changing the core programs within the LOBO NCS platform. By providing a platform for investigating the interaction between the transient plant behavior and its digital control systems, the LOBO NCS platform applied to a wide range of control system and cybersecurity research areas, including the

development of digital I&C system architectures for advanced nuclear reactors, SMRs, and microreactors. It can support the development of secure remote adaptive control using digital twins of SMRs and microreactors and of space reactor power systems for planetary surface power and space exploration missions (Metzger, El-Genk, Parlos 1991).

This section describes the architecture, various components, and capabilities of the LOBO NCS platform for a representative PWR plant and emulated PLCs within its digital I&C system (Fig. 3.3). The developed Matlab Simulink physics-based dynamic models, referred to as Providers, are linked to the emulated PLCs in the I&C system using fast and reliable data transfer interface and broker programs that form the core of the LOBO NCS platform (Hahn, Schriener, El-Genk 2020). These programs transfer the 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 platform uses the Modbus TCP ICS protocol as the default for the communications between the data broker and the PLCs (Fig. 3.3). The modular platform, however, can be adapted to support other ICS protocols such as DNP3. The same common core data transfer interface and broker programs in the LOBO NCS platform can be applied unchanged to different research and training applications. The user only needs to change the simulation data provider and the emulated and/or physical hardware PLCs needed for the application.

The developed model of a representative PWR plant in the LOBO NCS incorporates several physics-based models of various components with built-in inputs for their control systems (El-Genk, et al. 2021). They include models of the primary loop, the reactor coolant pump, the steam generator, the pressurizer, and coupled reactor point-kinetics and thermal-hydraulics. The integrated plant model is used to simulate various operation transients such as startup, shutdown, and changes in the steam load demand. Like ANS, the representative PWR plant model in the LOBO NCS platform simulates operational transients and abnormal operation scenarios initiated by cybersecurity events. It does not simulate design base or severe accidents. The PWR plant model in LOBO NCS, unlike that in ANS, can be configured to represent different plant designs.

The PWR plant Simulink model calculates the state variables including the position of control elements in the reactor core, the reactor thermal power, fuel and coolant temperatures in the reactor core, the water temperatures and flow rate in the primary loops, the pressure and water level in the pressurizer, the exit quality and the water level in the steam generator, the feedwater flow to the steam generator, and the shaft rotation speed of the primary coolant pumps.

In each timestep during a simulated operation transient, the Simulink models calculates the values of the state variables and communicates them to the data transfer interface (Fig. 3.3). The developed fast and reliable date transfer interface relays the information to the data broker and communication program (Hahn, Schriener, El-Genk 2020). The broker program serves as an intermediary between the data transfer interface and the emulated or real PLCs in the I&C system. It maintains a central record of all calculated state variables and of the returned control signals by the PLCs (Fig. 3.3).

The communications between the Simulink models and both the PLCs and the data broker are conducted using the Modbus TCP ICS protocol on an isolated network. The data transfer interface and the broker programs run on the same main server node as the Simulink models and the Graphical User Interface (GUI). The emulated PLCs run within separate VMs located on multi-processor server nodes connected to the isolated ethernet network. 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 developed and

incorporated into the LOBO NCS platform to initiate simulated cybersecurity events on the PLCs in the I&C systems (Fig. 3.3). This framework consists of several modules for cybersecurity simulation and capturing and inspecting network traffic for further analysis. These modules run on Linux PCs and communicate directly to the PLCs on the network. The data capture module records and inspects Modbus packets sent through the network.

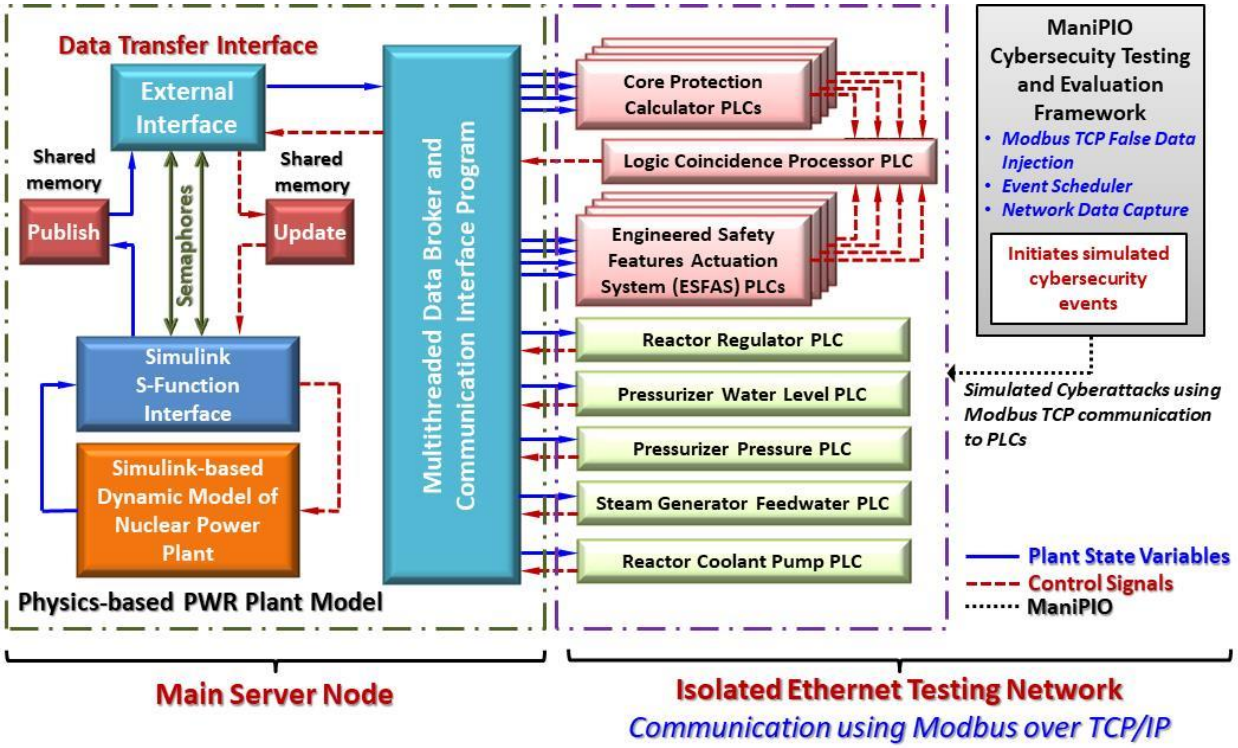


Fig. 3.3. A block diagrams of the LOBO NCS platform for a representative PWR plant and the emulated PLCs in the I&C systems (El-Genk, et al. 2021).

The isolated network handles traffic between the different computers and the real and emulated PLCs. The managed switch forwards all network traffic to the port connected to the computer running the capture module of the data packets on the network. The following sections detail the various components in the LOBO NCS platform and present the results of characterizing the OpenPLC runtime and the Modbus TCP communications to and from OpenPLC using the developed data transfer interface (Hahn, Schriener, El-Genk 2020).

3.2.1. Data Transfer Interface

The LOBO NCS platform employs an efficient and fast-running data transfer interface for linking the Matlab Simulink model of a PWR power plant to the broker program (Fig. 3.3) (El-Genk, et al. 2021). A specialized Simulink S-function written in the C programming language is developed to communicate the simulation state variables to an external interface program and the control values returned by the PLCs. The S-function allows for custom user code to be executed at distinct phases within the Simulink's process. This code enables the POSIX Inter-Process Communication (IPC) shared memory data transfer with the data transfer interface (Hahn, Schriener, El-Genk 2020).

The S-function writes the calculated state variables at the end of every major timestep to a

shared memory location named 'Publish' (Fig. 3.3). It then reads in the received values of the control signals from the I&C system's emulated PLCs from a second shared memory location named 'Update.' The control signal values in the model are kept constant throughout the minor timestep iterations to allow the Simulink solver to reach convergence. This ensures that the S-function communicates only properly converged values of the state variables to the PLCs in the I&C system.

The external interface program manages the opposing side of the shared memory communication with the S-function (Fig. 3.3). It reads the state variable values from the 'Publish' location and passes them to the data broker program. It then receives the PLCs' control signal values from the broker and writes them to the 'Update' shared memory location. The IPC semaphores coordinate access to the 'Publish' and 'Update' shared memory locations to ensure communications efficiency and reliability. The semaphores prevent communication interruptions, known as race conditions, which occur when both sides of the data transfer interface try to simultaneously access the same shared memory location. The external interface program also uses the semaphores to control the timing of the Simulink model to run in synch with real time. This synchronization is essential for capturing the correct transient behavior of PLCs which use time-dependent controller functions like PID controllers. The developed data transfer interface in the LOBO NCS platform is fast, highly dependable, and modular. The communication S-function can be added to any Matlab Simulink model to interface with the LOBO NCS platform. Thus, users can easily integrate the Simulink models they developed for their plant designs into LOBO NCS with minimal modifications. The modular nature of LOBO NCS also supports non-Simulink based simulation models or physical hardware with proper communicates interface with POSIX IPC libraries to the shared memory and semaphores.

3.2.2. Data Broker and Communication Interface

The multithreaded data broker and communication program exchanges information between the data transfer interface and the emulated or hardware PLCs in the I&C systems. The data broker program serves as the central repository of the received state variables values from the Simulink models and the returning control signals from the PLCs (Fig. 3.3). In each iteration cycle the data broker reads the most recent state variable values returned from the data interface to update its master database. The broker communicates the state variable values stored in its repository to each PLC and records recently returned values of the PLCs control signals. It then sends back these signals to the data transfer interface that communicate them to the Simulink models. The communication between the data broker and interface programs uses internal POSIX data queues.

The communication interface creates separate processing threads which connect to the individual PLCs in the test network. These threads pass information to and from the data broker using additional independent data queues; one for the bundle of state variables to each PLC and another for the generated control signals. These communication threads run independently and allow asynchronous updates from the different PLCs, which may have different internal scan times for updating their outputs. These threads communicate directly with the PLCs using an implemented ICS communication protocol like Modbus TCP, which is the default option in the LOBO NCS platform.

3.2.3. Graphical User Interface

The user-friendly GUI allows users to start up the different programs in the LOBO NCS platform and provides a real-time data display for the running simulations. The data broker

program communicates the current record of the state variables and PLCs' control signals to the GUI. The GUI then displays the simulation results in real time both numerically and graphically on a large screen connected remotely to the main server node running the data broker program (Fig. 3.3). The developed GUI allows users to create two-dimensional plots of the calculated state variables by the Simulink models, which continuously update during the simulation. The GUI also enables the user to function as an operator during the simulations and send manual command signals through the data broker to the Simulink models of the PWR plant model and/or the PLCs.

3.2.4. ManiPIO Framework

The ManiPIO framework within the LOBO NCS platform (Fig. 3.4) allows users to design and execute simulated ICS manipulations of the PLCs within the testing network and capture and record the network traffic (El-Genk, et al. 2021). It safely manipulates the signals to the PLCs' memory registers using established ICS network communication protocols. This allows the LOBO NCS platform to realistically simulate cyberattacks on the PLCs and record the impact on the operation of a representative PWR plant. The ManiPIO framework and the network capture and recording programs developed only for research purposes and built using open-source tools and common Python libraries and do not contain any malicious software.

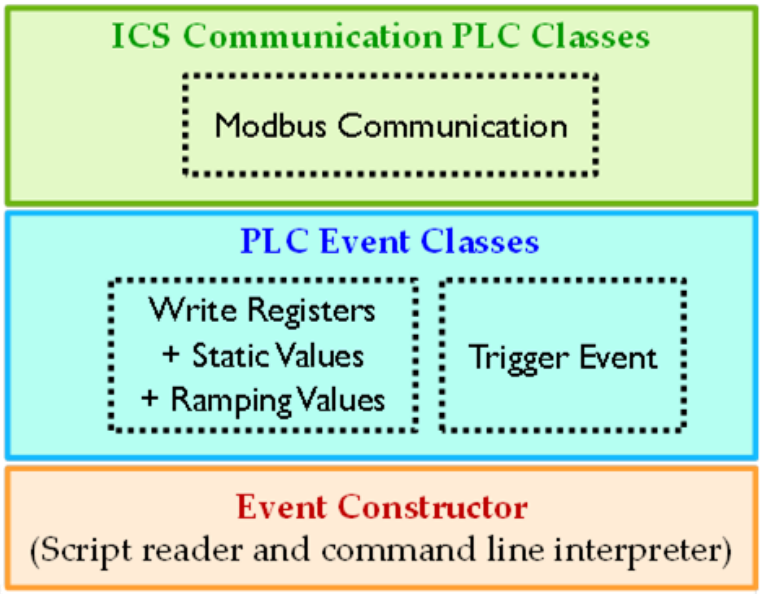


Fig. 3.4. A schematic of the structure of ManiPIO framework in LOBO NCS (El-Genk, et al. 2021).

The highly modular ManiPIO framework is adaptable and customizable to keep up with the evolving sophistication of cyberattacks on ICS. Features and new capabilities added as different Python program classes could be expanded and updated as needed. The main section of the program is the Event Constructor (EC) that reads the input script, coordinates the sequence of events, and builds the simulated manipulations of the ICS (Fig. 3.4). The user input script informs the EC of the communication protocols to use, the target memory registers on the PLC, 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 ManiPIO program includes classes of ICS communication protocols for interacting with the PLCs specified in the input

script. These communication classes are based on converted open-source Python ICS protocol libraries. The Modbus TCP protocol is the standard communication function in the ManiPIO program, but other communication protocols can be added as needed.

The ManiPIO program can script three classes of events, namely, (a) writing static values, (b) writing ramping values, and (c) setting up executing triggers (Fig. 3.4). In a single event, the program writes the specified value to the PLC memory registers either once or using persistent repeated rewriting. The persistent overwrite option in the ManiPIO program allows the user to either specify the time between overwrite attempts or for sending the overwrite attempts as fast as the program allows. In a ramp event, the written values to the memory registers change linearly over time. Trigger events monitor process variables stored in the PLC's memory registers and act when monitored values satisfy preprogrammed setpoints. Users can schedule time delays of all event classes to create a predesigned sequence of events to launch on the PLCs. An Event Constructor (EC) coordinates the sequence of events specified in the user generated input scripts and builds the simulated manipulations of the ICS (Fig. 3.4). The user supplied script informs the constructor of the communication protocols to use, the target memory registers on the PLC, and the types of events, and when to start them. The constructor then executes the events in individual threads and monitors them for completion.

The network traffic capture and record utility in the ManiPIO performs deep inspection of the Modbus TCP packets on the isolated testing network. This utility is adapted from the Scapy Python library and is separate from the main ManiPIO program so that it can run on any computer on the network. It monitors the ethernet and internal loopback networks for Modbus TCP packets, and captures, decodes, and records to a log file. The network traffic capture utility runs locally on the server or PLCs or on a VM connected to a network port. The utility on the VM records the forwarded switch traffic. This includes all the communications on the different servers and hardware PLCs and RTUs in the testing network. The network traffic capture utility could be configured on a local host server to capture internal loopback traffic between the LOBO NCS and any VMs running locally on the same server. The log provides useful data on the effects of the simulated cyber events on the response of the control system. The data is investigated for the recorded effects of the simulated cyber events on the functionality and the fidelity of the nuclear plant model.

In summary, the ManiPIO framework (Fig. 3.4) could be used to simulate cyberattacks targeting the PLCs in I&C systems of a representative PWR plant within the LOBO NCS platform. Users can script sequences of cybersecurity events using Modbus TCP communication protocol to write to the input and/or the output of one or more PLCs. These events could be initiated by monitoring the PLCs process variables or using timed sequences. A combination of triggered and timed events could be employed to investigate the effects of sophisticated cyberattacks on 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.

3.2.5. A Representative PWR Plant Model

The LOBO NCS platform includes a fast-running, physics-based dynamic model of a PWR plant to provide direct feedback to the emulated components of the digital I&C system (El-Genk, et al. 2020, 2021). The nuclear plant Simulink Model provides a modular environment with simplified physics-based models of different plant components. Fig. 3.5 presents a line diagram of the physics-based model of the representative two-loop PWR plant model in LOBO NCS with two steam generators and four cold legs. The plant model comprises physics-based models of: (a) the reactor, with coupled thermal-hydraulics and robust point-kinetics, (b) the primary loop,

which solves the coupled overall mass, momentum, and energy balance, (c) the steam generator, (d) the pressurizer, (e) reactor coolant pump, and (f) a simplified secondary loop. The PWR plant model incorporates the dimensions, masses, and materials for the plant components, the reactor kinetics parameters, the reactivity control and temperature reactivity feedback parameters, the reactor coolant pump characteristic curves, and the secondary loop thermodynamic parameters. The PWR plant component models and design input parameters can be changed to simulate assorted designs. The constituent equations in the Simulink models are solved simultaneously using discrete fixed timestep solver.

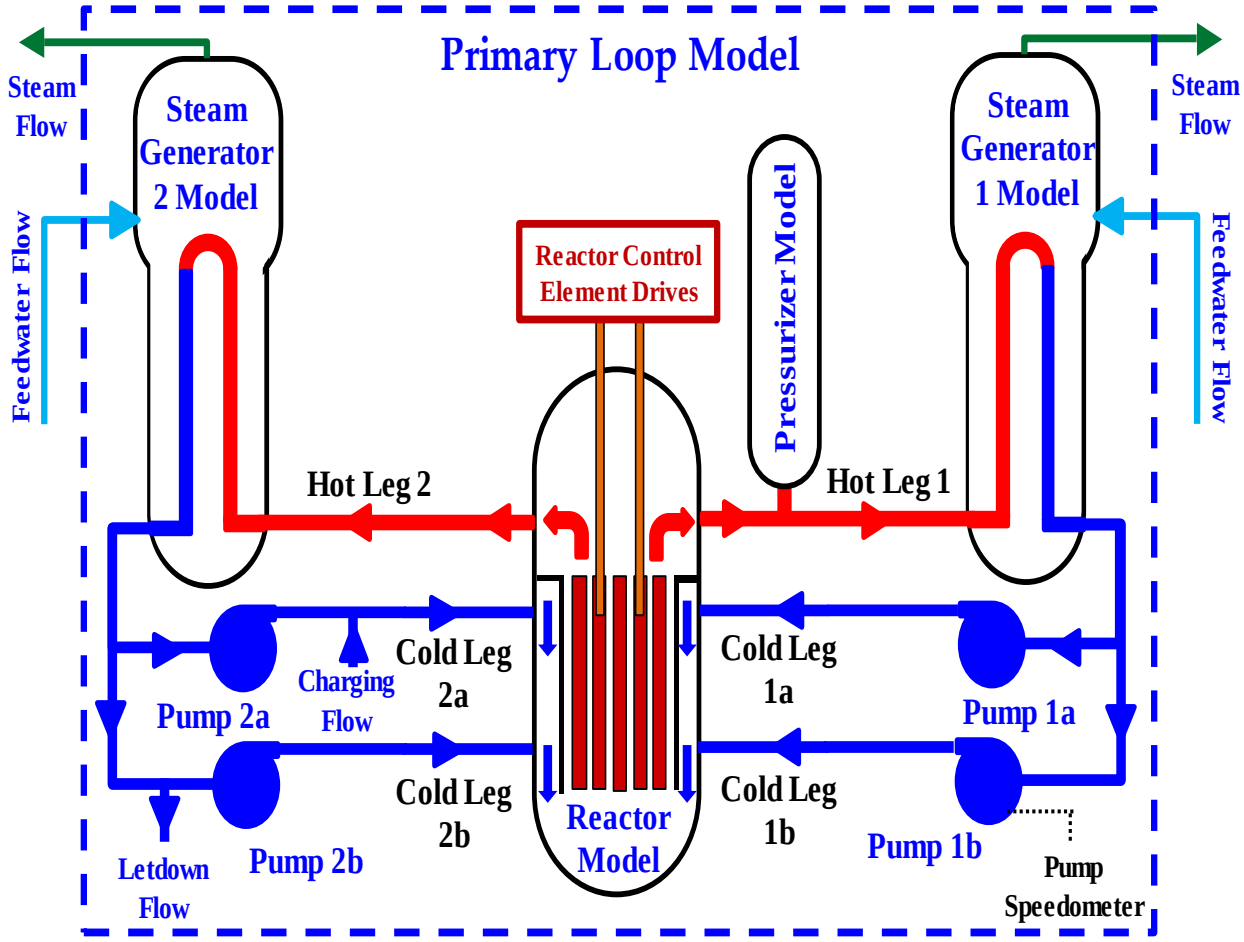
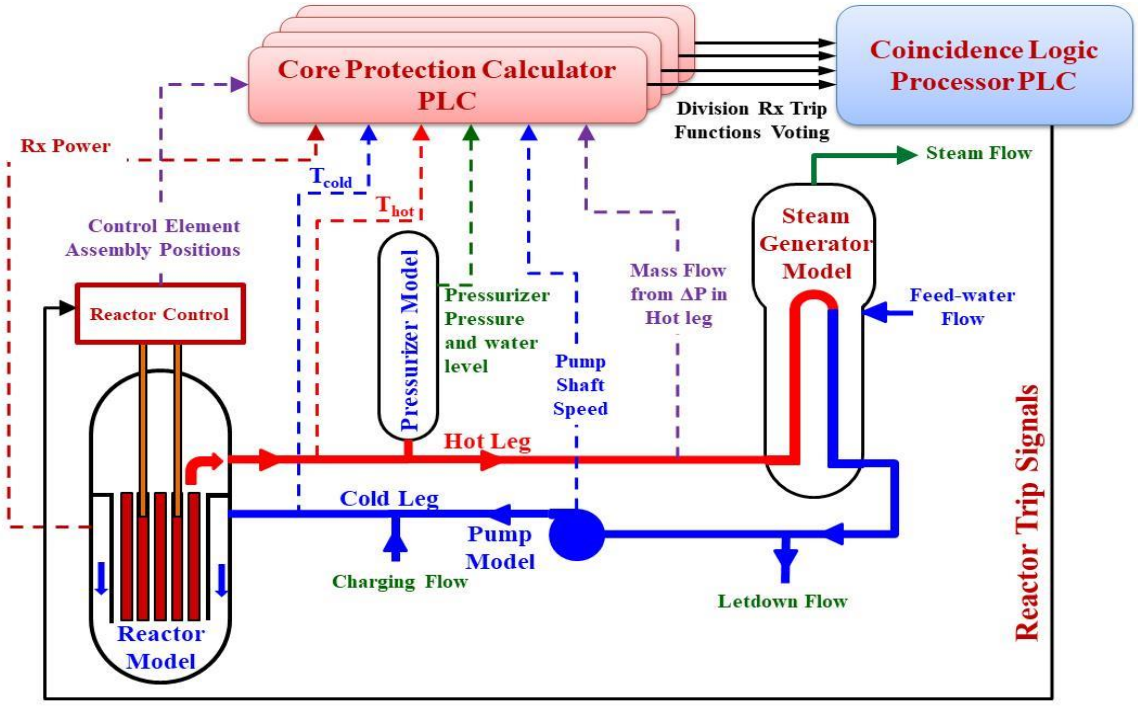
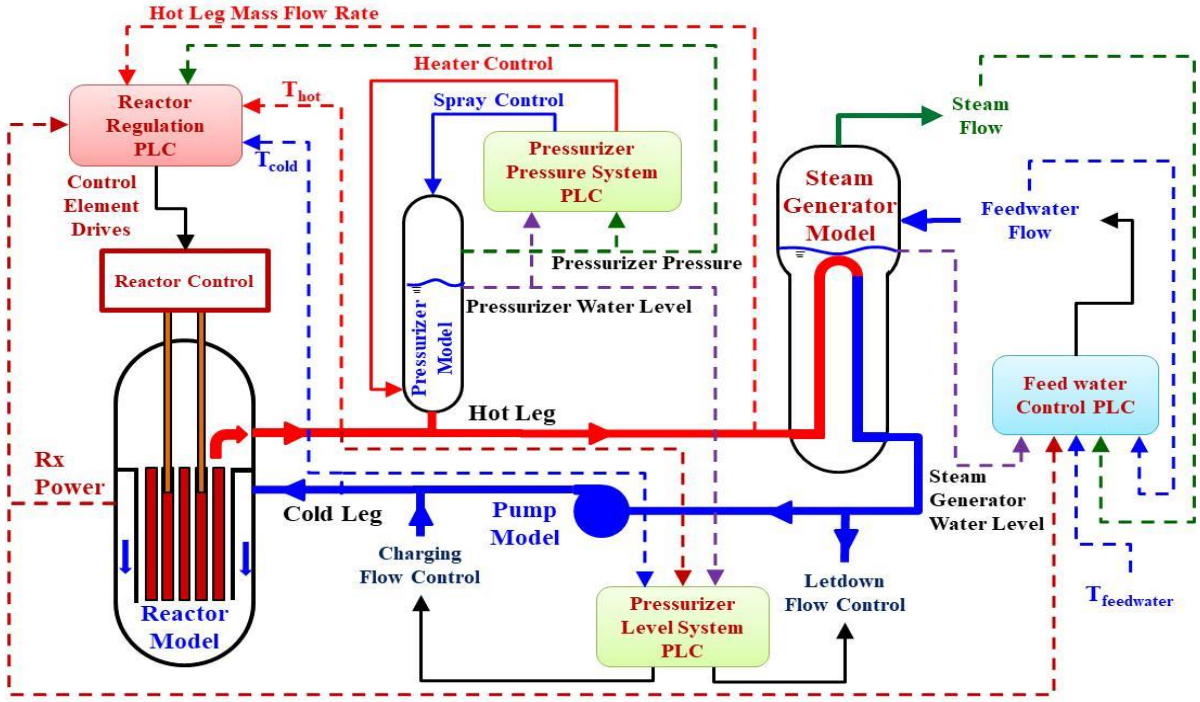


Fig. 3.5. Developed physics-based components model of a representative PWR plant in LOBO NCS platform (El-Genk et al. 2020).



(a) Reactor trip safety I&C system



(b) Plant operation I&C system

Fig. 3.6. A layout of the digital I&C systems of a representative PWR plant in the LOBO NCS Platform: (a) Reactor safety I&C system, (b) Plant operation I&C system (El-Genk, et al., 2021).

The primary loop model includes physics-based models of the ducts of the hot and cold legs, the reactor core, the pressurizer, the steam generators, and the primary coolant pumps. The calculated temperatures and system pressure determine the thermophysical properties of the coolant, fuel, and structural materials using the IAPWS-IF97 standard formulations (International Association for the Properties of Water and Steam 2007). The primary loop model accounts for the changes in the coolant inventory due to changes in temperature and pressure and the inflow and outflow through the charging and letdown valves in the cold leg (Fig. 3.5). The coolant inventory in the primary loops determines the rates of the coolant surge-in and out to and from the pressurizer. The overall momentum balance in the primary loop model determines the mass flow rate through each of the hot and cold legs and the total mass flow rate through the reactor core. The coolant flow rates in the primary loops are calculated from equating the total pressure losses to the pressure head generated by the primary coolant pumps (Fig. 3.5).

The reactor model in LOBO NCS couples point kinetics and thermal hydraulics. The point-kinetics model calculates the changes in the reactor fission power in response to an external insertion of reactivity due to the movement of control elements and temperature reactivity feedback effects for the fuel, cladding, and the moderator. The reactivity feedback parameters for the fuel and cladding are expressed as polynomial functions of temperature. The reactivity feedback parameters for the water moderator are specified as functions of temperature and the concentration of the soluble boron. The solution of the six-point kinetics equations uses a robust and efficient exponential matrix technique approximated using the 7th order Padé(3,3) function (El-Genk and Tournier 2016). This approximation is efficient, accurate and stable, and is independent of the timestep sizes used in the calculations. Thus, the timestep size for the coupled PWR plant model is not restricted by the reactor kinetics model, even when simulating fast power transients.

The reactor core lumped thermal-hydraulics model is for an average fuel rod and includes the in-vessel coolant and core structure such as the reactor vessel and core internals. The model discretizes the core into axial nodes to calculate axial temperature distributions in the fuel, cladding and coolant. For a given inlet coolant temperature and flow rate, this model calculates the average temperatures of the fuel, cladding and coolant, and the core pressure losses as a function of the reactor thermal power during nominal and transient operations. The axial reactor power distribution is used to determine the fission power values in the different axial nodes. The reactor core thermal-hydraulics model is coupled to the primary loop thermal-hydraulic mode to calculate the total pressure losses, the coolant flow rate and inlet temperature to the core.

The three-region, non-equilibrium pressurizer model in LOBO NCS calculates the transient changes in the system pressure and the water level in the pressurizer (El-Genk, Altamimi, Schriener 2021). It tracks the mass and energy exchanges between the top saturated vapor region, the middle-saturated water region, and a lower subcooled water region. The lower water region represents the surge-in of water from the hot leg into the pressurizer. The boundary between the middle and lower water regions moves up and down as subcooled water surges in and out of the pressurizer. This model accounts for the evaporation due to the thermal power dissipated by the submerged electrical heaters and the condensation onto the spray water droplets in the saturated vapor region. The pressurizer model also accounts for condensation due to heat losses through the pressurizer wall. The pressurizer model receives signals from the pressurizer PLCs to control the submerged electric heaters and the spray nozzle in the top region.

The Steam Generator (SG) model in the LOBO NCS platform calculates the rate of heat removal from the primary loop coolant into the U-tubes to the secondary water flow on the shell

side. It also calculates the steam exit quality and flow rate to the turbines for electricity generation (El-Genk, et al. 2021), the total pressure losses in the primary loop portion of the SG, and the inlet and exit enthalpies of the primary coolant flow through the U-tubes. The steam/water mixture on the shell side of the U-tubes is modeled using a separate flow approach. It determines the non-boiling and boiling heights and the steam exit quality to the turbine in the secondary loop in response to changes in steam demand. The water level in the annular downcomer is calculated from equating the weight of the water column in the downcomer to that of the water and steam column within the central section of the SG. The SG model accounts for thermal inertia in the energy balance equations for the primary but not in the secondary side. It incorporates the user specified thermodynamic pressure and temperature state points to calculate the thermophysical properties in the secondary loop.

The primary coolant pump model in the LOBO NCS calculates the performance characteristics of the pumps. It is partially based on the pump model in the RELAP5 system code (Nuclear Safety Analysis Division 2001). It uses homologous pump curves to calculate the pressure head and the hydraulic torque as functions of the operating conditions. The pump pressure head determines the corresponding coolant flow rate in the overall momentum balance equation for the primary loop. The calculated pump hydrodynamic and shaft torque are used to calculate the thermal energy dissipation to the primary coolant flow. Users can input different pump rated parameters and homologous head and torque curves to simulate the performance of a specific pump design by the user.

3.2.6. Emulated PLCs of I&C System in a Representative PWR

The LOBO NCS platform incorporates emulated PLCs in the Protection and Safety Monitoring System (PMS) and in the Operation I&C system for a representative PWR plant (Figs. 3.6a and 3.6b) (El-Genk et al. 2020). The PMS' PLCs provide the essential regulatory safety functions of autonomously tripping the reactor or actuating the ESF when any of the plant's state variables exceed preprogramed setpoints (Fig. 3.6a). The PLCs in the Operation I&C system provide semi-autonomous regulation of the operation variables within preprogramed setpoints (Fig. 3.6b). They receive the values of the state variables calculated by the Simulink physics-based models of the fully integrated PWR plant and the various plant components. A VM running the open-source OpenPLC software manages the control logic program for each of the emulated PLCs (Alves and Morris 2018). The OpenPLC software runs IEC 61131-3 standard PLC programming languages and communicates using the Modbus TCP ICS protocol.

3.2.6.1. Protection and Safety Monitoring I&C System in a PWR Plant

The LOBO NCS platform includes emulated PLCs for the PMS. The system's architecture comprises four divisions, each with a separate set of PLCs. These PLCs receive a bundle of the state variables that represent the measurements from the PMS's dedicated sensors in the plant. The PLCs in each of the four divisions vote independently on whether to trip the reactor or actuate one or more of the plant's safety systems. The PMS architecture has three types of PLCs in each of the four safety divisions: the CPC, the ESFAS, and the logic coincidence processor.

3.2.6.1.1. The Core Protection Calculator PLC

Each of the four independent CPC PLCs, one for each of the four safety divisions, receives a bundle of state variables representing the sensor measurements in an actual plant (Figs. 3.6, 3.7). The calculated reactor power represents the value determined by the ex-core fission ion

chambers located inside channels within the biological shield surrounding the reactor vessel (Fig. 3.7). The fission ion chambers are calibrated for their response to the neutron flux is proportional to the reactor thermal power. Additional ex-core neutron detectors may be used to assist the plant operator during a reactor startup, and when greater sensitivity is needed for accurate measurements when operating at low power (Westinghouse Electric Company 2011; Palo Verde Nuclear Generating Station 2017). The positions of the Control Element Assemblies (CEAs) in the reactor core for each of the CEA groups are sent to the CPC. They are measurements by the Rod Position Indication system, which comprises a series of either Reed switches or electromagnetic coils around the shafts of the CEAs. These sensors determine the vertical positions of the control assemblies in the reactor core.

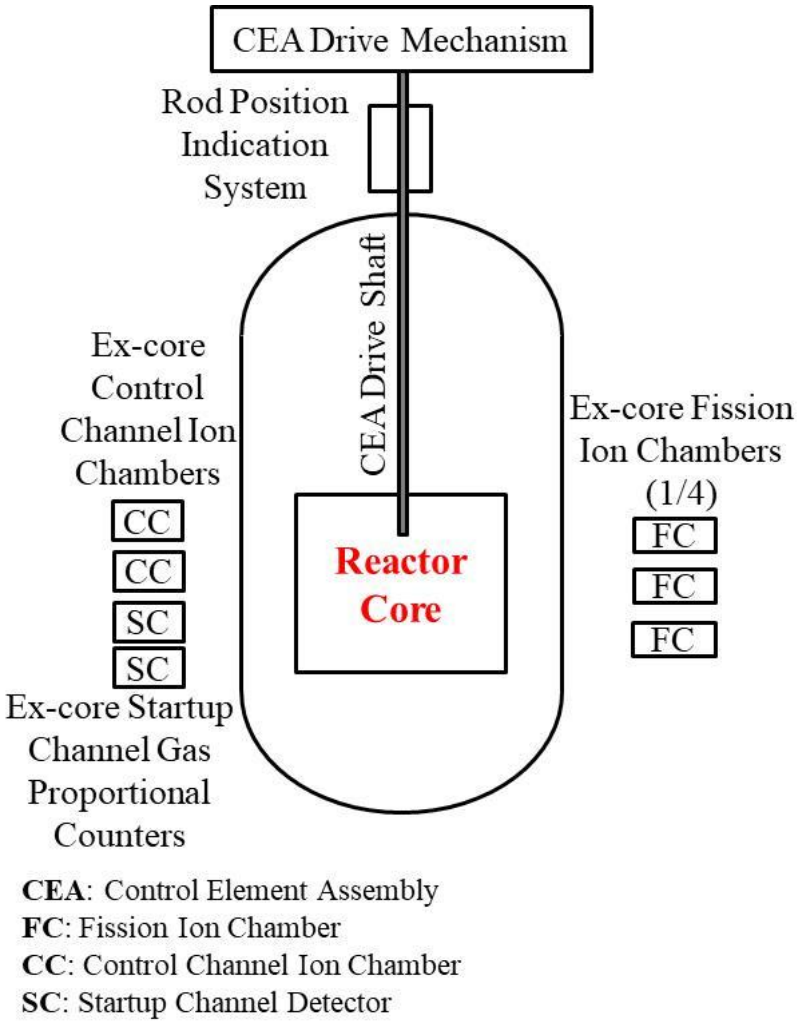
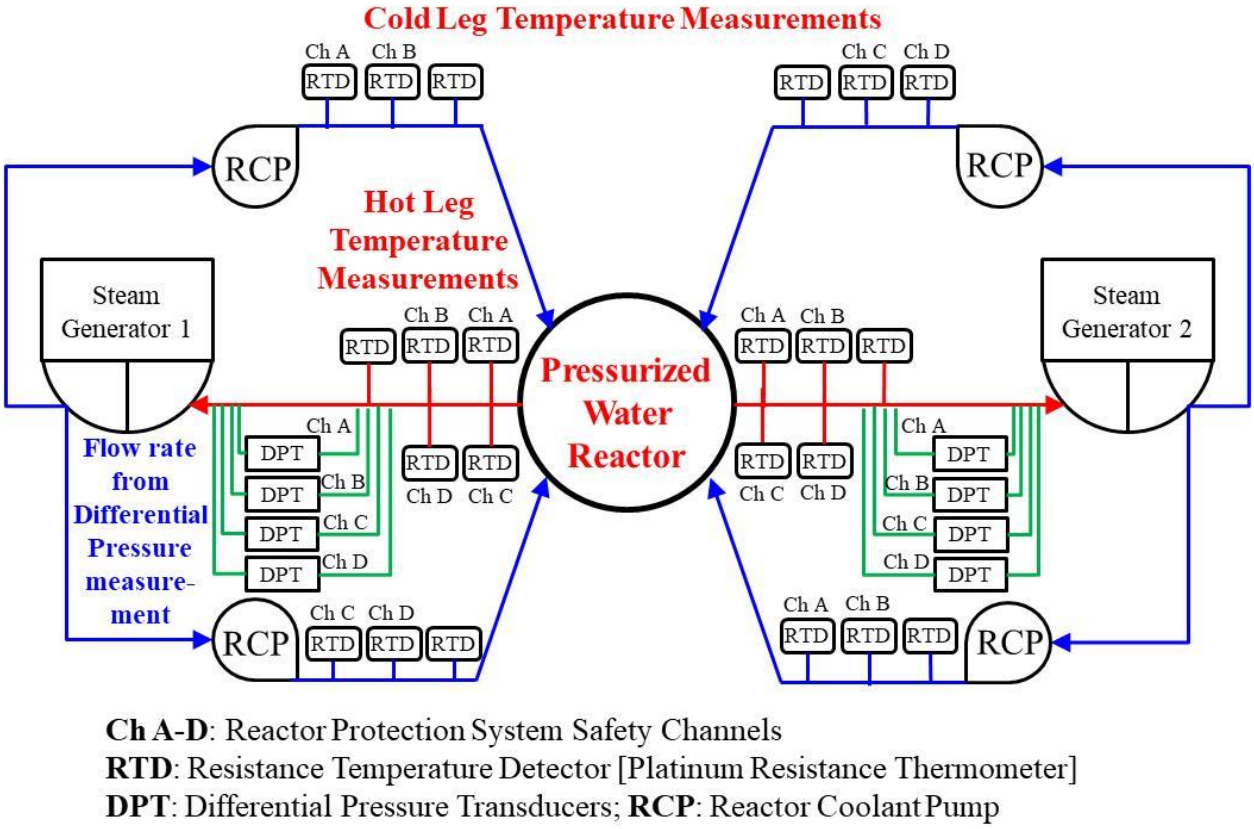


Fig. 3.7. A schematic of the instrumentation's layout in a representative PWR (El-Genk and Schriener 2022).

The logic programming of the CPCs uses the received state variables to calculate the safety parameters and compare them to preprogramed setpoints. The calculated safety parameters include: (a) the CHFR in the hottest channels in the reactor core, (b) the coolant flow rate through the reactor core, and (c) the margin of the temperature of the coolant exiting the core

from the saturation temperature at the system pressure (Fig. 3.9). The calculated CHFR is based on the determined axial distributions of the surface heat flux for the rods in the hot channels in the reactor core. The CHFR safety setpoint is typically set at 1.5–2.5. The PLC program sends a trip voting signal to the coincidence logic processer PLC when the CHFR in one of the hot channels in the core reaches or drops below its low setpoint (Fig. 3.9). Similarly, the CPC sends a trip voting signal when the margin of the reactor coolant exit temperature drops below its safety setpoint.

In addition to the trip protection functions, the CPC monitors different state variables in the plant and sends warning signals to the operator when their values exceed preprogrammed setpoints (Fig. 3.9). During steady state operation, the CPC compares the values of the coolant flow rate determined from the pump speed and programmed reactor coolant pump characteristics to that determined from the measured pressure drop across a pipe section of the hot leg. When this difference is larger than a preprogramed tolerance the CPC sends a warning signal to the operator. Another safety monitoring function of the CPC (Fig. 3.9) is to compare the shaft rotation speed of the reactor coolant pumps to that determined from the pump characteristics. The shaft rotation speed is determined from the intersections of the pump's supply curves with the demand curve of the reactor primary loop. The CPC sends a warning signal to the operator when the difference is greater than the allowed tolerance, as this may indicate a failure of the pump's speed sensors.



Ch A-D: Reactor Protection System Safety Channels
RTD: Resistance Temperature Detector [Platinum Resistance Thermometer]
DPT: Differential Pressure Transducers; **RCP**: Reactor Coolant Pump

Fig. 3.8. A layout of the instrumentation sensors for the coolant in the I&C systems of a representative two loop PWR plant (El-Genk and Schriener 2022).

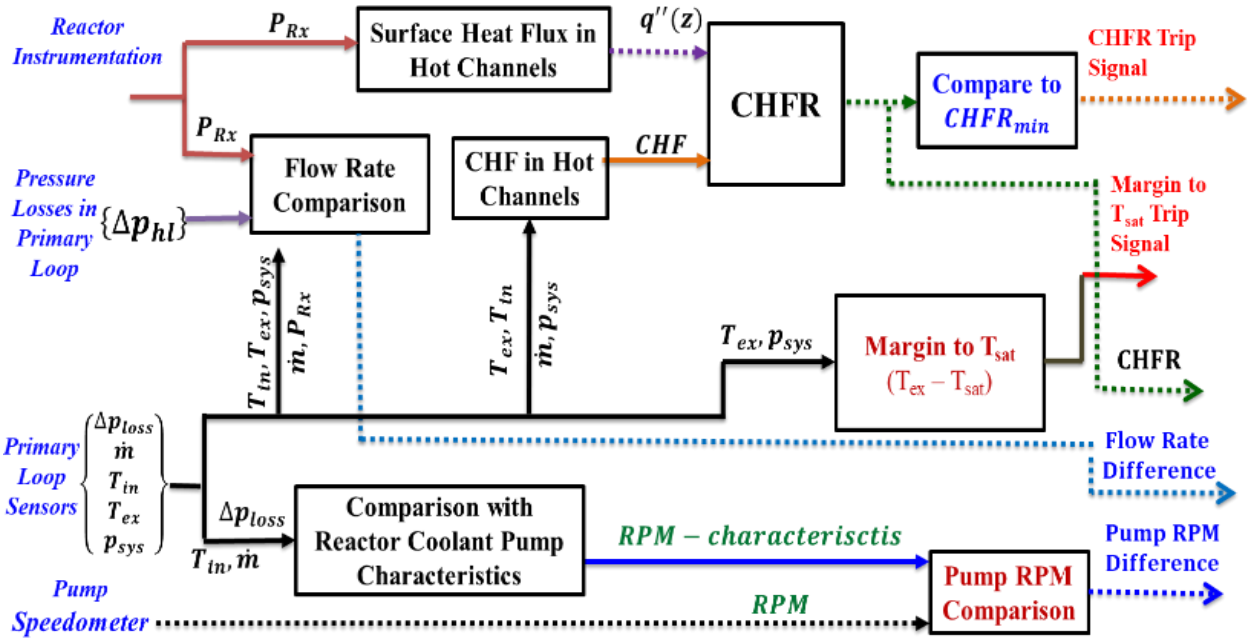


Fig. 3.9. Determination of CHFR, the temperature margin of the coolant exiting the reactor core, and the shaft rotation speed of the reactor pumps, for actuating the CPC safety functions (El-Genk and Schriener 2022).

3.2.6.1.2. Engineered Safety Features Actuation System PLC

The four emulated PLCs in the ESFAS compare the received values of the plant's various state variables to the preprogramed setpoints of the PLCs in the ESF systems (Fig. 3.10). When a received value exceeds the preprogramed setpoints, each PLC sends a voting signal to the coincidence logic processor PLC. The representative ESFAS PLC performs actuation functions for: (a) the Safety Injection System, (b) the Containment Isolation System, (c) the Main Steam Isolation System, and (d) the Auxiliary Feedwater System (Fig. 3.10). These systems intended to mitigate design basis accidents. A cyberattack that successfully prevents actuating one or more ESF functions or actuates one of these systems when not warranted can have significant consequences on the operation and safety of the plant. Thus, the ESFAS PLCs represent a potential cybersecurity target in the PMS I&C architecture of nuclear power plants.

The Containment Isolation Actuation System (CIAS) isolates the reactor containment to prevent an unplanned release of radioactivity to the environment following a LOCA (Palo Verde Nuclear Generating Station 2017). When actuated, the CIAS isolates the containment by closing the valves of the lines that penetrate the containment. The Main Steam Isolation System (MSIS) isolates the steam generators to limit the energy release into the containment when one or more of the measured signals exceed preprogramed setpoints. The MSIS actuation function generates a signal when either the pressure on the shell-side in the SG drops below a setpoint, or the water level in the SG exceeds the preprogrammed setpoint. These actuation signals isolate the main vapor/steam flow, the main feedwater flow, and blowdown lines in both SG, regardless of which steam generator generated the signals.

In the event of a LOCA, the Safety Injection Actuation System (SIAS) injects borated water into the primary coolant loops (Blank 2007; Palo Verde Nuclear Generating Station 2017). The PLC's actuation function generates a signal when either the system pressure decreases below a

setpoint, or the containment pressure increases above a setpoint. The generated signals open valves to inject borated water into the reactor coolant loops and start the emergency core cooling system.

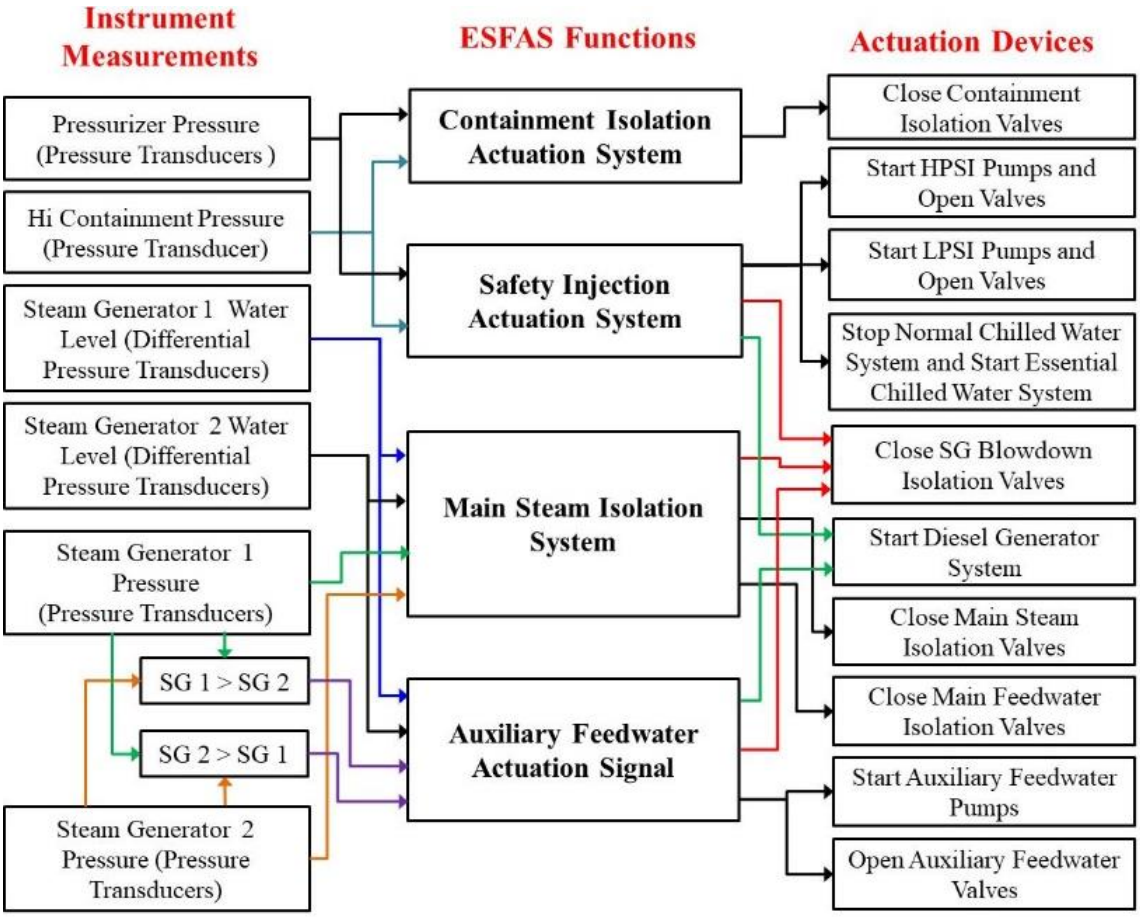


Fig. 3.10. A block diagram of the Engineered Safety Features Actuation System functions in PLC for a representative PWR plant (El-Genk and Schriener 2022).

The Auxiliary Feedwater Actuation System (AFAS) protects against dry out in the SGs (Blank 2007; Palo Verde Nuclear Generating Station 2017). The PLC generates an actuation signal when the water level on the shall-side of the steam generator decreases below a setpoint or when the difference between the measured shell-side pressures in the steam generators differ by more than a specified margin. An actuation of the AFAS assumes that the steam generator that initiated the signal is damaged and the PLC sends a signal to start the auxiliary feedwater pumps and open the auxiliary feedwater valves of the remaining, assumed intact SGs. The AFAS remains in operation until the actuation system is reset and manually secured by the plant personnel.

3.2.6.1.3. Coincidence Logic Processor PLC

The coincidence logic processer PLC compares the voting signals received from the four CPC PLCs and the four ESFAS PLCs for the four separate safety divisions. It generates a reactor trip signal when there is a 2/4 voting coincidence of the voting PLCs. Similarly, in response to a

2/4 vote by the ESFAS PLCs the coincidence logic processer PLC generates and sends actuation signals to the hardware associated with the plant's safety systems. The comparisons of the voting signals are performed separately for each ESF function. To count as a positive vote, the received signal needs to remain steady for a minimum amount of time, typically several milliseconds. This ensures that a momentary errant fluctuation in the signal does not accidentally trigger a reactor shutdown or actuate the ESF system (Palo Verde Nuclear Generating Station 2017). The combinatorial logic programming checks for all combination of the voting by the PLCs for the four safety divisions (A, B, C, and D). There are six positive voting combinations of the divisions AB, AC, AD, BC, BD, and CD. When any of the voting combinations lasts true for the required length of time, the PLC generates a control signal to either trip the reactor or actuate the specific ESF function.

3.2.6.2. Plant Operation I&C System in a Representative PWR Plant

The operation control I&C system regulates specified parameters to assist the plant operators. The emulated PLCs function independent of the operator using pre-programed setpoints. Others allow the operators to change the setpoints to adjust the plant operation. The reactor PLC automatically regulates the thermal power as specified by the operator. The pressurizer pressure PLC regulates the system pressure in the primary loop by controlling the power to the immersed proportional and backup heaters in the lower sections of the pressurizer and the water droplets spray nozzle in the upper vapor section (Figs. 3.11, 3.12).

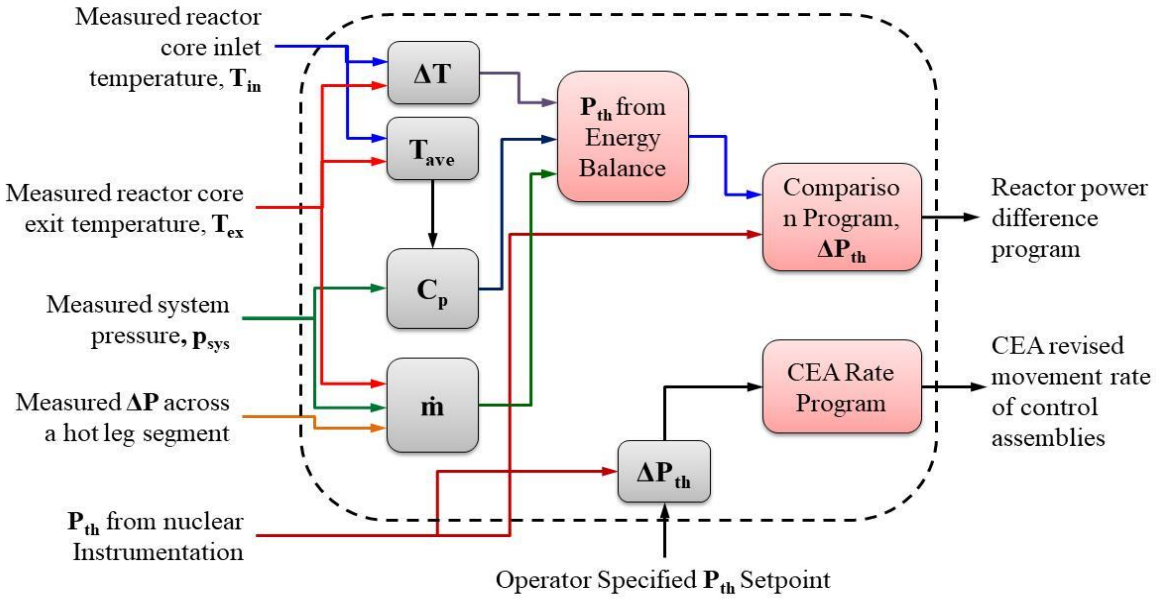


Fig. 3.11. Block diagram of control program of the reactor power regulation PLC in LOBO NCS (El-Genk and Schriener 2022).

The pressurizer's water level PLC regulates the inventory in the primary loops by controlling the water charging and letdown rates (Fig. 3.5). The feedwater PLCs adjust the rate of feedwater injection into the plant's SGs to maintain the water level in accordance with the preprogramed setpoints. The reactor coolant pumps PLCs regulate the shaft rotational speeds according to the prescribed pump characteristics. These PLCs receive the values of the calculated state variables by the PWR plant Simulink model and produce control signals for the appropriate equipment,

which are also communicated back to the Simulink model to adjust the plant's operation.

3.2.6.2.1. Reactor Power Regulation PLC

The representative Reactor Regulation PLC autonomously controls the insertion of the control rod assemblies into the core to maintain the thermal power at the level specified by the operator. This PLC does not operate during startup, but functions after the plant reaches nominal operating condition and the reactor control switches to the automatic mode. Fig. 3.11 shows a functional block diagram of the control program for the emulated PLC in the LOBO NCS platform. The PLC receives the values of the coolant temperature entering and exiting the reactor, T_{in} and T_{ex}, the pressure in the pressurizer, p_{sys}, the coolant total flow rate, $\dot{m}$, and the reactor thermal power (Fig. 3.11). It then adjusts the vertical positions of the CEAs in the core to maintain the reactor power, P_{Rx}, at that specified the operator.

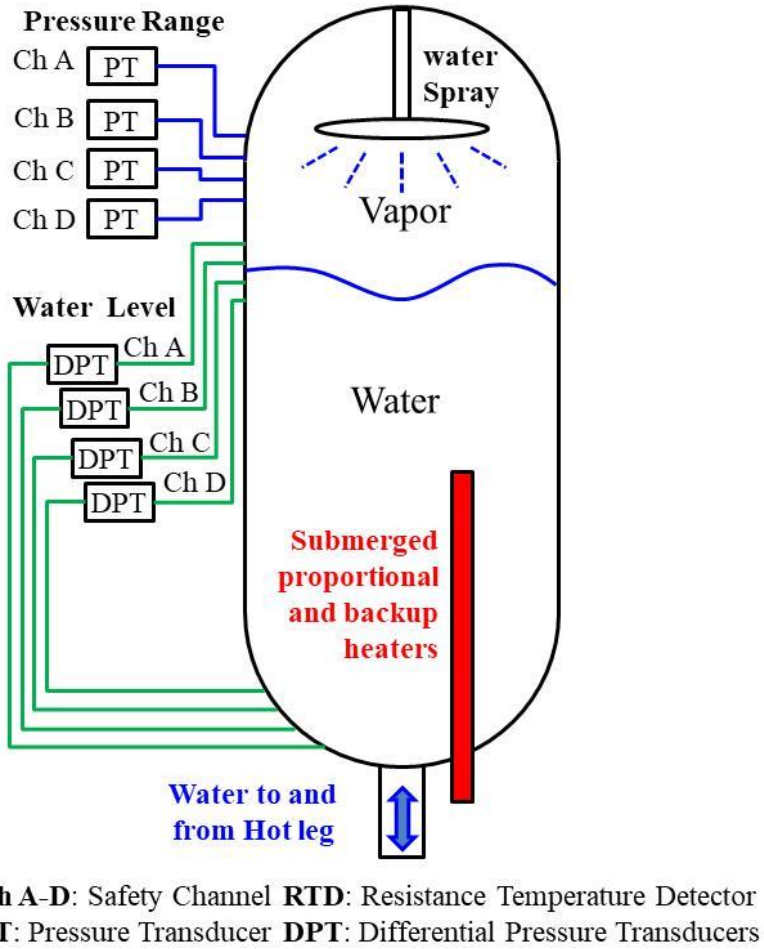


Fig. 3.12. An illustration of the measurement's sensors of the pressurizer in a representative PWR plant (El-Genk and Schriener 2022).

The control program of the PLC compares the calculated value of P_{Rx}, from the point kinetics model to that specified by the operator, P_{th}, and communicate the difference, $\Delta P_{th} = P_{Rx} - P_{th}$, to a sub-controller of the CEAs. The sub-controller calculates the needed movement rate of the CEAs to adjust the core reactivity to maintain the reactor thermal power at the specified value by the operator. This PLC also monitors the difference between the calculated reactor power by the

Simulink model, P_{Rx}, to that calculated from the overall energy balance in the primary loop, P_{th}. The value of P_{th} is based on the measured temperature rise across the reactor core, $\Delta T = (T_{ex} - T_{in})$, and the specific heat capacity, C_p, at the average coolant temperature, T_{ave}, and p_{sys}. A mismatch between the two reactor power values, which caused by an instrumentation error, recorded, and indicated to the operator for appropriate action as needed.

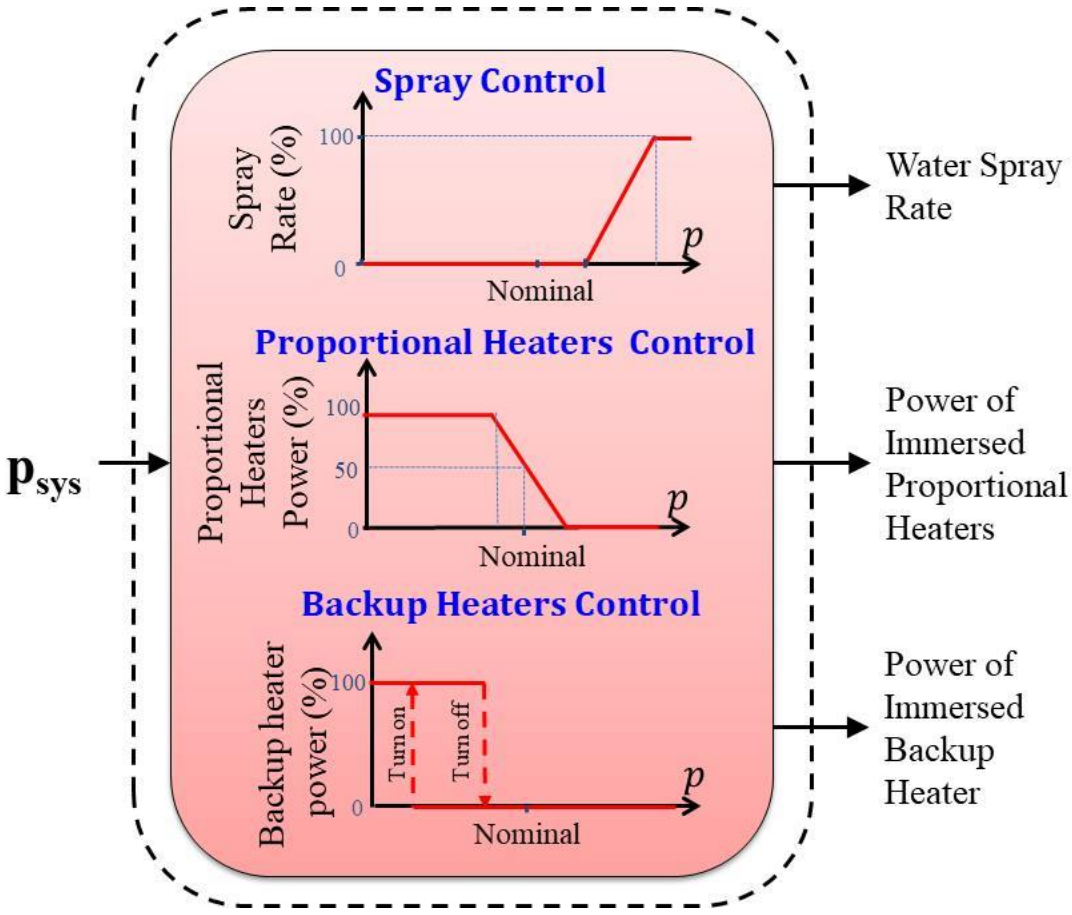


Fig. 3.13. A block diagram of the control program of the Pressure PLC in the LOBO NCS platform (El-Genk and Schriener 2022).

3.2.6.2.2. Pressure PLC

The Pressure PLC for the pressurizer adjusts the system pressure within the primary loop in accordance with preprogramed setpoints. It controls the power supplied to the immersed proportional and backup heaters and the rate of water spray into the vapor section of the pressurizer (Figs. 3.12-3.13). Fig. 3.13 shows a functional block diagram for the control program of the Pressure PLC. The value of the system pressure, p_{sys}, supplied by the physics-based Simulink model of the pressurizer represents the pressure sensors' measurements of the internal pressure in the pressurizer (Fig. 3.12). This pressure value is compared to the preprogramed pressure setpoints for three control mechanisms: water spray, the power level to the proportional heaters, and turning on or off the submerged backup heaters (El-Genk, Altamimi, Schriener 2021).

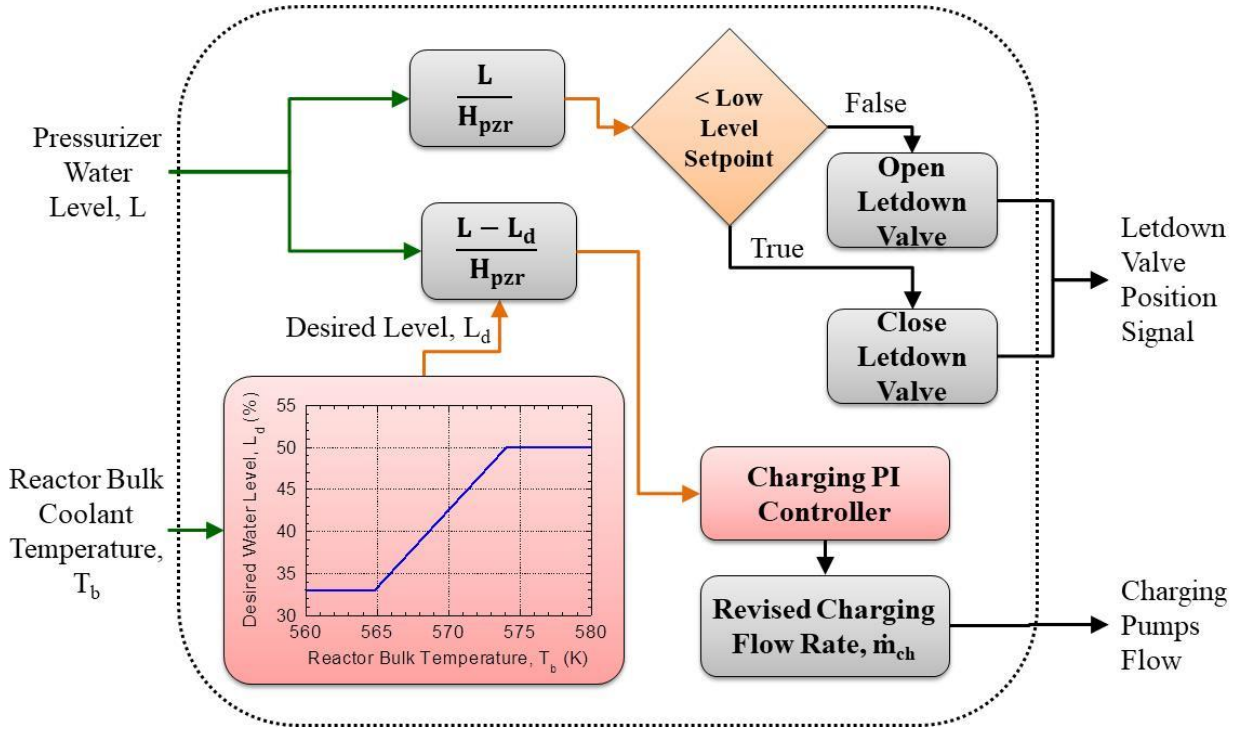


Fig. 3.14. A control program for a representative pressurizer Water Level PLC (El-Genk and Schriener 2022).

The power of the proportional heaters is regulated commensurate with the difference between the desired and actual system pressures (Fig. 3.13). During nominal steady state full power operation, the pressure is midway between those for the on and off setpoints for the proportional heaters. These heaters nominally operate at 50% of full power to make up for heat losses through the pressurizer's wall to the surrounding. When p_{sys} decreases, the power supplied to the proportional heaters increases linearly up to 100% to increases the rate of flash evaporation and hence the system pressure.

The Pressure PLC turns on the submerged backup heaters in the middle and bottom regions of the pressurizer when p_{sys} continues to decrease below its low pressure setpoint. Unlike the proportional heaters the backup heater is either fully on or fully off (Fig. 3.13). When p_{sys} increases above the low setpoint, water spray injected into the pressurizer through the swirl-vane nozzle to help reduce the system pressure. The spray valve increases the flow rate of the water droplets spray linearly proportional with the pressure increase, from 0% with the valve closed at the pressure low setpoint to 100% with the valve fully open at the upper pressure setpoint (Fig. 3.13).

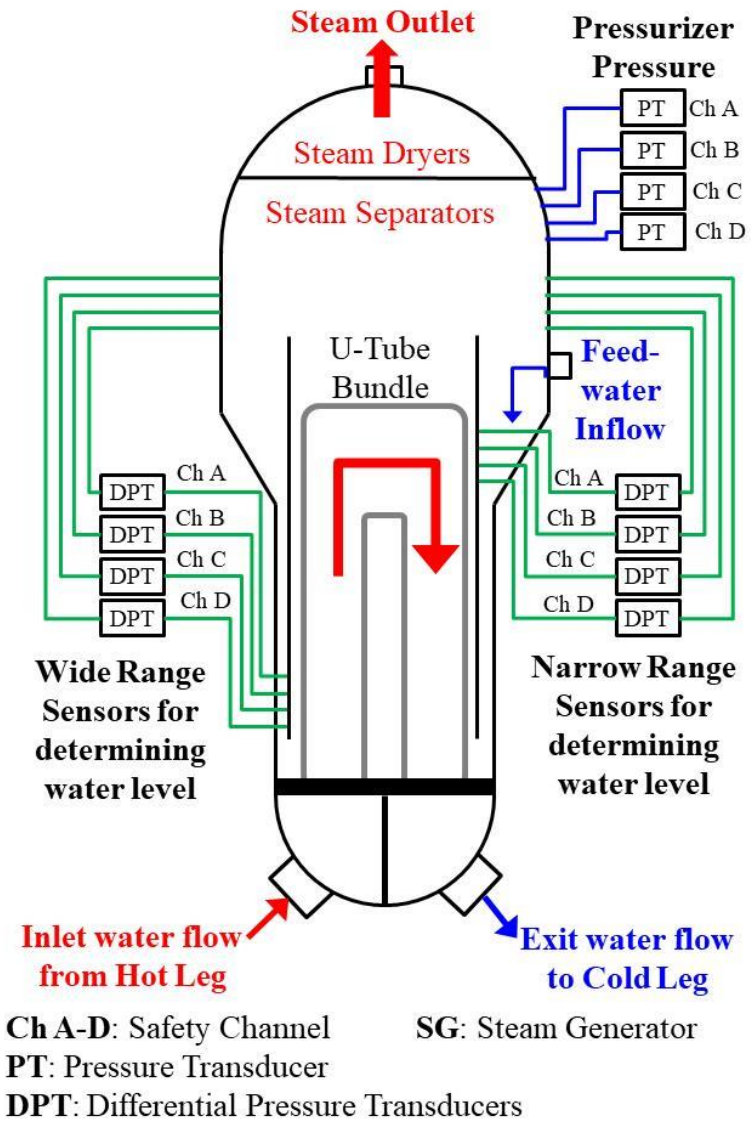


Fig. 3.15. Instrumentation arrangements in SG of a representative PWR plant in LOBO NCS platform (El-Genk and Schriener 2022).

3.2.6.2.3. Pressurizer's Water Level PLC

This PLC controls the total water inventory in the primary loops by monitoring the calculated water level in the pressurizer Simulink model. In the plant, this level calculated based on the measured water static pressure head using DPTs located along the pressurizer wall (Fig. 3.12). In addition to this value of the water level, the PLC also receives the calculated values of the average water temperature in the pressurizer, T_b (Fig. 3.14). The water level in the pressurizer adjusted by controlling the inflow and outflow rates of water to and from the primary loops. The rate of water inflow controlled by the charging pumps and the outflow by adjusting the letdown valves (Fig. 3.5). The PLC compares the actual water level in the pressurizer, L, to the preprogramed desired value, L_d, depending on the bulk water temperature, T_b. The adjustment of the water level helps accommodate the changes in the water volume in the primary loop due to thermal expansion or contraction during plant operation. The difference between the measured

and calculated water levels normalized to the height of the pressurizer, H_{pzr}, $((L-L_d)/H_{pzr})$, communicated to a PI controller to adjust charging rate (Fig. 3.14).

The PI controller acts to minimize both the present value of the normalized water level difference and its integral over time. The opening and closing of the letdown valve are based on comparing the value of L/H_{pzr} to a low water level setpoint. The letdown valve stays open when L/H_{pzr} equals or above the setpoint, otherwise closed. The difference between the charging and the letdown rates represents the net inflow or outflow of the coolant into and from the primary loop, assuming no leakage. When the water level in the pressurizer drops below the desired level L_d, the control program of the Water Level PLC adjusts the charging rate upward. The increased inflow, combined with closing the letdown valve, results in net inflow water into the primary loops to increase the water inventory. Conversely, when the water level is above the desired level, the charging rate is decreased, and the letdown valve opens.

3.2.6.2.4. Feedwater PLCs

These PLCs help adjust the water inventory on the SGs' secondary or shell sides to remain within preprogramed setpoints for ensuring that the U-tube bundles in the SG are covered with water. The PLCs, one for each SG, receive the measured water level in the SG, the calculated reactor thermal power, and the steam and feedwater flow rates determined by the Simulink models in the LOBO NCS platform. The calculated water level represents that measured in the SGs' downcomer using two sets of DPTs mounted on the wall (Fig. 3.15): a narrow range set that measures the static head of the water column in the wider upper section of the stream SG, and a wide range set that measures the static head in the annular downcomer (Palo Verde Nuclear Generating Station 2017). The internal pressure values represent those measured by pressure transducers in the upper region of the SG.

The PLCs adjust the injection rate of the feedwater on the shell sides of the SGs commensurate with the changes in the steam load demand and/or the state variables in the primary loops. The feedwater flow rate in the representative PWR plant is controlled by changing the opening of throttle valves located between the main feedwater pumps and the feedwater injection ring in the SGs (Fig. 3.15). The LOBO NCS platform uses a control parameter, C* to help the Feedwater PLCs adjust the throttle valve position (Fig. 3.16). This parameter is proportional to the product of two state variables. One is the difference between the water levels in the SG annular downcomer, L, and the desired water level, L_d, normalized to the maximum desirable water level, L_{max}. This term is determined as a function of the reactor thermal power, P_{Rx}.

The second term is the difference between the steam flow rate exiting the SGs to the turbine on the secondary loop of the plant, $\dot{m}_s$, and the feedwater flow rate into the SG, $\dot{m}_{fw}$. The C* parameter ensures that the PI controllers for the PLCs act simultaneously to minimize the difference between the current and desired water level in the SG and that between the steam production and feedwater flows. This combination helps achieve gradual changes in both the water level and feedwater rate during operational transients simulated in the LOBO NCS platform for the representative PWR plant.

The value of the control parameter C* passes through a dead band filter which zeros out the values that fall within the preprogramed dead band width, X_{db}. This inhibits action when the differences between the actual and desired levels are small, limiting the frequency of adjusting the opening of the feedwater throttle valves during the simulated operation transient. The output from the dead band filter is communicated to the feedwater PI controller to produce the desired feedwater flow rate (Fig. 3.16). The Feedwater PLCs then send command signals back to the

PWR plant Simulink model to adjust the valves and the feedwater flow rates to the plant's SGs.

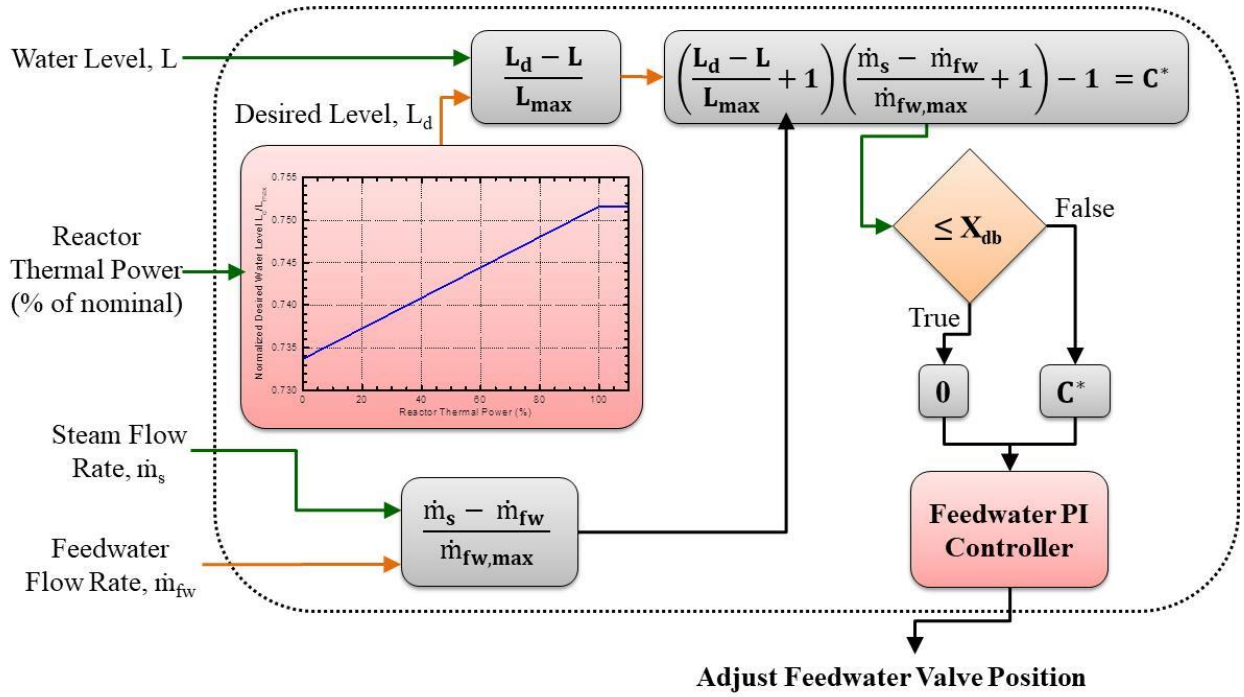


Fig. 3.16. Block diagram of control program of SG's Feedwater PLCs in the LOBO NCS platform (El-Genk and Schriener 2022).

3.2.6.2.5. Reactor Coolant Pump PLC

The PLCs controlling the reactor coolant pumps regulate the shaft rotation speed commensurate with the desired total flow rate in the primary loops in the Simulink model of a representative PWR plant. These large pumps are placed between the steam generators and the cold legs of the primary loops. They circulate the coolant in each of the four branches of the primary loop before entering the downcomer of the reactor vessel (Fig. 3.5). The control programs of the emulated pump PLCs (Fig. 3.17) in the LOBO NCS platform receive the pumps' shaft rotation speed, the reactor thermal power, the hot and cold leg temperatures, the system pressure, and the pressure drop along across a piping section of the hot leg (Fig. 3.8). The values of these state variables calculated by the Simulink models for a representative PWR plant in the LOBO NCS platform.

The pumps' PLCs use the determined total flow rate to estimate the shaft rotational speed, RPM_C, from the programed characteristics curves for the pumps (the insert in Fig. 3.17). The difference between the measured shaft rotation speed, RPM, and that determined from the pump characteristics, RPM_C, communicated to the PLCs' PI controllers. Subsequently, the emulated PLCs for the pumps adjust the shaft rotation speed of the primary pumps within preprogramed setpoints and, hence the coolant flow rates in the primary loops of a representative PWR plant. In addition to controlling the shaft rotational speed, the pumps' PLCs check the consistency of the calculated two values of the total flow rates. The first flow rate is that determined from the solution of the overall energy balance in the primary loops, as a function of the hot and cold leg temperatures, the reactor thermal power, and the water specific heat at the average coolant

temperature (Fig. 3.17). This value of the total flow rate compared to that determined from the measured pressure drop across a segment of the hot leg piping. When there is a significant disagreement between the two flow rates during nominal operation, the pumps' PLCs generate warning signals to the operator. Such a disagreement may indicate either an error in sensors' measurements in the actual plant or a malfunction of one the reactor pumps.

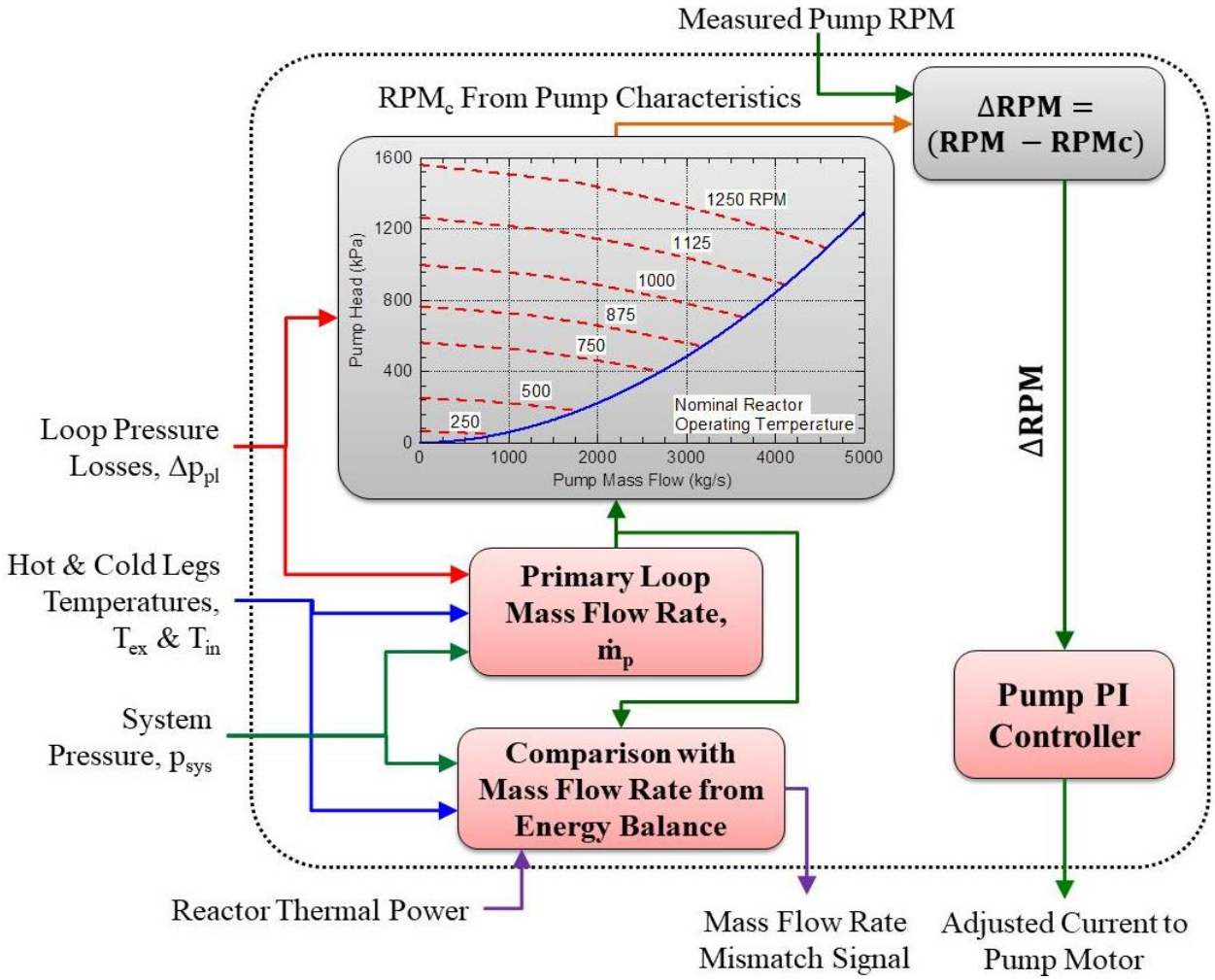


Fig. 3.17. Block diagram of a PI controller program logic for PLCs of reactor primary coolant

3.3. Summary

This section described the LOBO NCS platform developed at the UNM-ISNPS in collaboration with SNL. This versatile and modular cybersecurity 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. A variety of cybersecurity modeling platforms, such as the IAEA's ANS, developed to help address cybersecurity concerns for nuclear plant digital I&C systems, with different strengths and focuses. The LOBO NCS platform is developed for supporting cybersecurity investigations of digital I&C architectures for commercial PWR plants. This platform is designed with increased flexibility to enable applications to other nuclear cybersecurity applications, such as advanced SMRs and microreactors, and space nuclear power

systems.

The LOBO NCS platform links the Simulink models and the emulated I&C architectures using an efficient data transfer interface. The data broker and communication program couples a multitude of PLCs performing different control functions in the Simulink model. The LOBO NCS's user-friendly graphic interface provides real-time display of the calculated state variables during nominal and transient operation of the plant and while the PLCs in the I&C systems are subject to simulated cyberattacks. Simulated cybersecurity events affecting the PLCs implemented using the ManiPIO cybersecurity testing and evaluation capabilities developed at SNL in collaboration with the UNM-ISNPS.

This section also presented the dynamic model of an integrated PWR plant and emulated PLCs in representative PMS and Operation I&C systems. Following the modular philosophy of the LOBO NCS platform these models can be adapted to represent different PWR designs and I&C architectures. This allows the dynamic PWR plant model and emulated PLCs to investigate how simulated cybersecurity events impact the operation of the PLCs and in turn the state variables of the plant in response the PLCs' control signals. The next section presents the results of a series of sample cybersecurity tests of the LOBO NCS platform demonstrating its capabilities to investigate the effects of simulated cyberattacks on different PLCs within the representative plant I&C systems.

4. LOBO NCS CYBERSECURITY INVESTIGATIONS FOR A REPRESENTATIVE PRESSURIZED WATER REACTOR PLANT

This section presents results of select investigations demonstrating the ability of the LOBO NCS platform to investigate the effects of simulated cybersecurity events on the PLCs in the I&C system. In these investigations, the LOBO NCS platform links the developed Matlab Simulink physics-based model of a representative PWR plant to the emulated PLCs in the Operation and PMS I&C systems. The results compare the responses of the plant and PLCs during nominal operation to those when the emulated PLCs are targets to simulated False Data Injection Attacks (FDIAs) using the ManiPIO program (El-Genk, et al. 2021). ManiPIO used to generate simulated Modbus TCP FDIAs on the input and output holding registers of the emulated PLCs. The FDIAs in these scenarios timed to affect the PLCs in the I&C system of the plant during an operational transient. Subsection 4.1 investigates the effects of an FDIA targeting the emulated Feedwater PLC of the SG. Sections 4.2-4.4 use the LOBO NCS platform to model a simulated reactor startup for the representative PWR with and without an FDIA targeting on of the PLCs in the I&C system. Subsection 4.3 presents results of a cybersecurity investigation of a simulated FDIA targeting the emulated Pressure PLC of the pressurizer in the representative PWRs Operation I&C system. Finally, subsection 4.4 presents the results of a scenario where a simulated FDIA targeting one of the emulated CPC PLCs in the plant PMS I&C system.

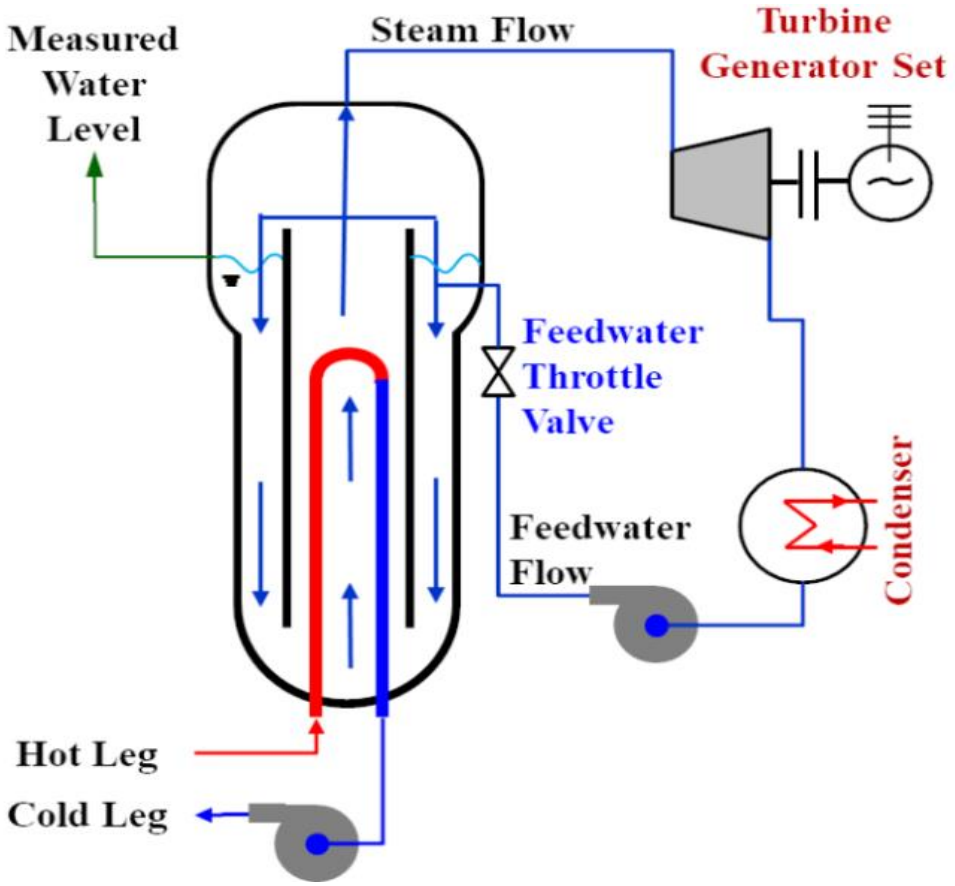


Fig. 4.1. Linked SG model to secondary loop in a representative PWR plant (El-Genk, et al. 2021).

4.1. Steam Generator Nominal Operation and when Targeted by an FDIA

The first cybersecurity scenario investigated uses the LOBO NCS platform to simulate an operational transient using the SG Simulink model (Fig. 4.1) linked to the SG's emulated Feedwater PLC. The simulated transient follows a change in steam demand for nominal operation and when the Feedwater PLC is subject to a FDIA. The simulated nominal operation transient of the SG in a representative PWR plant models a 10% increase in the steam load demand followed by a return to the original steam demand level (Fig. 4.2). These results are compared to those of the same transient but while the emulated Feedwater PLC is targeted by a simulated FDIA by the ManiPIO program (El-Genk et al. 2021). In this scenario the SG Simulink model is run standalone separate from the integrated PWR plant model. In this configuration the parameters for the water flow entering the SG from the hot leg specified in the model input.

The LOBO NCS platform links the SG model to the emulated Feedwater PLC (Fig. 3.16) that runs on a Raspbian VM (Fig. 3.3). In this simulation the OpenPLC program configured with an input scan time of 10 ms and the SG Simulink model used a fixed timestep of 20 ms. The time synchronization function in LOBO NCS kept the simulation in synch with real time. The emulated Feedwater PLC (Fig. 3.16) uses a PI controller to regulate the rate of the feedwater to the steam generator by adjusting the position of the feedwater throttle valve (Fig. 4.1). The values used for the proportional constant, P = 0.02, and integral constant, I = 0.6, for the PI controller produce the smoothest results (El-Genk et al. 2021).

The simulated operation transient starts from nominal steady state operation conditions. These are the steam demand and feedwater flow rates of 660 kg/s, a normalized water level in the SG of 74.5%, and water temperature of 594.1 K in the hot leg of a representative PWR plant (Figs. 3.6 and 4.1). The flow rate and temperature of the water entering from the hot leg to the U-tubes of the steam generator are kept constant throughout the transient. The SG model calculates the changes in the water level in the annular downcomer and the exit steam quality to the secondary loop as the steam load demand increases. The operation transient begins at t = 100 s (point 1 in Fig. 4.2) in response to a 10% linear increase in the steam load demand over a period of 600 s (point 2 in Fig. 4.2). Subsequently, the steam demand is held steady for 600s (point 3 in Fig. 4.2) before decreasing linearly initial value at t = 1,300 s (point 4 in Fig. 4.2).

Figure 4.2 presents the calculated transient response of the SG model following a 10% linear increase in steam load demand and a subsequent linear decrease in steam demand to its initial value. The steam generation rate increases in response to the simulated increase on the steam load demand. This increases the rate of heat removal from the water flowing from the hot legs through the U-tube bundles in the steam generator and hence of the rate of boiling of the secondary loop's water flowing on the shell side of the U-tubes bundle in SG (Fig. 4.1). The Feedwater PLC increases and decreases the feedwater flow rate (Fig. 4.2b) in response to the simulated linear increase and decrease in steam demand (Fig. 4.2a).

The PLC response lags the increase in the steam demand, decreasing the water level on the secondary side of the SG (Fig. 4.2c). During the simulated transient (Fig. 4.2a), the water level in the SG (Fig. 4.2c) decreases to 74.5%, which is 0.9% lower than its initial steady state value of 75.4% (Fig. 4.2c). When the steam load demand returns to its initial value the Feedwater PLC injects water into the SG at a higher rate than that of the steam from SG to the turbine. Subsequently, the PLC returns the water level in SG and the feedwater injection rate to their initial values at the end of the simulated transient (points 1, 4 in Figs. 4.2b and c).

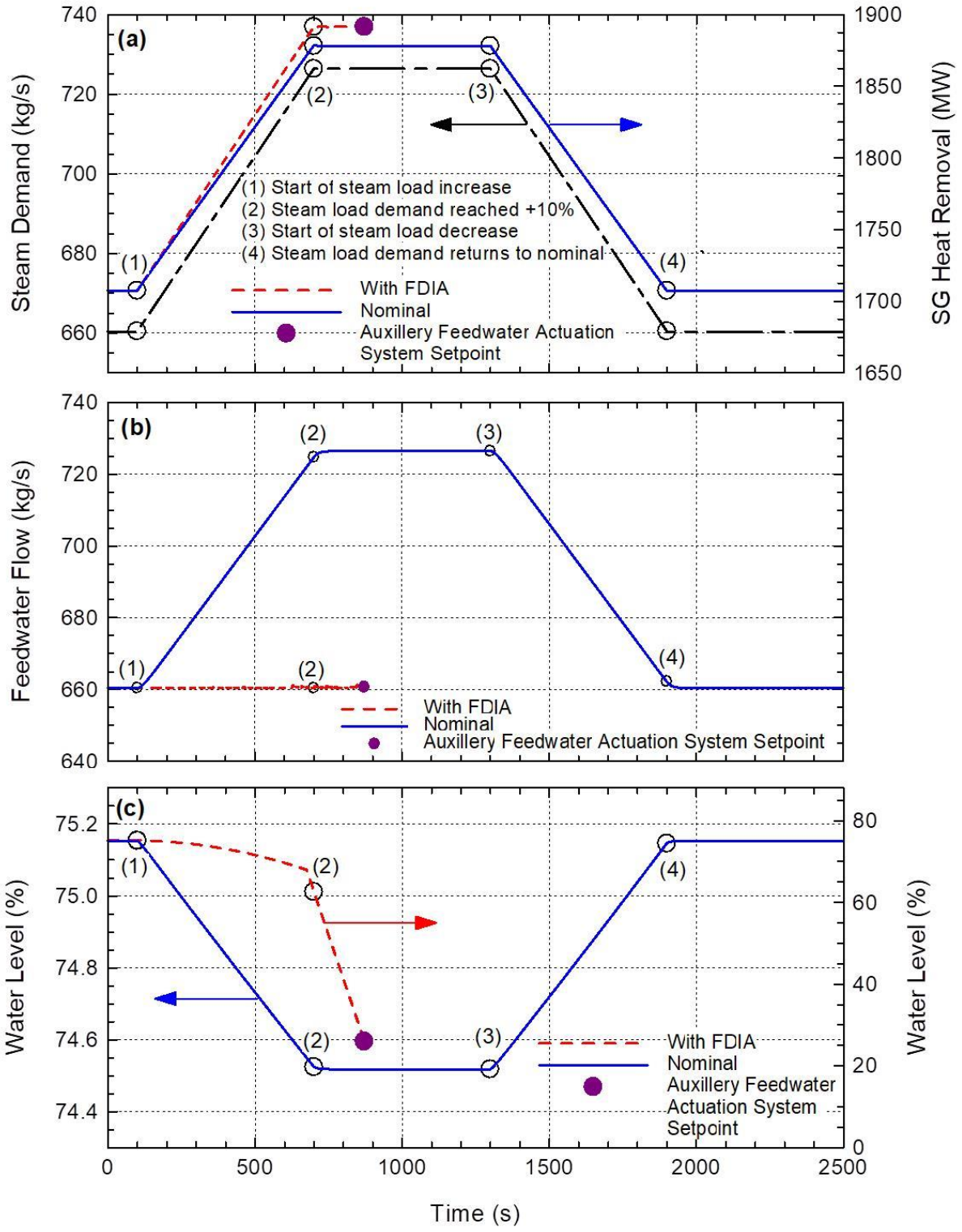


Fig. 4.2. Results of simulated transient of SG linked to the Feedwater PLC following a 10% increase in steam demand during of nominal operation and when the PLC is a target to a simulated FDIA by ManiPIO program in the LOBO NCS Platform (El-Genk, et al. 2021).

4.1.1. Response of Representative PWR SG Model with a Simulated FDIA

The same simulated transient following a 10% sequential linear increase and decrease in steam load demand is repeated while the emulated feedwater PLC is under a simulated FDIA generated by the ManiPIO program. Obtained results are compared to those with the PLC operating nominally in Figs. 4.2a-c. The simulated cyberattack monitors the water level in the SG that is stored in the input memory registers of the OpenPLC runtime for the Feedwater PLC. The simulated FDIA begins while the water level in the SG is decreasing in response to the increase in the steam load demand. The ManiPIO program repeatedly overwrites the memory register associated with the SG water level prior to the increase in the steam load demand. The FDIA attempts to obscure the effects of the transient and to manipulate the PLC to not increase the feedwater injection rate in response to the actual decrease in the water level in the SG.

As shown in Fig. 4.2 as the steam demand continues to increase (Fig. 4.2a) the FDIA successfully manipulated the PLC to maintain the feedwater injection rate steady at its preattack value (Fig. 4.2b). This causes the water level in the SG to decrease faster than nominal (Fig. 4.2c). The change in the slope of the decreasing water level in Fig. 4.2c is due to the change in the cross-sectional area of the annular downcomer in the SG as the water level drops from the wider upper section to the narrower lower section (Fig. 4.1).

The water level in the SG continues to decrease until reaching the actuation setpoint of the ESFAS PLC (Fig. 3.10) indicated by the solid circle symbol in Figure 4.2a-c. This PLC votes to activate the Auxiliary Feedwater Actuation System at t = 872s of the simulated transient while the Feedwater PLC is under the simulated FDIA attack. At such time, the simulated transient is terminated. During the FDIA the rate of heat removal in the SG is higher than nominal (Fig. 4.2) because of the decrease in the water recirculation rate in SG due to the low feedwater injection, while the SG continues to supply the same steam load.

At the time of activating the Auxiliary Feedwater Actuation System, the water level on the shell side of the SG decreases to only 26%. This is much lower than the nominal value of 74.5% prior to initiating the simulated transient. The results in Figs. 4.2a-c, demonstrate the abilities of the ManPIO program of successfully simulating FDIAs on the emulated PLCs when connected to a physics-based Simulink models of a representative PWR plant and components. The next subsection presents results of a test of the integrated representative PWR plant model coupled to multiple emulated PLCs simulating a reactor startup scenario for both nominal operation and with two different simulated FDIAs.

4.2. Simulated Nominal Startup Transient of Representative PWR Plant

This subsection presents the results using the LOBO NCS platform to simulate a reactor startup of the integrated Simulink model of a representative PWR plant linked to the emulated PLCs in the Operation I&C system (Figs. 3.3–3.6). During this simulation, the Simulink model of the integrated PWR plant controlled by the PLCs of the pressurizer's Pressure and Water Level, the SG's Feedwater, and the reactor coolant pumps. The model also follows a user input script of the withdrawal of the control assemblies in the reactor core and the soluble boron concentration in the coolant. The Simulink model uses a fixed discrete simulation timestep of 20 ms and the emulated PLCs configured with an input scan time of 50 ms. The results of the simulated startup transient presented in Figs. 4.3 - 4.7 with the plant starting up at a hot critical condition. The simulated reactor startup initiated by withdrawing the control element assemblies in the core to insert 2.07¢ of external reactivity (point 1 in Figs. 4.3-4.7) and increase the reactor power to 2% of its nominal full power value (point 2 in Figs. 4.3-4.7). The rate of steam supply

by the SG increases commensurate with the increase in the reactor thermal power (Fig. 4.6a).

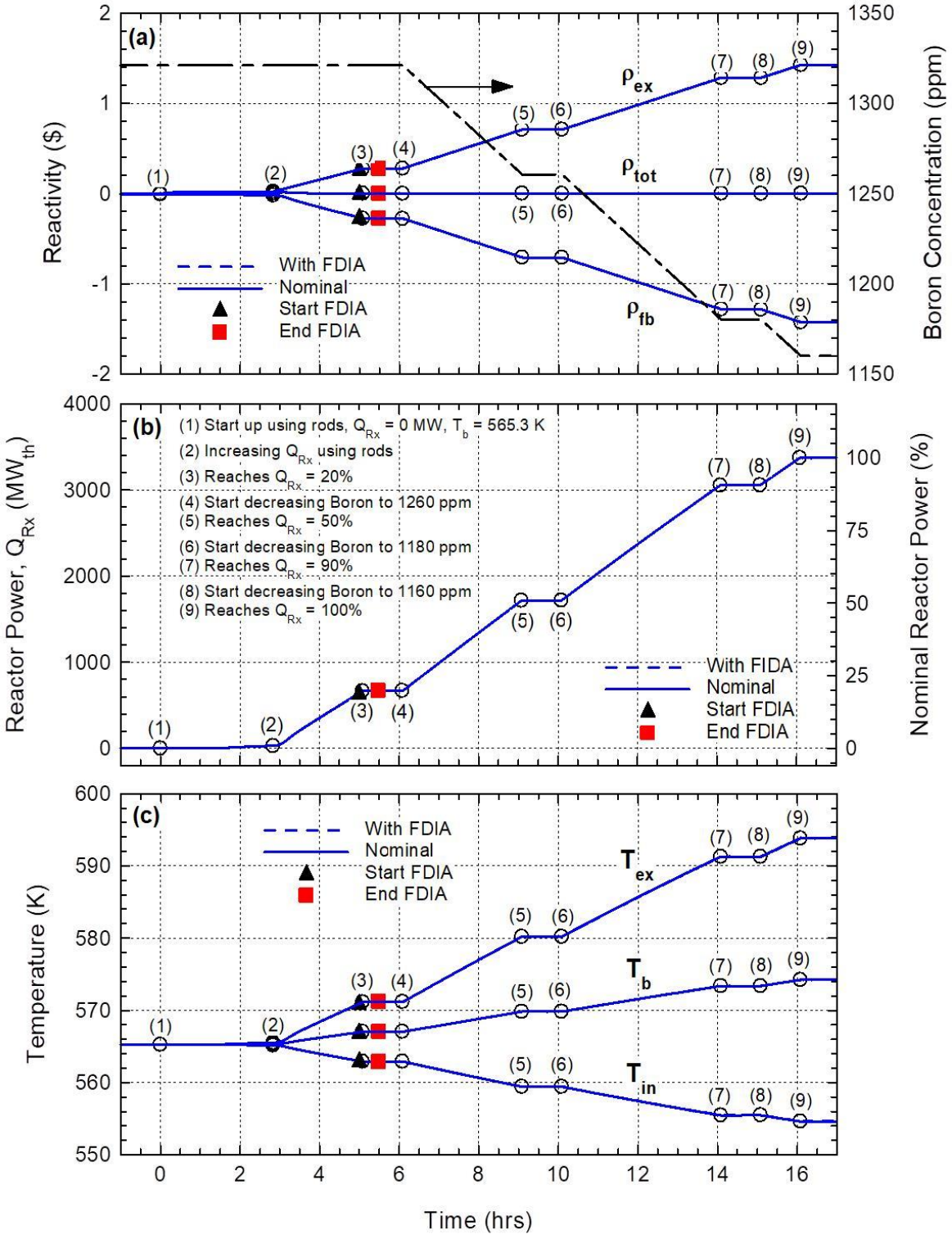


Fig. 4.3. Calculated state variables of a representative PWR plant using the reactor Simulink model during simulated startups without and with a FDIA (El-Genk and Schriener 2022).

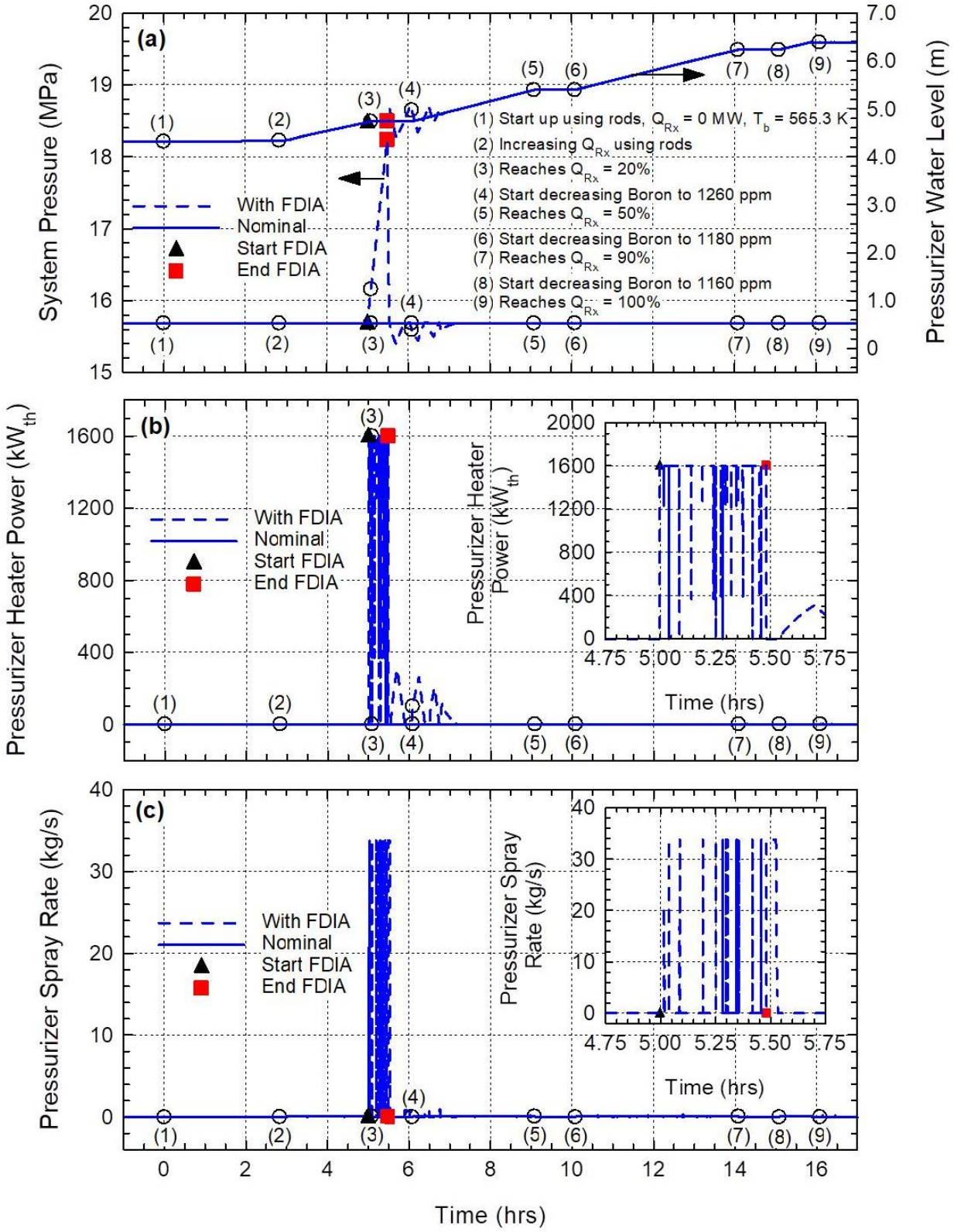


Fig. 4.4. Calculated state variables of a representative PWR plant using the pressurizer Simulink model linked to the Pressure PLC during a simulated startup without and with an FDIA (El-Genk and Schriener 2022).

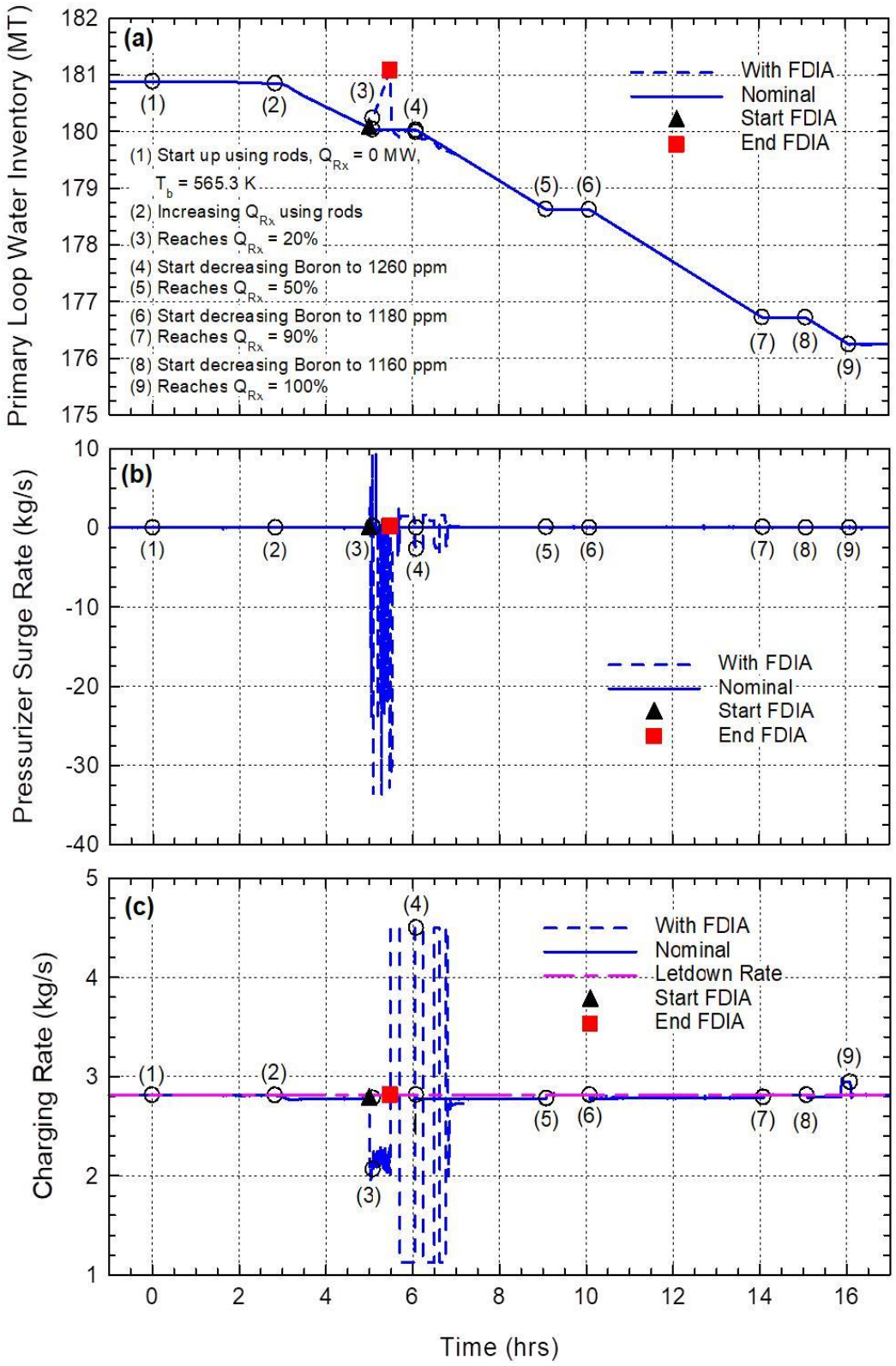


Fig. 4.5. Calculated state variables of a representative PWR plant using the primary loop Simulink model linked to the pressurizer Water Level PLC during a simulated startup without and with an FDIA (El-Genk and Schriener 2022).

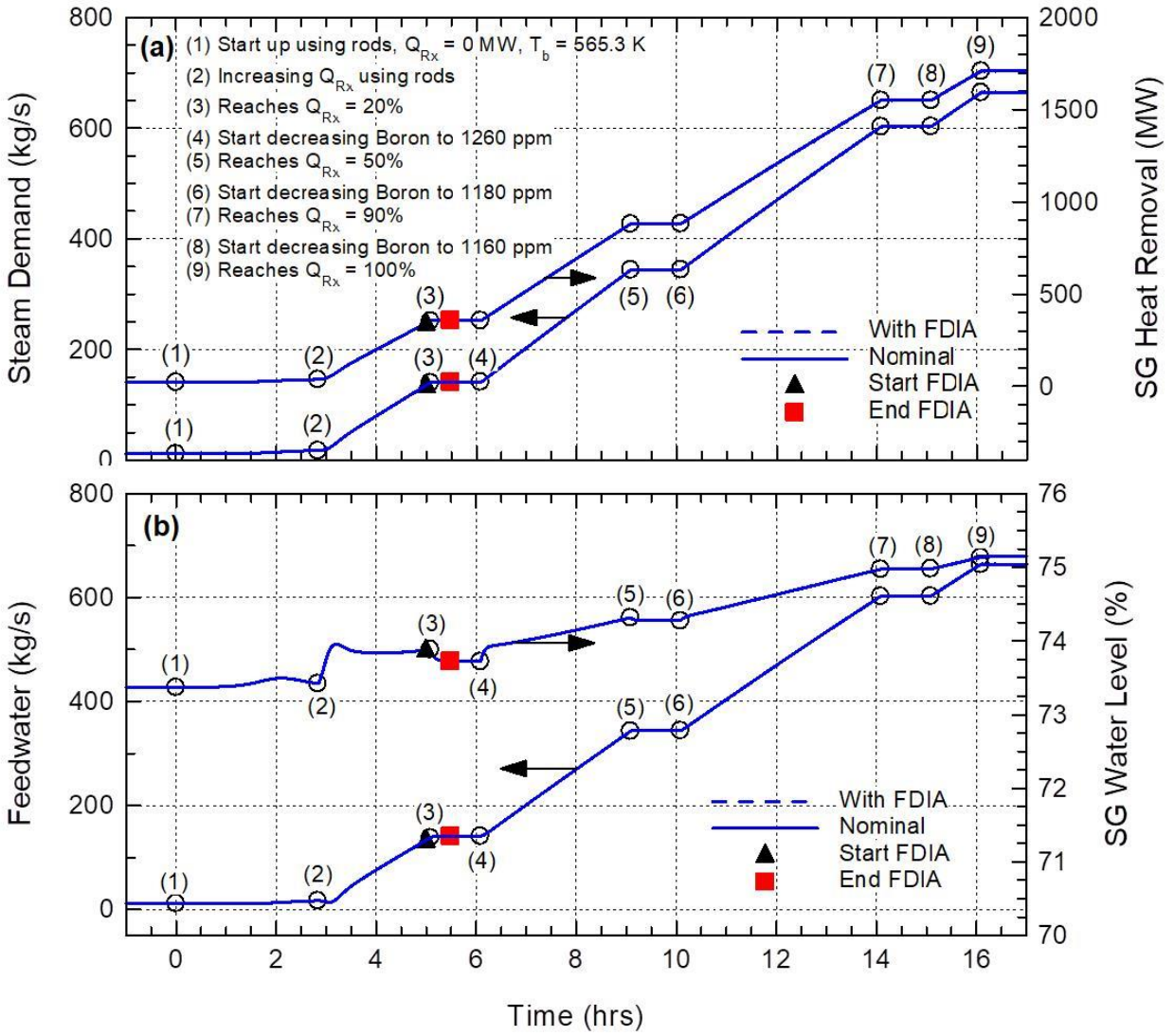


Fig. 4.6. Calculated state variables of a representative PWR plant using the SG Simulink model linked to Feedwater PLC during a simulated startup without and with an FDIA (El-Genk and Schriener 2022).

The plant startup begins with: (a) all four reactor coolant pumps running at a shaft rotation speed of 1,053.1 rpm and dissipating 15 MW_{th} into the circulating water in the primary loops, (b) the pressurizer operation controlled by the Pressure and Water Level PLCs to maintains a system pressure of 15.686 MPa, (c) the circulating water in the primary loops at a mean temperature of 565 K due to the thermal dissipation from the reactor pumps, and (d) the heat from the hot legs of the primary loops being removed in the steam generators to the circulating water from secondary loop.

At point (2), the control element assemblies in the reactor core are withdrawn further to insert a total of 27.77¢ of external reactivity and raise the reactor thermal power to 20% of nominal (point 3 in Figs. 4.3-4.7) and increase the rate of steam generation to the turbine on the secondary side of the plant. These conditions are held steady for one hour to allow the system to achieve steady state operation at this power level. Subsequently, the position of the control element

assemblies in the core is held constant and an additional external reactivity insertion is accomplished by diluting the concentration of the soluble boron in the circulating primary coolant in the reactor core.

The boron concentration initially at 1,321 ppm, decreased to 1,260.6 ppm to bring the reactor power up to 50% of nominal (point 5 in Figs. 4.3-4.7). This condition held constant for one hour for the operators to recalibrate the nuclear instrumentation. Subsequently, the soluble boron concentration in the primary loop further decreased to 1,180.1 ppm to increase the reactor power to 90% of nominal (point 7 in Figs. 4.3-4.7). This power level held constant for one hour for the nuclear instrumentation to be recalibrated prior to bringing the reactor to full power. To do that, the boron concentration in the primary loop decreased further to 1,060 ppm and the reactor thermal power eventually reached 100% of nominal or 3,373 MW_{th} (point 9 in Figs. 4.3-4.7).

The transient values of select state variables of the plant during the described startup sequence are shown in Figs. 4.3- 4.7. Results in Fig. 4.3a-c are of the state variables calculated by the developed reactor Simulink model in the LOBO NCS. Results in Fig. 4.4a-c are of the pressurizer model linked to the Pressure PLC. The results of primary loop model linked to the pressurizer's Water Level PLC shown in Fig. 4.5a-c. The calculated state variables by the SG model linked to the Feedwater PLC are shown in Fig. 4.6a-b. The calculated water flow rate and the shaft rotation speed of the primary pump model linked to the pumps PLCs shown in Fig. 4.7.

During the simulated start up transient the increase in the reactor thermal power (Fig. 4.3b) increased the flow rate and exit temperature of the coolant circulating through the reactor core (Fig. 4.3c). The increased temperature introduces a negative reactivity feedback, which equals the positive external reactivity insertion, and maintains the reactor core critical with near zero total reactivity (Fig. 4.3a). The corresponding decrease in the temperature of the coolant entering the reactor core caused by the increased rate of steam production in the SG to the turbine in the secondary side of the PWR plant (Fig. 4.6a). As shown in Fig. 4.3c, the increase in the exit temperature of core coolant is more than the decrease in its inlet temperature, increasing the bulk temperature of the coolant/moderator in the core. Such increase in temperature introduces a negative temperature reactivity feedback into the core (Fig. 4.3a).

The Feedwater PLC adjusts the rate of water injection to maintain the water level in the SG at the preprogramed setpoint (Fig. 4.6b). The magnitude of the adjustment depends on the reactor thermal power during the simulated startup transient (Fig. 3.16). During the startup sequence the Pressurizer PLC maintains the system pressure within preprogramed setpoints (Fig. 3.13). As a result, the system pressure experiences minor change relative to the nominal value of 15.686 MPa (Fig. 4.4a). This accomplished by small adjustments of the electrical power to the immersed proportional heaters (Fig. 4.4b) and of the water droplets spray in the pressurizer (Fig. 4.4c) (El-Genk, Altamimi, Schriener 2021).

The thermal expansion of water in the primary loop during the simulated startup scenario causes a surge-in of water into the pressurizer (Fig. 4.5b). In response, the Water Level PLC for the pressurizer decreases the charging rate of the primary loop to maintain the water level in the pressurizer within preprogramed setpoints (Figs. 4.4a and 4.5c). Decreasing the charging rate below the letdown rate in the primary loops (Fig. 4.5b) decreases in the total coolant inventory in the primary loops (Fig. 4.5a). The Water Level PLC increases the setpoint commensurate with the reactor bulk coolant temperature (Fig. 4.3c). This helps accommodate the thermal expansion of the primary loops coolant while minimizing the adjustment of the charging rate (Figs. 4.3a and 4.5c). Over time, the water level in the pressurizer follows a similar profile to that of the reactor thermal power, increasing linearly during the simulated external reactivity insertion

periods (Figs. 4.3a-b, 4.4a).

The increased water level in the pressurizer increases the system pressure (Fig. 4.4a) prompting the Pressure PLC to decrease the power to the submerged electrical heaters and actuate the droplets spray of subcooled water from the cold leg into the saturated steam region of the pressurizer (Figs. 4.4b-c). The minor increase in the charging rate of the primary loops between points (8) and (9) during the startup scenario is because the PI controller of the Water Level PLC over adjusts the charging rate when the reactor thermal power increases from 90% to 100% full power (Fig. 4.5c). To compensate for these differences, the PLC adjusts the charging rate to align the water level with the preprogramed setpoint (Fig. 4.4a).

The pump PLC increases the shaft rotation speed during the simulated reactor startup to increase the mass flow rate of the water coolant through the core commensurate with the increase in the reactor power (Fig. 4.7). The increased shaft rotation speed increases the pump head and hence the flow rate of the water coolant in the primary loops (Fig. 4.7). The pump shaft speed is 1,053 rpm at the start of the simulated startup (point 1 in Fig. 4.7) increases to 1,069 rpm at the end of the external reactivity insertion at point (9). It continues to increase slightly at the end of the 17-hr long startup transient and levels off later than other controlled parameters. At the end of the simulated reactor startup transient the integrated PWR plant Simulink model the plant operates at nominal full power conditions.

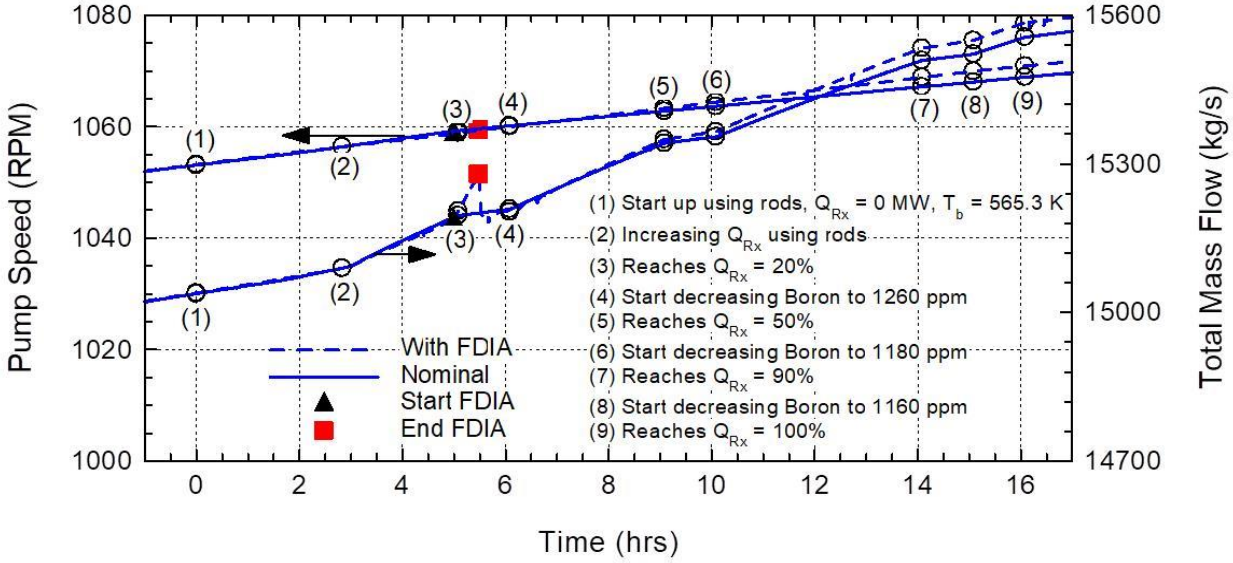


Fig. 4.7. Calculated state variables of a representative PWR plant using the linked Simulink model of the reactor coolant pump to the pumps PLCs during a simulated startup without and with an FDIA (El-Genk and Schriener 2022).

4.3. Simulated Startup with an FDIA Targeting Pressure PLC

This subsection investigates the transient response of the integrated PWR plant Simulink model linked to the PLCs in the I&C system during the same startup scenario described in the previous subsection, but with the pressurizer's pressure PLC is targeted by a simulated FDIA. The simulated cyberattack is timed to begin at t = 5 hrs. into the simulated startup transient (solid triangular symbol in Figs. 4.3–4.7) at the end of the second external reactivity insertion. At such point, the control element assemblies are withdrawn from the reactor core to bring the thermal power to 20% of the nominal (Figs. 4.3 and 4.4). The ManiPIO program writes a false low

system pressure of 15 MPa to the Modbus input holding register of the Pressure PLC. In response the PLC's logic programming sends commands to turn the electrical powers to the immersed proportional and backup heaters fully on and keep the water spray fully off. The simulated FDIA lasts for 0.5 hr. (solid square symbol in Figs. 4.3–4.7), and beyond which the Pressure PLC returns the plant to its normal operating conditions.

Figures 4.3–4.7 compare the results of the simulated startup of a representative PWR plant with a FDIA targeting the Modbus input holding register of the pressure PLC to those obtained earlier for a nominal startup without a FDIA. Prior to the introduction of the simulated FDIA, the Simulink model of the integrated PWR plant calculates the same state variables as during the nominal startup. After the FDIA in introduced, the ManiPIO program continues to repeatedly overwrite the system pressure in the Modbus holding register with an artificially low value of 15 MPa. In response, the Pressure PLC sends a control signal to turn on the proportional heaters to full power and switch the backup heaters on (Fig. 4.4b). Together these heaters supply 1.6 MW_{th} to the water within the pressurizer which increase the rate of flash evaporation into the upper vapor region of the pressurizer to increase the system pressure (Fig. 4.4a).

The simulated FDIA on the Pressure PLC rapidly increases the system pressure for the duration of the FDIA (Fig. 4.4a). This pressure peaks at 18.238 MPa, which is 2.553 MPa higher the nominal pressure setpoint of 15.686 MPa. Despite the high pressure the FDIA manipulates the PLC to keep the heaters on and close the water spray nozzle and the pressure relief valve. During the simulated FDIA the ManiPIO program competes with the data communication program in the LOBO NCS to write to the holding register of the Pressure PLC. The rate at which the ManiPIO code sends overwrite requests is set to run as fast as the code can process and is measured to have a period of ~1.1 ms. In contrast, the data broker & communication program communicates with the PLC once per 50 ms simulation timestep.

Because these programs communicate with the PLC at different frequencies, their write events are sometime misaligned. For example, occasionally the Modbus TCP writes request received by the PLC prior to reading the stored value in the register that is received from the communication program and not the simulated cyberattack. These instances correspond to the spikes in the inserts in Figs. 4.4b and c. When they occur, the PI controller attempts to correct the high-pressure by momentarily shutting off the heaters and injecting water spray droplets into the pressurizer to induce condensation and decrease the system pressure (Figs. 4.4a-c). Once the simulated cyberattack again overwrites the false low pressure the water spray shuts off and the submerged heaters turn back on. The resulting brief misalignments do not appear to affect the rise in the system pressure during the FDIA.

The increase in the system pressure causes out-surges of the water from the pressurizer into the hot leg of the primary loop (Fig. 4.5b). Conversely, the decreases in the system pressure following the actuation of the water droplets spray causes and surge-in from the hot leg into the pressurizer. During the series of surge-in and surge-out events the pressurizer's Water Level PLC attempts to change the charging rate of water into the primary loops to keep the water level in the pressurizer at the programmed setpoint (Fig. 4.5c). This results in oscillations in the total water inventory in the primary loops as the Water Level PLC attempts to increase and decrease the charging rate water into the primary loops in response to the decrease and increase in system pressure, respectively (Figs. 4.5a-c). The combined effects of the increased pressure and the adjustments of the water charging rate slightly increases the water inventory in the primary loop compared to that at nominal conditions (Fig. 4.5a).

The changes in the system pressure also affect the water properties in the primary loop, and

hence the mass flow rate of the water coolant by the reactor pumps (Fig. 4.7). The Pump PLC slightly adjusts the shaft rotation speed of the pumps to maintain the flow rates through the reactor core during the startup scenario with a FDIA within preprogramed setpoints. The effects of the simulated FDIA on the reactor coolant inlet and exit temperatures and the state variables calculated by the SG Simulink model in the LOBO NCS are negligible (Figs. 4.3c and 4.6).

Once the simulated FDIA ceases, the Pressure PLC returns the system pressure to its normal value. The PLC acts to rapidly decrease the system pressure by fully opening the water spray nozzle (Figs. 4.4a and c). The Water Level PLC also acts to bring the water inventory in the primary loops back to nominal, in line with the system pressure (Fig. 4.5a and c). The control actions of this PLC dampen oscillations in the water level until reaching the nominal value (Fig. 4.4a, 4.5c). Most of the other state variables return to their calculated values during the nominal startup without an FDIA (Figs. 4.3-4.6). The exception is the pumps' shaft rotation speed. This is because the Pump PLC does not adjust downward the shaft speed, which remains slightly higher than nominal during the simulated startup transient with an FDIA (Fig. 4.7).

The presented results show that the simulated FDIA on the emulated Pressure PLC significantly increases in the system pressure. The FDIA attempted to overwrite the actual system pressure to the input holding register of the pressurizer PLC every scan cycle. Occasionally during the simulated FDIA the nominal pressure value did get through to the PLC. In these instances, the effects on the pressure rise during the FDIA are negligible. After the simulated FDIA ends the Pressure PLC restores the pressure by increasing the rate of the water droplets spray into the vapor region of the pressurizer. Simultaneously, the Water Level PLC adjusts the charging rate into the primary loop to bring the water level in the pressure to its nominal value shortly afterwards. During the simulated startup with a FDIA, the responses of the other emulated PLCs in the I&C systems of the PWR plant kept other state variables close to their nominal values during the simulated startup without a FDIA (Figs. 4.3-4.7).

4.4. Simulated Startup with an FDIA Targeting Core Protection Calculator PLC

While previous subsections presented results of a simulated cyberattack on the PLCs in the Plant Operation I&C system, the work in this section presents results of a simulated FDIA targeting one for the Core Protection Calculators (CPCs) PLCs in the representative PWR plant's PMS I&C system. The Matlab Simulink PWR plant model used to simulate the same reactor startup scenario as in 4.2 and 4.3 with the emulated PLCs in the Plant Operation I&C system controlling the plant's semiautonomous control functions. The emulated CPCs (Fig. 3.9) monitor the state variables determined by the Simulink plant model and communicated to the PLC's input registers by the LOBO NCS data broker and communication program (Fig. 3.3). The values of state variables and calculated parameters, such as the CHFR value for the identified hot channels, compared against the CPC's programed setpoints to determine whether the PLC will send voting signals to trip the reactor (Fig. 3.9). The PLC configured with an input scan time of 50 ms (Hahn, El-Genk, Schriener 2020).

The investigated cybersecurity event has the ManiPIO program writing a false high value for the reactor exit temperature value to the PLC's corresponding Modbus input holding register to manipulate the CPC to determine that the plant condition exceeds its safety setpoints and vote to trip. As the startup sequence progresses the reactor power and core exit and bulk average temperatures increase in increments as the external reactivity increased (Fig. 4.8a-c). The calculated value of the CHFR in turn decreases with the increases in the coolant temperature (Fig. 4.9a). The minimum calculated CHFR decreases to 6.56 in the identified hot channel (Fig.

4.9a) when the plant reaches 50% of nominal full power (point 5 on Figs. 4.8-4.9).

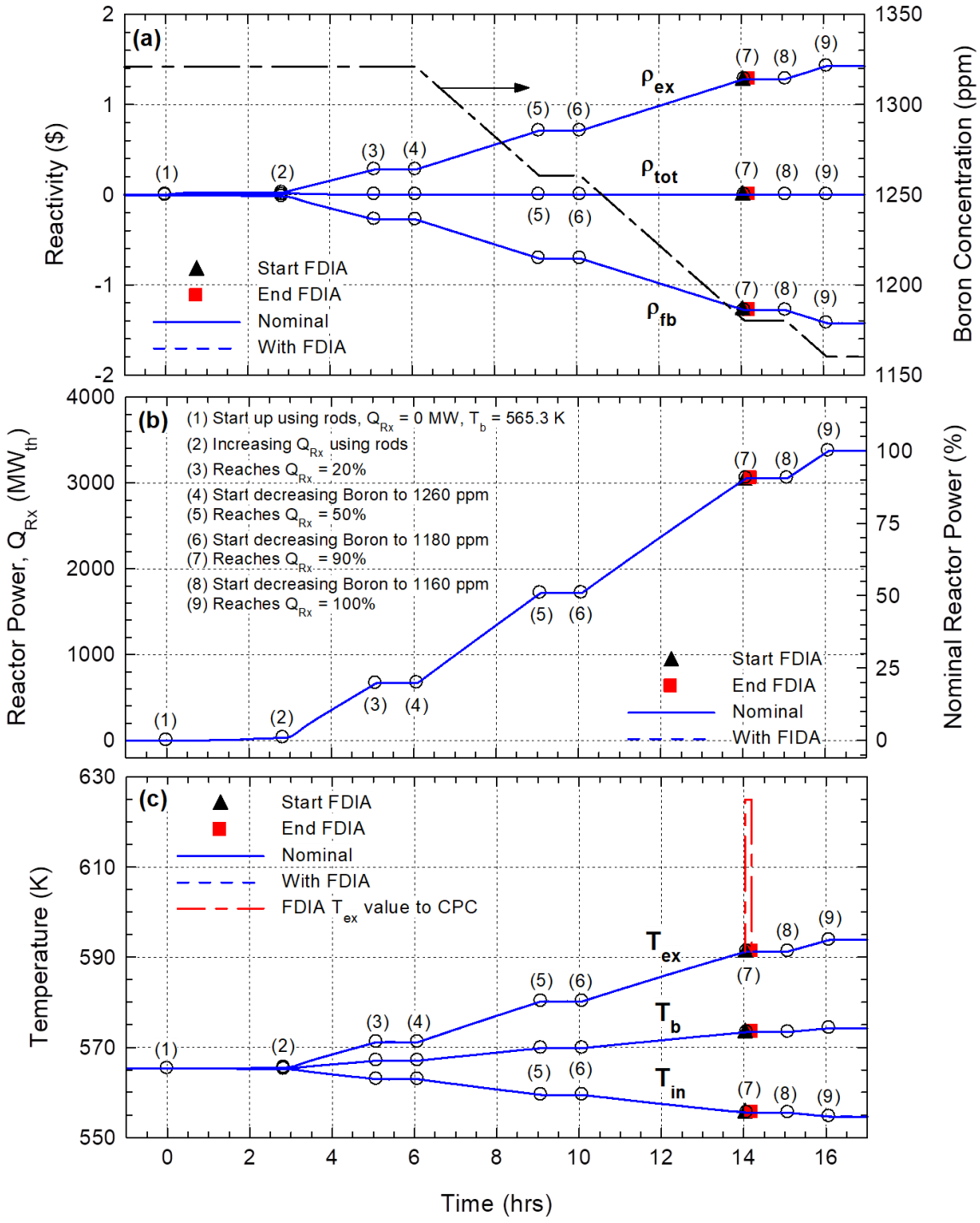


Fig. 4.8. Calculated state variables of a representative PWR plant using the primary loop Simulink model linked to the pressurizer Water Level PLC during a simulated startup without and with an FDIA targeting one of the four Core Protection Calculator PLCs (El-Genk and Schriener 2022).

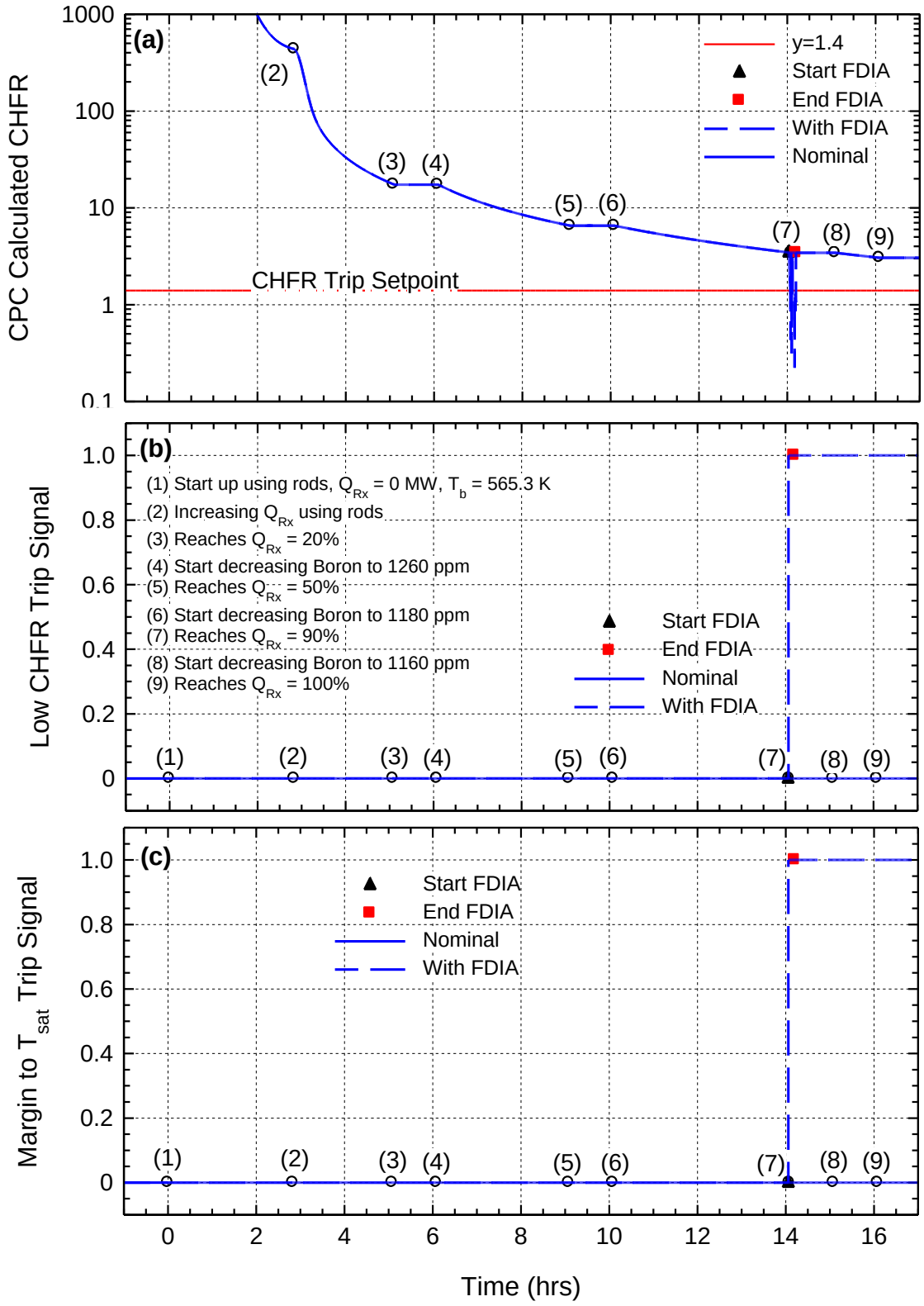


Fig. 4.9. Calculated CHFR and trip voting signals for emulated Core Protection Calculator during simulated startup without and with an FDIA targeting the PLC (El-Genk and Schriener 2022).

When the reactor power levels off at 90% of nominal power (point 7 in Figs. 4.8-4.9) the FDIA is initiated and the ManiPIO program sends a false high value of T_{ex} of 625 K to the input holding register of emulated PLC (Fig. 4.8c). The false value is written repeatedly for a period of 10 min. before the cyberattack ceases. The rate at which the ManiPIO code sends the overwrite requests is set to run as fast as the code can loop through its subroutines.

When the reactor power levels off at 90% of nominal power the calculated value of the CHFR decreases to 3.46. At this step in the representative reactor startup sequence the reactor exit temperature reaches a values of T_{ex} = 591 K. This temperature is 34 K below the false value of 625 K written to the PLC by the FDIA. The higher value of T_{ex} results in the PLC calculating a value of the CHFR as low as 0.22. This low value is well below the trip setpoint value of 1.4 (Fig. 4.9a). During the period FDIA is active, the Modbus holding register on the emulated PLC is successfully overwritten 99.92% of the time. However, as seen in the FDIA in Section 4.3, there are instances when the ManiPIO program is unable to successfully overwrite the holding register for the reactor outlet temperature. When this occurs, the CPC PLC calculates the true CHFR value of 3.46 (Fig. 4.9a). Once the FDIA successfully again overwrites the register the CPC returns to calculating the false low CHFR value.

When the calculated value of the CHFR decreases to ≤ 1.4 the PLC's logic program sends an affirmative reactor trip voting signal for its CHFR Trip function (Figs. 4.9a-b). This indicated by the Boolean logic value for the trip voting function changing from a value of 0 (vote not to trip) to a value of 1 (vote to trip) (Fig. 4.9b). Once the PLC votes to trip, it programmed to continue to vote affirmatively even if the calculated value of the CHFR drops below the setpoint. This results in the trip signal remaining positive throughout the remainder of the startup simulation even after the FDIA ceases and the calculated value of the CHFR returns to the un-manipulated value. The false high value of the reactor exit temperature written to the PLC's Modbus input holding register also results in the PLC sending an affirmative reactor trip voting signal for its Margin to T_{sat} Trip Function (Figs. 3.9, 4.9c). The false high value of T_{ex} of 625 K is above the saturation temperature of 618 K at the system pressure, resulting in a negative margin calculated by the CPC. This causes the logic program on the PLC to switch the value for the trip voting function from 0 (vote not to trip) to 1 (vote to trip) to indicate an affirmative vote to trip the reactor. As with the CHFR Trip Function this trip signal correctly remains positive once the PLC makes the initial vote to trip.

As the effected emulated PLC is one of four independent voting CPC PLCs in the PMS, the affirmative reactor trip voting signal is unable to force a reactor trip as a single positive vote does not satisfy the 2/4 voting coincidence required to trip the reactor. As a result, the representative PWR plant model continues to progress through the programmed startup scenario uninterrupted by the CPC PLC affected by the FDIA. Forcing a reactor trip would have required the simulated cyberattack to affect at least two of the four CPCs operating on separate fieldbus networks. In this scenario the separation between these networks thus prevents an unintended reactor shutdown.

4.5. Summary

The results presented and discussed in this section demonstrate the capabilities of the LOBO NCS platform to conduct cybersecurity investigations of a representative PWR plant. Presented are three different simulated FDIAs on the emulated PLCs during simulated operation transients. In the first scenario, the ManiPIO program simulated a FDIA targeting the input holding register of the Feedwater PLC and succeeded in writing a false value of the water level to the PLC and

manipulating its control logic to function as if the water level is constant despite the increase in the steam load demand. This resulted in a rapid decline in the water level inside the SG, eventually reaching the trigger setpoint for the emergency Auxiliary Feedwater Actuation System to actuate.

The LOBO NCS platform links the integrated Simulink models of a representative PWR plant and the emulated PLCs of the I&C systems to simulate a reactor startup scenario. The simulation begins from a hot zero power critical condition continues until reaching nominal full operating reactor power of 3,373 MW_{th}. The platform used for a series of cybersecurity investigations simulating FDIAs on PLCs within the plant's I&C systems. The first simulated FDIA targets the Pressure PLC in the Operation I&C system during the startup sequence. The FDIA repeatedly overwrote a false low system pressure to the PLC's holding register. The simulated FDIA initially caused a rapid increase in the system pressure by manipulating the Pressure PLC to increase the power to the submerged proportional heaters and turn on the submerged backup heaters in the pressurizer. The second simulated FDIA targets one of the CPC PLCs to repeatedly overwrite a false high core exit temperature to manipulate the PLC to vote to trip the reactor.

During the simulated FDIAs, the ManiPIO program repeatedly overwrites the targeted input register to attempt to force the PLC to either falsely maintain the proportional heaters at their maximum power and to turn on the backup heaters in the case of the Pressure PLC or vote to trip the reactor in the case with the CPC PLC. At the same time, the LOBO NCS data broker and communication program is competing to write the actual state variable value to the same Modbus holding register. At few instances during the attack, the PLC manages to receive the real state variable value despite the attempts by the ManiPIO program to overwrite it. This race condition determines the last write request accepted prior to the PLCs reading the stored register values at the beginning of their scan cycle. The communication program sends the new state variable values received from the pressurizer Simulink model once every 50 ms. In contrast, the determined time between Modbus write requests by the ManiPIO program averages 1.10 ms.

These two cycles not synchronized, so despite the ManiPIO FDIA overwrites having a faster frequency, a small percentage of the time the data broker still broke through and was able to overwrite the Modbus holding register on the emulated PLC before it ran its scan cycle. During these incidences, the PLC attempts to return to its normal operation before the FDIA once again rewrites the register and it returns to the manipulated state. For the FDIA targeting the Pressure PLC these failed overwrites resulted in the increase in the system pressure reduced during the transient. The FDIA targeting the CPC PLC resulted in a few instances when the PLC calculated the true value of the CHFR but did not otherwise affect the simulated cybersecurity event.

The next section demonstrates the capability of the LOBO NCS platform linking emulated PLCs to a physics-based Simulink model of an integrated space reactor power system with CBC energy conversion for the avoidance of single point failures. This arrangement used to investigate the system operation during a simulated startup scenarios nominally and when the PLCs are subjected to a simulated FDIA.

5. AUTONOMOUS REMOTE CONTROL AND CYBERSECURITY INVESTIGATIONS OF SPACE REACTOR POWER SYSTEMS

This section uses the versatile LOBO NCS Platform to perform I&C and cybersecurity investigation of a space nuclear reactor power system (El-Genk 2008; El-Genk, Tournier, Gallo 2010). Such reactor power systems would enable future space exploration throughout the Solar System and for missions requiring 10's to 1000's of kW_e and where the solar power option is impractical or unavailable. These space power systems are compact and could operate continuously for periods of 10–15 years, or even longer (El-Genk 2008). These power systems could also be designed for intermittent operation with multiple startups and shutdowns, although such operation can be challenging and depends on the reactor design and the type of the working fluid. In addition to providing surface power to future human outposts on the Moon and Mars, the generated electrical power could drive high specific impulse (5,000–15,000 s) plasma thrusters for fast travel to distant planets in the Solar System (Fig. 5.1).

For space reactor power systems operating at destinations far from Earth, it takes long times to communicate with ground control by human operators. Even at the speed of light, one way communication from Earth could take many minutes resulting in lengthy delays in communication and signals' transmission. This makes direct ground control impractical. In addition, radio communication between an Earth control center and the power system could easily be interfered with and presents a potential cyberattack vulnerability. Nuclear reactor power systems with intelligent I&C systems for fault detection and autonomous control could employ digital twins to support autonomous operation and control and ensure safe and reliable operation.

5.1. Digital Twin Concept

The concept of using digital twins to ensure reliable autonomous operation and control of nuclear reactors investigated in reference-model adaptive control concepts and successfully applied to space nuclear reactor power systems (Metzger, El-Genk, Parlos 1991). The effectiveness of reference model adaptive control demonstrated successfully for the SP-100 space reactor power system developed in the US in the eighties and early nineties (Marriott and Fujita 1994; Metzger and El-Genk 1992). This power system designed to generate 105 kW_e for 7-10 years to support a host of space and planetary exploration missions

A digital twin is a physics-based model that accurately simulates the transient and steady operation of the integrated nuclear reactor power system and components. The fidelity of the physics-based models of the various components of the integrated power system validated using a combination of actual measurements and detailed simulation analysis results. The actual values of state variables for the nuclear power system are compared in real time to those predicted by the digital twin. This helps identify any changes in the parameters of the power system or malfunctions of components. Digital twins could also aid in diagnosing potential causes for the observed change and recommend actions to continue operation without compromising long-term safety and operation of the power system (Metzger, El-Genk, and Parlos 1991; Lin, et al. 2021).

Redundant measurements of the actual system state variables such as temperatures, flow rate, pressure, and reactor control and thermal power are highly recommended to avoid false positive errors in the diagnosis. Digital twins developed to identify the optimum number, kind, and locations of the sensors measuring state variables for the PLCs in the I&C systems. They could also be used to detect and predict potential malfunctions of sensors or components (Metzger, El-Genk, Parlos 1991; Lin, et al. 2021; Sabharwall, et al. 2021). Transient simulations using a

digital twin of the actual power system could be used to predict and differentiate potential malfunctions by comparing the observed sensor measurements to those predicted for different scenarios. Digital twins capable of running many times faster than real time are suited for evaluating the effects of different control actions on the values of the operation parameters and on future performance and safety of the power system. These capabilities are essential for autonomous and remote control of both terrestrial and space nuclear reactor power systems. The PLCs in the I&C system in conjunction with Artificial Intelligence (AI) and Machine Learning (ML) capabilities (Sabharwall, et al. 2021) would identify corrective actions needed to avoid compromising the safety or long-term operation of the power system.

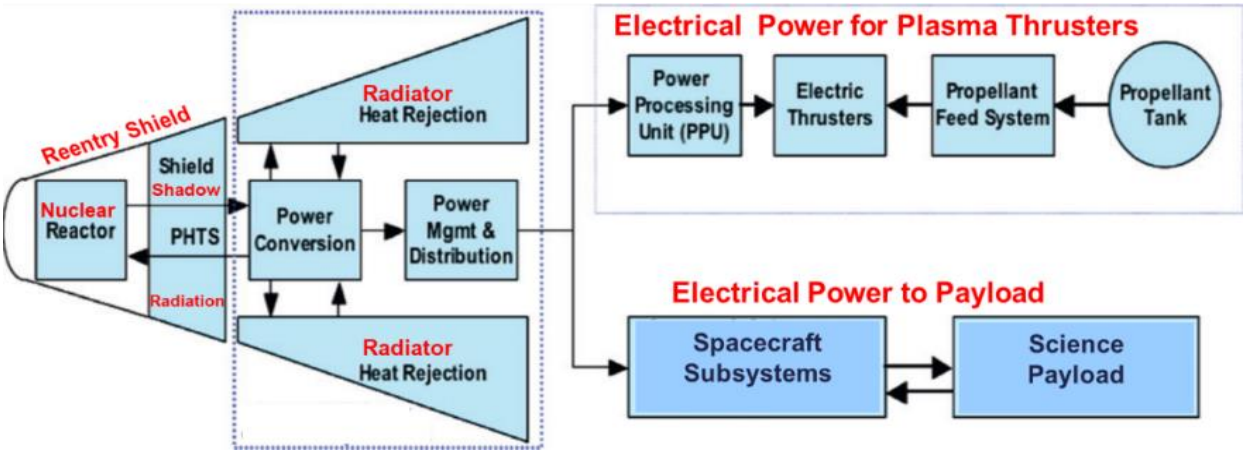


Fig. 5.1. A generic space nuclear reactor power system for electric thrusters and for science payload (PHTS: primary heat transport system).

To demonstrate the utility of the digital twin concept for cybersecurity investigations of space nuclear reactor power system, a dynamic model of power system design developed at UNM-ISNPS (El-Genk, Tournier, Gallo 2010) incorporated into the LOBO NCS platform (El-Genk, et al. 2021). The power system in the present cybersecurity investigations comprises a gas cooled nuclear reactor with sectored core to avoid single point failures in cooling and energy conversion. The three core sectors are neutronically and thermally coupled, but hydraulically separate. Each sector has its own CBC loop and turbomachine unit for energy conversion and water heat pipes radiator panels for waste heat rejection into space. The single-shaft UNM-BRU-1 turbomachine units have been designed and analyzed at UNM-ISNPS (Gallo and El-Genk, 2009). The digital twin dynamic model of the integrated space reactor power system, named DynMo-CBC, has been developed using the Matlab Simulink package (El-Genk, et al., 2010).

The following subsections describe the components of this space reactor power system and the DynMo-CBC model. They also describe the integration of the DynMo-CBC model into the LOBO NCS platform with emulated PLCs to simulate the nominal operation of the power system. The implemented DynMo-CBC model into the LOBO NCS platform is employed to investigate the response of the power system and the emulated PLCs to a simulated cyberattack aiming to disrupt the startup of the reactor and the power system.

5.2. Description of CBC Space Reactor Power System

The space nuclear power system investigated in this chapter includes the Submersion-Subcritical Safe Space (S^4) gas cooled reactor with sectored core (King and El-Genk 2007) and

three recuperated CBC energy conversion loops, each with multiple heat rejection radiator panels with water heat pipes (El-Genk, Tournier, Gallo 2010). The reactor coolant and working fluid for the CBC loops and the turbomachines is a He-Xe binary gas mixture with a molecular weight of 40 g/mole (El-Genk and Tournier 2007). This high molecular weight working fluid has the same convective heat transfer coefficient as that of pure helium (4 g/mole) and the same molecular weight as pure argon (40 g/mole). This noble He-Xe gas mixture reduces the heat transfer surface area in the recuperator. It also increases the aerodynamic loading of the blades of the turbine and compressor and effectively reduces the size and mass of the CBC turbomachines (Gallo and El-Genk 2009; El-Genk and Tournier 2007). The reactor core sectors are thermally and neutronically coupled, but hydraulically independent and separated by metallic dividers (King and El-Genk 2009). Each core sector (Fig. 5.2a) is coupled a separate CBC loop with UNM-BRU-1 unit (Fig. 5.3) (Gallo and El-Genk 2009; El-Genk, Tournier, Gallo 2010).

Figure 5.2 presents radial cross-sectional views of the S^4 reactor core and of a fuel stack-coolant channels unit cell (El-Genk, Tournier, Gallo 2010). The S^4 reactor has a monolithic Mo-14%Re alloy (molybdenum with 14 wt% rhenium) hexagonal core structure containing cylindrical cavities loaded with uranium nitride (UN) fuel pellets and surrounded by He–Xe coolant channels (Figs. 5.2a and 5.2b). There are a total of 217 UN fuel stacks and 1,977 coolant channels in the reactor core. Each fuel stack with 95 wt% enriched UN cooled by 9 channels (Figs. 5.2a and 5.2b).

The UN fuel stacks are wrapped in Iridium foils (0.1 mm thick) to enhance heat conduction to the solid core block. These foils also suppress the diffusion of solid fission products from the fuel pellets to the core block. The UN fuel pellets include 1.95 wt% ^{151}EuN additive to ensure that the bare core of the S^4 reactor remains sufficiently subcritical when submerged in wet sand and flooded with seawater following an unlikely launch abort accident (King and El-Genk 2009). The ^{151}Eu neutron poison minimally affects reactivity in the fast neutron energy spectrum S^4 reactor during nominal operation. However, this isotope effectively absorbs the thermal and epithermal neutrons in the submerged and flooded reactor core during a postulated launch abort accident, thus keeping the reactor core safely subcritical (King and El-Genk 2009).

The neutrons emanating from the reactor core during nominal operation are reflected radially and axially inward using beryllium oxide (BeO) clad in thin MA-ODS-956 steel (King and El-Genk 2009). The reactor operation is controlled using six rotating B_4C/BeO drums placed within the BeO radial reflector (Fig. 5.2a). Each drum is faced by a thin, 120° neutron absorber segment of B_4C that is fully enriched in ^{10}B. The reactor is sufficiently subcritical when the B_4C segments in the control drums are inward facing the core ($\theta = 0°$) (Fig. 5.2a). During reactor startup, the B_4C segments in the control drums are slowly rotated outward from the core to insert reactivity and bring the reactor to critical operation. During the life of the reactor the control drums continue to rotate outward to maintain criticality and compensate for the fuel burnup and the accumulation of fission products in the UN fuel. At end of life, the B_4C segments in the rotating control drums face 180° away for the reactor core.

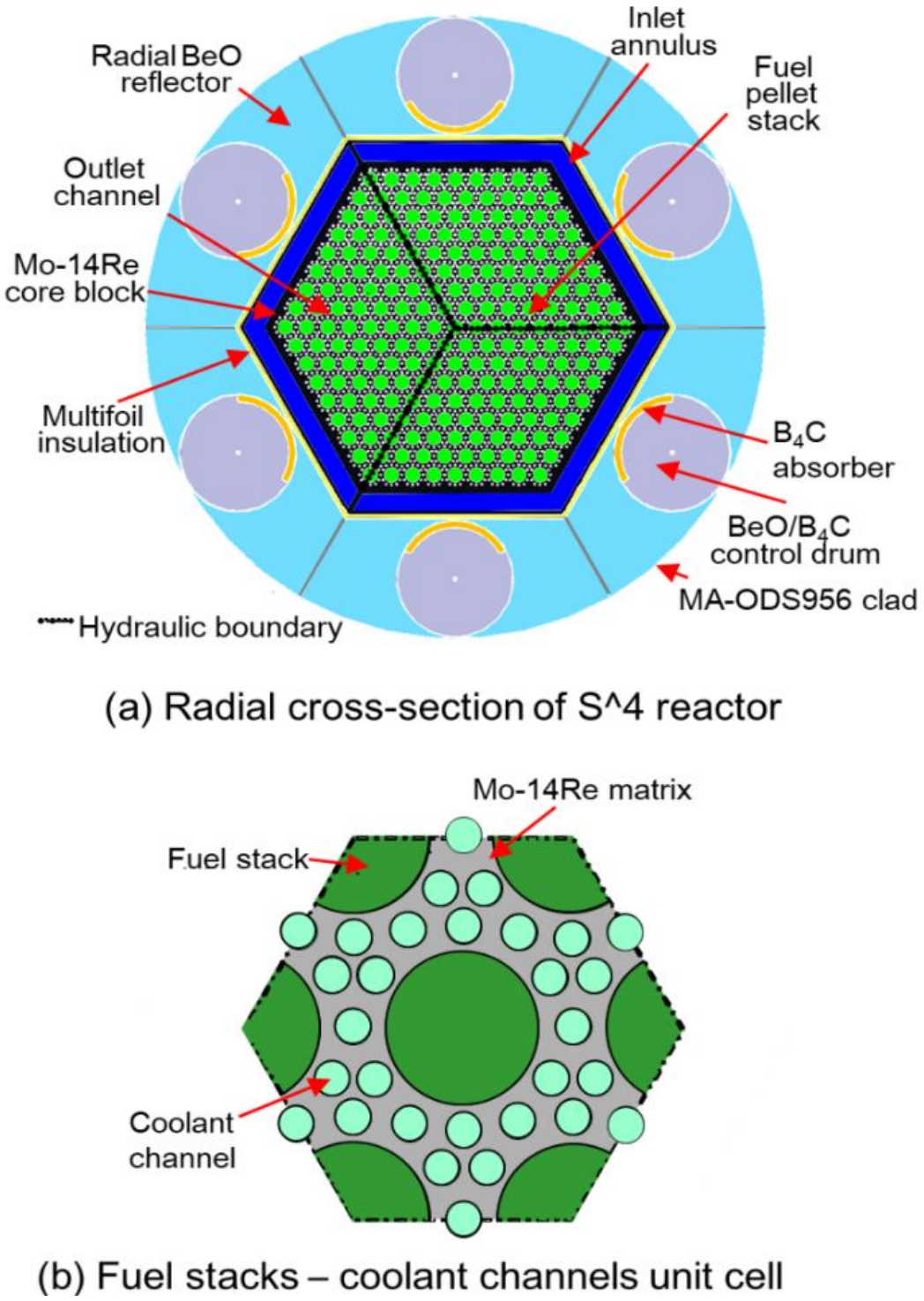


Fig. 5.2. Radial cross views of the S^4 reactor core and fuel stacks – coolant channels unit cell (El-Genk, Tournier, Gallo 2010).

Figure 5.3 presents a schematic diagram of the one of the CBC loops of the space reactor power system (El-Genk, Tournier, Gallo 2010). Each of the three UNM-BRU-1 CBC turbomachines has the centrifugal flow turbine and compressor mounted on the same shaft as a

Permanent Magnet Alternator (PMA) (Fig. 5.4) (Gallo and El-Genk 2009). The shaft employs gas foil bearings to virtually eliminate wear during operation. A bleed line diverts a small fraction of the working fluid exiting the compressor to cool the permanent magnets within the alternators of the CBC turbomachines (Figs. 5.3, 5.4). The bleed flow combines with that exiting the turbine before entering the recuperator. The PMA of the UNM-BRU-1 unit has an efficiency of 95%. The gas recuperator in the CBC loop recovers heat from the He-Xe flow exiting the turbine before returning to the compressor. The gas working fluid exiting the compressor returns to the reactor to be heated by the fission power generated in the designated sector of the reactor core to the design exit temperature of 1,149 K before entering the turbine of the CBC unit (Fig. 5.3).

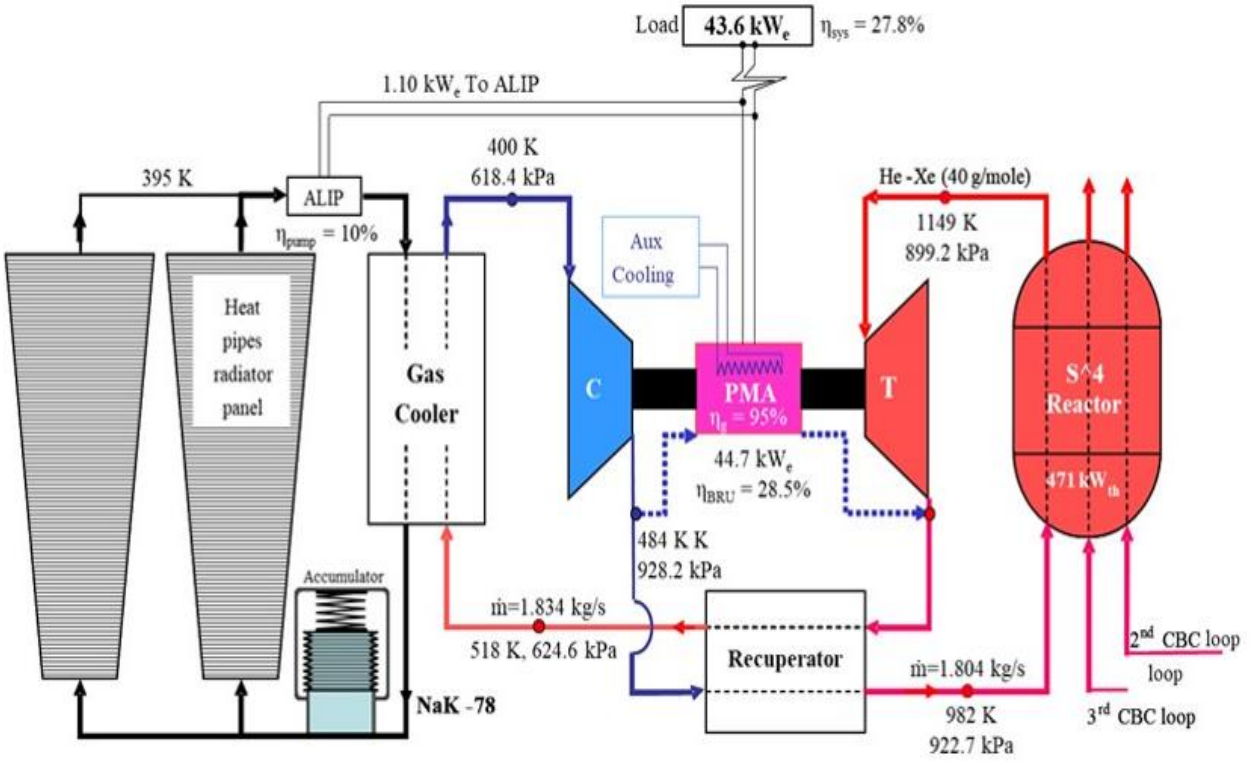


Fig. 5.3. A layout of the DynMo-CBC integrated space reactor power system (El-Genk, Tournier, Gallo 2010).

The CBC turbomachine design (Fig. 5.4) has been optimized for a peak thermal efficiency and electrical power of 28.5% and 44.7 kW_e, respectively. The peak efficiency is for operating at turbine and compressor inlet temperatures of 1,149 K and 400 K, respectively, shaft rotation speed of 45 krpm, and input thermal power to the turbine of 157 kW_{th} (Gallo and El-Genk 2009). This input power corresponds to a total reactor thermal power of 471 kW_{th}, divided equally among the three core sectors (King and El-Genk 2009; El-Genk, Tournier, Gallo 2010).

At this nominal power level, the S^4 CBC power system can operate continuously for up to 12.4 full power years, generating 134.1 kW_e of electrical power (Fig. 5.3). Fig. 5.5 is a schematic of the fully deployed CBC-space reactor power system. Waste heat from each of the three CBC loops removed by a circulating liquid NaK-78 secondary loop and rejected into space using two sets of water heat-pipes radiator panels (Figs. 5.3, 5.5). The He-Xe primary and the NaK-78 secondary loops are thermally coupled in a gas/liquid heat exchanger made of Mo-14%Re alloy.

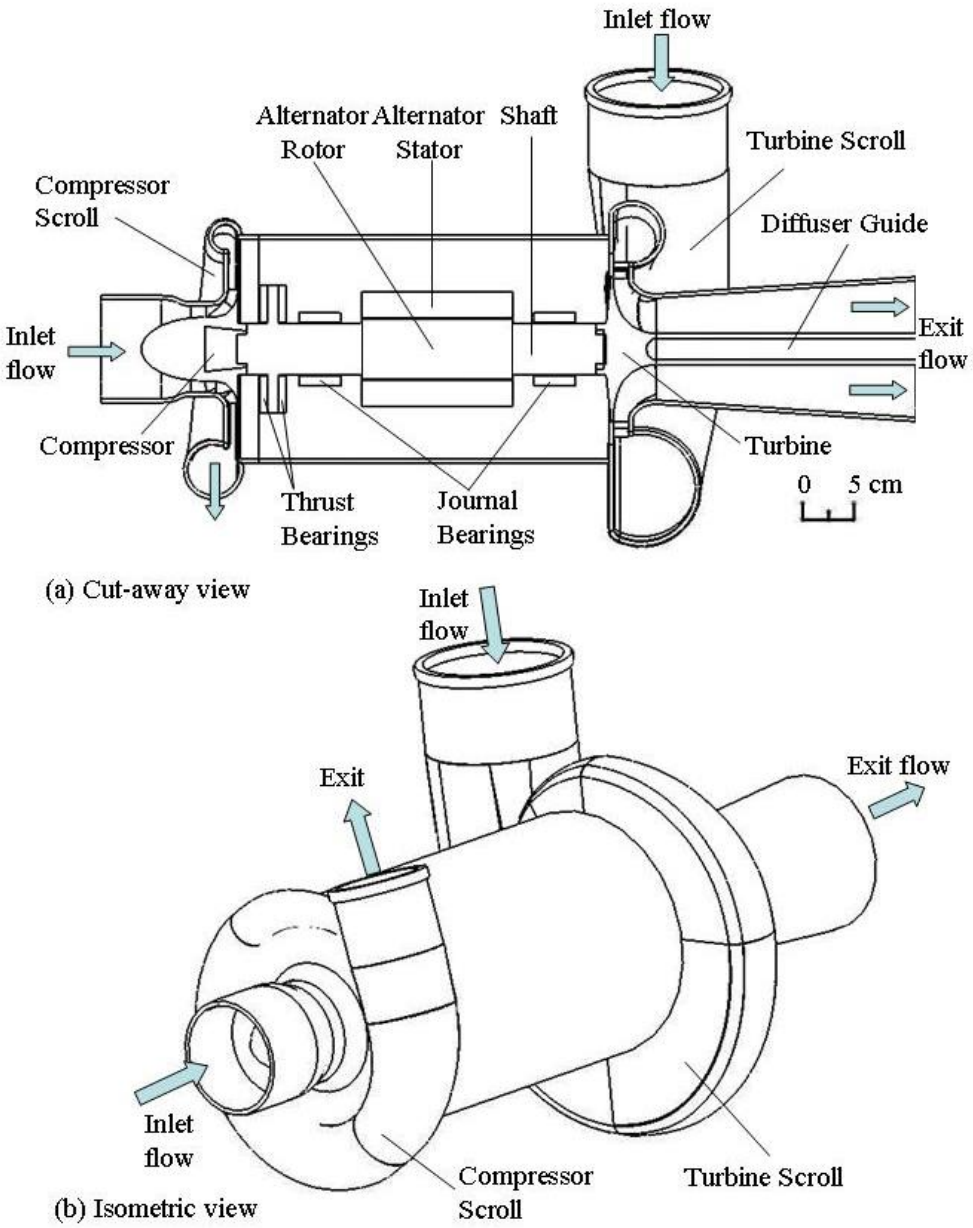


Fig. 5.4. Cutaway and isometric views of single-shaft UNM-BRU-1 unit (Gallo and El-Genk 2009).

Each heat rejection radiator panel consists of a forward fixed segment and two rear deployable segments hydraulically connected in parallel to reduce the pressure losses in the NaK-78 secondary loops, enhancing performance, and reducing the size of the radiator heat rejection panels. Bellows-type accumulators accommodate the volume changes and pressure of the NaK-78 coolant in the secondary loops of the heat rejection radiator panels (Tournier and El-Genk 2006). Annular Linear Induction Pumps (ALIPs) circulate NaK-78 in the three heat rejection loops (Fig. 5.3). Each ALIP consumes 1.1 kW_e of the power generated by the PMA in the CBC turbomachine, netting 43.6 kW_e to the electrical load, for a total system power of 130.8 kW_e (Fig. 5.5). The sectored S^4 CBC space reactor power system with multiple CBC loops avoids single point failures in reactor cooling, energy conversion, and heat rejection (El-Genk,

Tournier, Gallo 2010).

In the event of a loss of coolant in one of the three primary He-Xe CBC loops the reactor thermal power is reduced to avoid hot spots in the affected core sector and continue the space mission at a lower electric power output (King and El-Genk 2009). The fission heat generated in the affected reactor core sector transfers by conduction in the high thermal conductivity Mo-14%Re alloy solid core structure to the adjacent two sectors. The circulating He-Xe gas the fission heat generated in the remaining two functional CBC loops.

The developed Dynamic Model of the S^4 reactor and CBC space power system (DynMo-CBC) (El-Genk, Tournier, Gallo 2010) (Figs. 5.3) for simulating operation transients during startup and shutdown and following a change in the electrical load demand described in the next subsection. The DynMo-CBC model is incorporated into the LOBO NCS platform to investigate the performance of the power system during nominal transients and when under a cyberattack (see Subsection 5.4). The results of these investigations are presented and discussed in subsection 5.5.

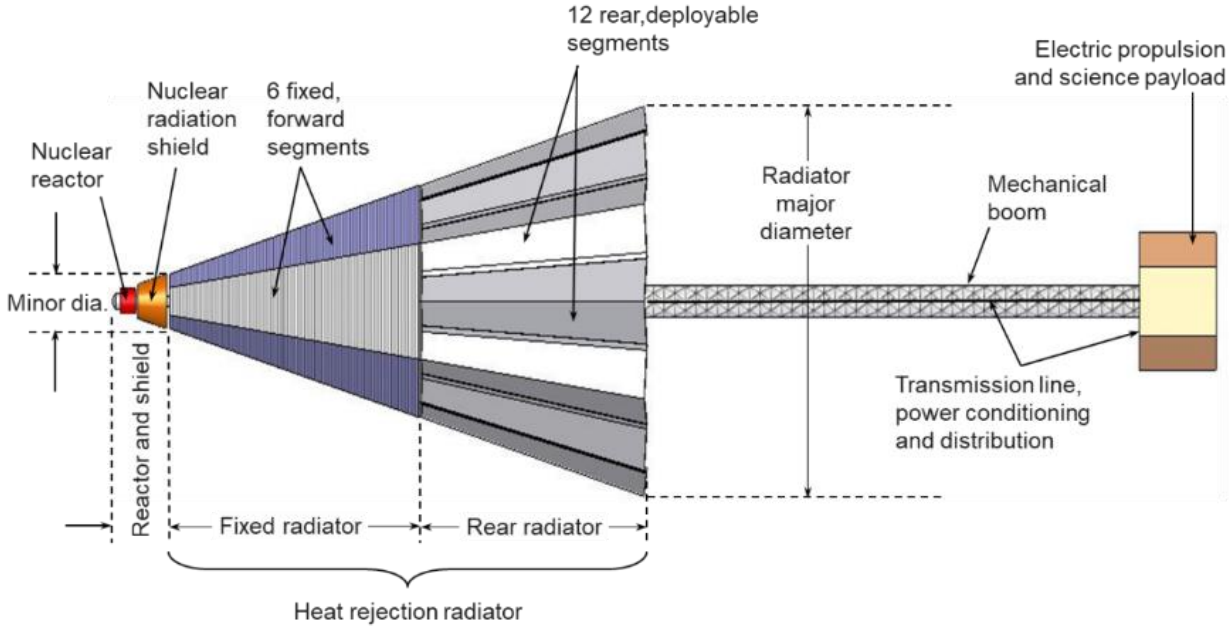


Fig. 5.5. A schematic of the fully deployed S^4 CBC space reactor power system (El-Genk, Tournier, Gallo 2010).

5.3. Dynamic Model of S^4 CBC Space Reactor Power System

The DynMo-CBC model of the S^4 reactor CBC space power system described in Subsection 5.2 uses the capabilities of the versatile Matlab Simulink package (El-Genk, Tournier, Gallo 2010). The differential equations describing the different processes in the integrated power system together with those for the various system components solved simultaneously using the ode23s Modified Rosenbock solver in Simulink with a variable timestep (The Mathworks 2020).

The DynMo-CBC Simulink model comprises coupled physics-based models of the different system components within the primary loops of the space nuclear power system (Fig. 5.3). These include coupled six-group point kinetics and thermal-hydraulics models of the S^4 reactor core, an integrated thermal-hydraulic model of one of the three CBC loops with Simulink models of the gas recuperator, and the UNM-BRU-1 turbomachine with transient models of the turbine and compressor. The secondary loops in the DynMo-CBC space nuclear power system are

represented by a simplified lumped model that satisfies the overall energy balance and accounts for radiative heat rejection

The six-group reactor kinetics model calculates the changes in the reactor thermal power in response to an external reactivity insertion at system startup using the rotating control drums placed in the BeO radial reflector (Fig. 5.2a) and accounts for the various temperature reactivity feedback effects in the core. These include the temperature reactivity feedback effects in the UN fuel, the monolithic Mo-14%Re solid core, and the He-Xe binary gas mixture flowing through the core coolant channels. The corresponding temperature reactivity feedback coefficients for the fast spectrum S^4 reactor calculated in 3-D Monte-Carlo neutron transport analysis performed using the MCNPX code (Pelowitz et al. 2009; El-Genk, Tournier, Gallo 2010).

The thermal-hydraulics model calculates the temperatures in the various parts of the core using a quasi-2D lumped parameter methodology. It also calculates the radial heat transfer from the fuel to the core structure, and then to the circulating gas coolant through the core of the S^4 reactor. This lumped model discretizes the core axially into multiple control volumes and solves the energy balance equations accounting for the axial temperature profile in an average fuel stack in the reactor core (Fig. 5.2b) to determine the average temperatures of UN fuel, Mo-14%Re core structure, and He-Xe coolant in the core.

The overall CBC loop model solves the coupled mass, momentum, and energy balance equations for the He-Xe reactor coolant and CBC loop working fluid. These equations are formulated for compressible flow and account for the effects of pressure and temperature on the properties of the He-Xe working fluid in the nuclear reactor and throughout the CBC loops (El-Genk and Tournier 2007). The CBC turbomachine submodel calculates the enthalpy losses in the turbine and compressor and the mechanical losses for the turbomachine shaft and assumes a PMA electrical efficiency of 95%. The shaft losses include the windage losses in the turbine and compressor wheels, the gas-foil bearings, the PMA, and the shaft surface. It also calculates the heat transfer to the bleed gas flow from the compressor outlet to cool the PMA (Fig. 5.3).

The turbine and compressor submodels include pre-calculated performance maps for determining the transient pressure ratios and polytropic efficiencies of the compressor and turbine as functions of the flow rate, inlet temperature and pressure of the He-Xe working fluid, and the shaft rotational speed. These performance maps were calculated using the detailed turbomachine simulation model used to design the UNM-BRU-1 CBC turbomachine (Gallo and El-Genk 2009). These maps allow the Simulink DynMo-CBC model to remain computationally lightweight and fast running without compromising the underlying physics. The turbomachine model also calculates the surge margin for the compressor to ensure sufficient safe margin during simulated transients.

5.4. DynMo-CBC Model and Emulated PLCs

The DynMo-CBC model is integrated into the LOBO NCS platform to conduct cybersecurity analysis of the coupled reactor power system (Fig. 5.6) with emulated PLCs in the digital I&C (Fig. 5.6). The DynMo-CBC in the LOBO NCS platform demonstrates the ability to integrate pre-existing Simulink plant models with emulated PLCs within the platform. A digital I&C system with two emulated PLCs developed for the control of the S^4 reactor and the operation of the CBC power system (Fig. 5.6). One PLC controls the rotation of the six drums in the radial reflector (Fig. 5.1). The Drums PLC calculates and sends the desired rotation rate to the drive motors of the drums. This PLC is programed to follow a specified startup sequence for the reactor. At the designated startup time of the reactor, this PLC rotates the control drums outward

at a constant rate until the rotation angle reaches the setpoint position for nominal full power operation. If the rotation angle of the drums exceeds this setpoint value, the PLC will rotate back the drums inward at a constant speed to the desired angle.

The shaft rotation speed in the CBC turbomachine units is controlled by the CBC Speed PLC. During the reactor startup, the shaft rotation is maintained by operating the PMAs as a driving motor. During this phase, the net shaft power is negative and the motor supplies power to maintain the shaft speed at the programmed setpoints. Once the shaft becomes zero, meaning the turbine and compressor powers are equal, the operation of PMAs is reversed to operate in the power generation mode. In this mode, the shaft rotation is controlled by an analog PID controller using a parasitic load resistance (Word, Fischer, Ingle 1967).

This parasitic load resistance, shaft control scheme has been investigated for space CBC turbomachines and can achieve extremely fast responses (Wright, Lipinski, Vernon, Sanchez 2006; Word, Fischer, Ingle 1967). Terrestrial CBC systems commonly employ a scheme which controls the volume of working fluid in the CBC loops to regulate the turbomachine shaft speed. This method, however, requires bulky gas storage tanks not suitable for use in a space system (Word, Fischer, Ingle 1967). The load parasitic resistance is connected in parallel with the main spacecraft load (Fig. 5.6). During startup, the spacecraft load is disconnected, and the electrical power generated by the PMA is sent to a shunt resistance radiator for rejecting heat to space.

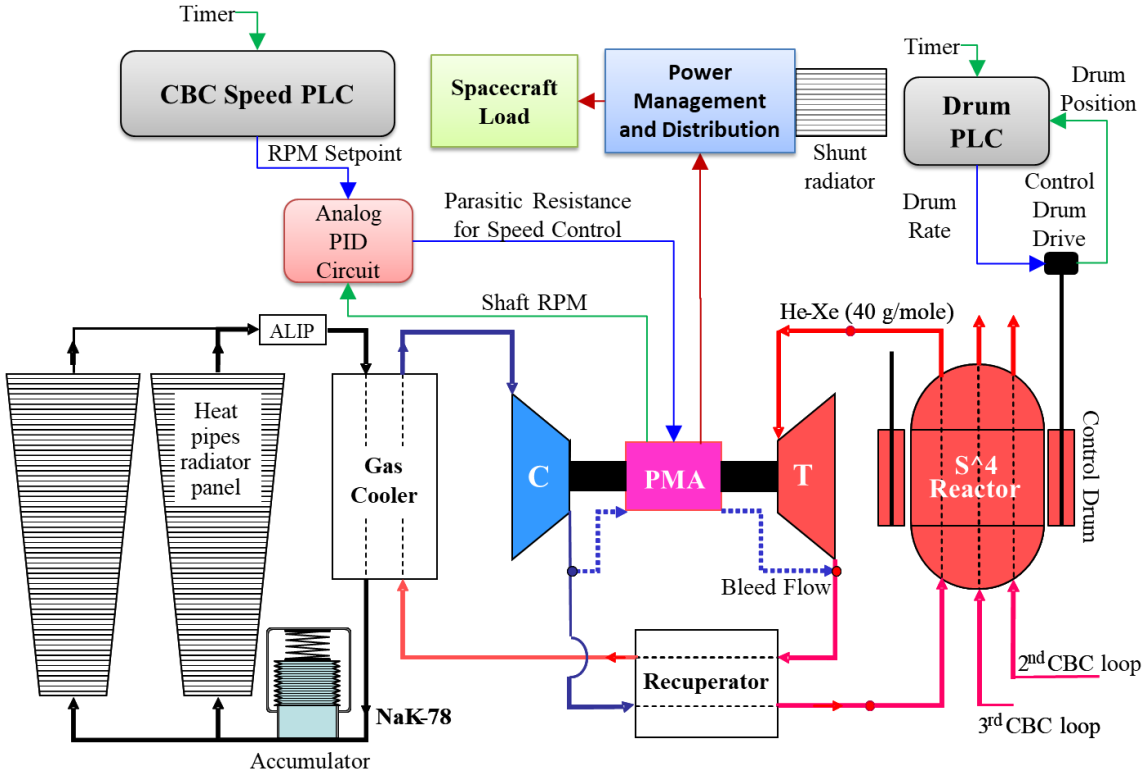


Fig. 5.6. A block diagram of the implemented DynMo-CBC space reactor power system model and emulated PLCs in the LOBO NCS platform.

The CBC Speed PLC determines the setpoint for the analog PID controller based on a programed startup sequence. When the shaft rotation speed of the CBC turbomachine units is below setpoint, the parasitic load resistance is reduced to increase the shaft speed. Conversely, when the shaft speed is higher than the setpoint, the PID controller increases the load resistance

which serves as a brake on the shaft and slows its rotation. During the simulated startup sequence the CBC Speed PLC is programed to ramp the shaft speed from an initial value of 22 krpm to the nominal steady state shaft rotation speed of 45 krpm. During nominal operation, this rotation speed is maintained at this setpoint by the PLC. When the reactor reaches full nominal thermal power, the spacecraft load is connected, and the power management and distribution unit of the power system send the electrical power generated by the turbomachines' PMAs to various load components.

The LOBO NCS data transfer interface links to the DynMo-CBC Simulink model using the developed S-function described in Subsection 3.2.1 (Hahn, Schreiner, El-Genk 2020). The S-function in Simulink sends the state variables calculated by the DynMo-CBC system model to the data transfer interface. These variables include the angular position of the rotating control drums in the BeO radial reflector of the S^4 reactor and the operation frequency of the PMA in the CBC turbomachine unit. The values of these variables then communicated to the emulated PLCs controlling the rotation angle of the control drums and the shaft rotation speed of the CBC unit (Fig. 5.6).

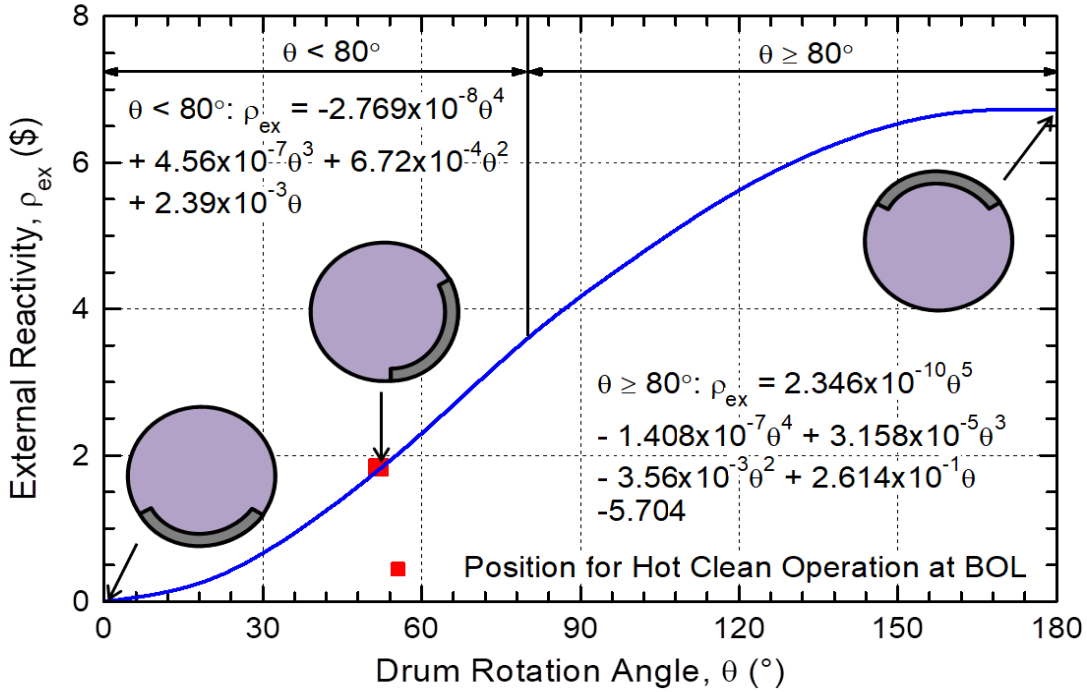


Fig. 5.7. Changes in BOL hot-clean external reactivity insertion, ρex, into the S^4 reactor core as a function of the rotation angle, θ, of the B4C/BeO rotating control drums in the BeO radial reflector (Hahn, Schriener, El-Genk 2020).

The values returned by the PLCs to the Simulink model adjust the operation of the simulated CBC space reactor power system to within preprogramed setpoints. The analog PID controller in the DynMo-CBC model adjusts the parasitic load resistance to control the shaft rotation speed commensurate with the setpoint received from the CBC Speed PLC. Some of the calculated state variables by the Simulink model of the S^4-CBC power system (Fig. 5.3) sent via the Simulink S-function to the LOBO NCS data broker to be recorded and used for monitoring purposes.

The rotation angle of the control drums is related to the magnitude of the external reactivity insertion into the S^4 reactor (Fig. 5.2). Fig. 5.7 presents the developed relationship of the

external reactivity insertion in the S^4 reactor as a function of the rotation angle of the control drums in the radial BeO reflector (Hahn, Schriener, El-Genk 2020). This relationship is determined using a least square fit of the obtained results using 3-D neutronics analyses of the S^4 reactor. The emulated PLCs in the I&C system of the DynMo-CBC space reactor power system use the OpenPLC software (Alves and Morris 2018) to implement the IEC 61131-3 standard structured text programming within Raspbian OS VMs (Fasano, et al. 2020). The VMs use the VMWare Pro software (VMWare 2019) running on a multiprocessor Windows 10 server. The OpenPLC control program configured with a PLC scan time of 5 ms.

The LOBO NCS data transfer interface program communicates the state variables and control signals to and from the OpenPLC software using the Modbus TCP communication protocol within the libmodbus library (Raimbault 2019). The server running the VMs for the PLCs connected to the server running the DynMo-CBC Simulink model and the LOBO NCS data transfer and broker program on an isolated Ethernet network using a managed switch. For cybersecurity investigations, the ManiPIO cyber event generation utility (El-Genk, et al. 2021) in the LOBO NCS platform simulates cybersecurity attacks on the emulated PLCs in the I&C system of the DynMo-CBC reactor power system.

The present digital I&C and cybersecurity testing platform would support design and testing efforts to develop control system architectures with advanced autonomous capabilities for the DynMo-CBC space reactor power system. The coupled Simulink model of the power system to the emulated PLCs can be used to evaluate the performance of the PLC's control programs for different operational transients and simulated equipment malfunctions. It supports conducting cybersecurity investigations of the integrated power system including the responses of the reactor and the CBC turbomachines to simulated cyberattacks targeting the controllers of the PLCs. The obtained results for the DynMo-CBC power system during a simulated startup transient without and with a simulated cyberattack presented and discussed next.

5.5. Applications to Cybersecurity Investigations

This subsection presents the obtained results of two startup simulations of the DynMo-CBC nuclear reactor power system with emulated PLCs in its digital I&C system, using the LOBO NCS platform. The first, described in Subsection 5.5.1, is of a nominal startup of the power system from a critical hot-clean condition until reaching full power steady state operation. The second simulation, described in Subsection 5.5.2, is also of a startup of the power system from a hot clean critical condition, but while the system is subjected to a simulated cyberattack. For this attack, the ManiPIO program simulates a FDIA that targets the PLC controlling the rotation of the control drums in the BeO radial reflector of the S^4 reactor (Fig. 5.2a, 5.6).

The FDIA overwrites the output holding register of the rotating control drums PLC to increase the rate of external reactivity insertion beyond nominal during the simulated startup transient. The higher rate of external reactivity insertion increases the reactor's thermal power and temperatures beyond those in the first, nominal simulated startup transient of the power system. The results of the two startup simulations are compared to demonstrate the impact of an FDIA on the power system operation and safety.

5.5.1 Nominal Startup of DynMo-CBC Power System without an FDIA

The sequence of events during the simulated nominal startup of the power system is indicated in Figs 5.8-5.10. The simulated startups begin from a hot-clean zero-power critical condition at an isothermal temperature of 400 K and with the driver motor for the CBC turbomachines

maintaining the shaft rotation speed at 22 krpm. For the hot-clean critical condition the control drums in the BeO radial reflector of the S^4 reactor rotated 15.95° outward. The reactor thermal power, Q_{rx}, is initially at 10 W and the radiator panels covered by an insulating blanket to inhibit heat dissipation from the power system. The simulated startup transient of the reactor power begins at t = 0 hr. (point 1 in Figs. 5.8-5.10) by rotating the control drums outward at a constant rate of 0.005°/s (Fig. 5.8a). This inserts reactivity into the core, increasing the reactor power and temperatures (Figs. 5.9a-c). After a time, t = 0.267 hrs. into the simulated startup transient (point 2) the CBC shaft rotation Speed PLC sends a command to the drive motor to start increasing the shaft rotational speed in the CBC units at a constant rate of 5.18 rpm/s (Fig. 5.8c).

Subsequently the reactor thermal power decreases because of the increased reactor temperatures (Fig. 5.9c) introduces a negative temperature reactivity feedback into the reactor core (Fig. 5.9a). Simultaneously, the temperature of the He-Xe working fluid at the exit of the compressor of the CBC units increases due to the increase in the compressor workload at the higher shaft rotation speed and the reactor thermal power (Fig. 5.10a). However, the rise in the temperature the He-Xe gas in the reactor is modest due to the energy recovery in the recuperator and the heat transfer losses from the piping to the surroundings (Fig. 5.9c).

At t = 0.5 hrs. into the simulated startup transients (point 3 in Figs. 5.8-5.10), the insulating blanket of the radiator panels is removed gradually within the following 60 s. Once the blanket is removed and jettisoned into space the heat rejection from the radiator panels decreases the temperatures of the He-Xe working fluid in the CBC loop. The drop in the reactor core temperature increases the reactor thermal power due the decrease in the negative temperature reactivity feedback (Figs. 5.9a-c). Subsequently, the reactor temperatures rise gradually with time until eventually the power system reaches nominal steady state operation after the end of the external reactivity insertion process (points 6 and 7 in Figs. 5.9c and 5.10a).

The calculated power produced by the turbine in the CBC unit and consumed by the compressor during the simulated startup transients shown in Fig. 5.10b. At point 4 during the simulated startups the turbine power in the CBC units exceeds that consumed by the compressor and that due to the losses. At this point the driving motors of the shafts in the CBC units are disconnected, and the PMAs are connected to the shunt radiator in the power management and distribution system (Fig. 5.6). The PMA generates increasing amount of electrical power, which is shunted and radiated into space, as the difference between the turbine and compressor powers increases (Figs. 5.10b-c). The shaft speed is now maintained by the PID controller by adjusting the parasitic load resistance. At t = 1.5 hrs. (point 5) the shaft speed reaches 45 krpm and is maintained by the PID controller of the CBC PLC during the startup sequence (Fig. 5.6).

The reactor thermal power and temperatures, and the electrical power to the load continue to increase smoothly as the external reactivity insertion continued. The increase in the load electrical power is because the power supplied by the turbine in the CBC turbomachine units increases faster than that consumed by the compressor (Figs. 5.8b, c). When the rotation angle of the control drum during the simulated startups reaches 61.05° the Drums PLC stops the outward rotation of the drums and hence the external reactivity insertion (point 6 in Figs. 5.6a-b).

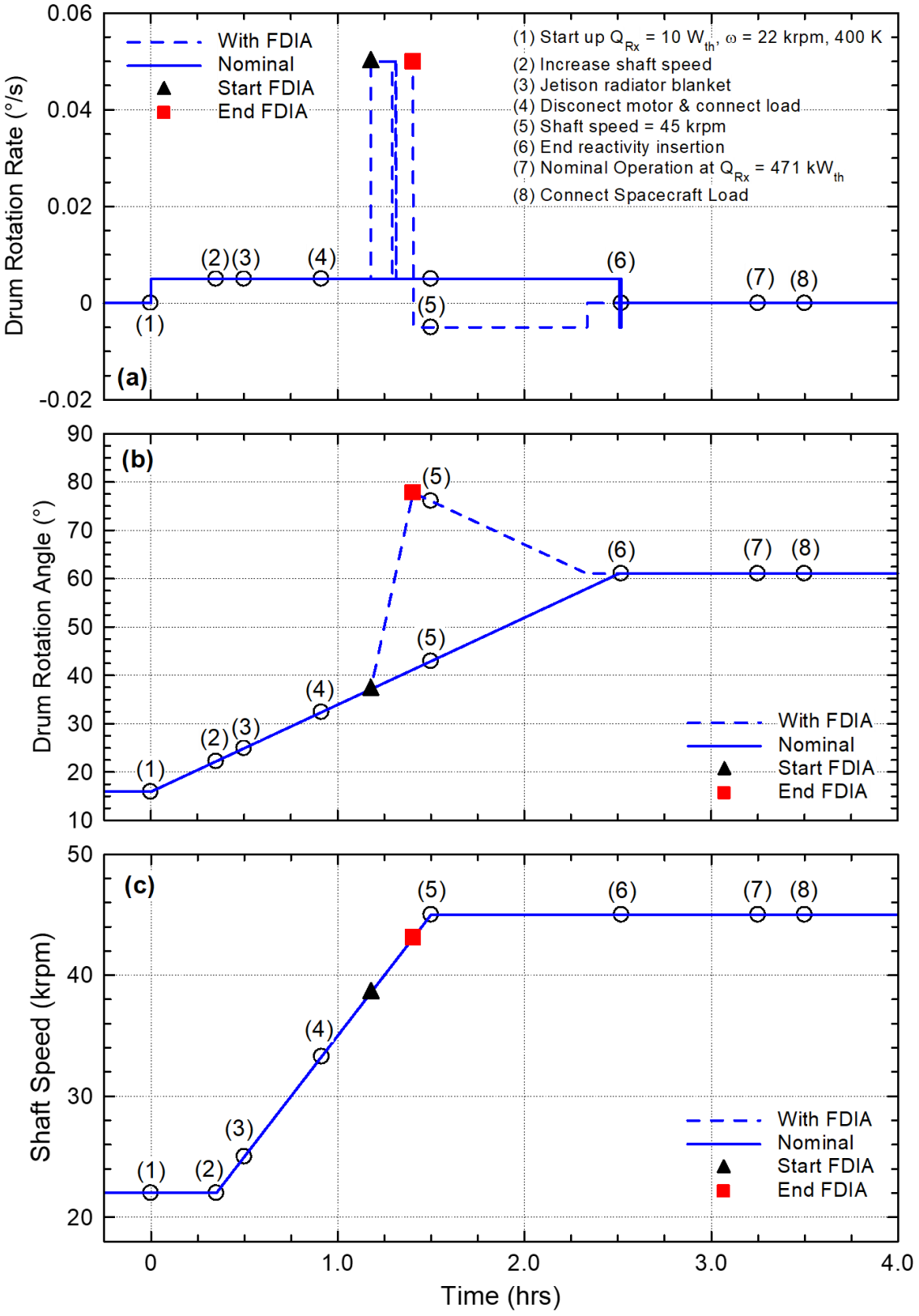


Fig. 5.8. Control variables of the DynMo-CBC space reactor power system during a simulated startup without and with a FDIA (El-Genk and Schriener 2022).

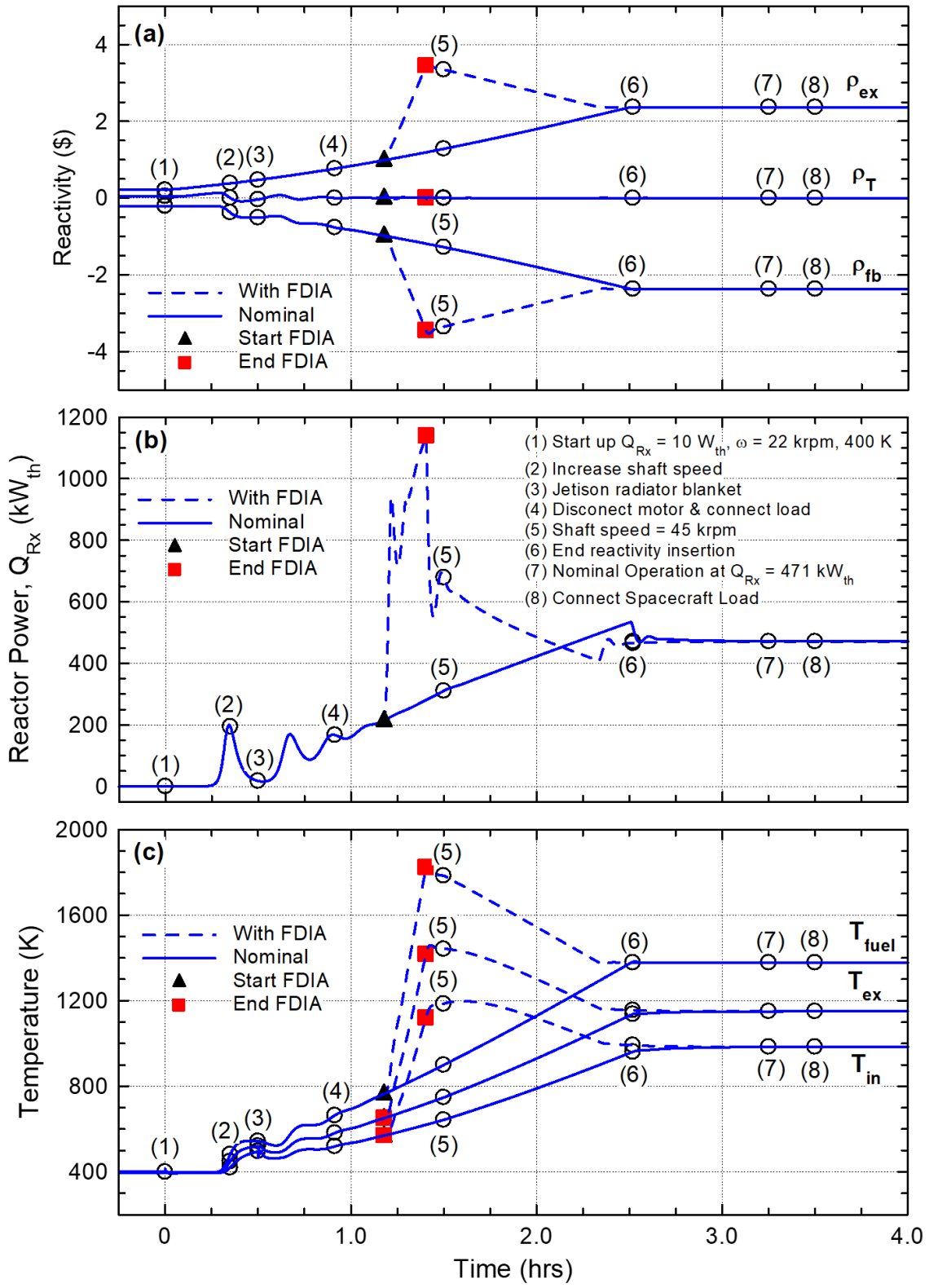


Fig. 5.9. Calculated S^4 reactor variables during the simulated startups without and with a FDIA (El-Genk and Schriener 2022).

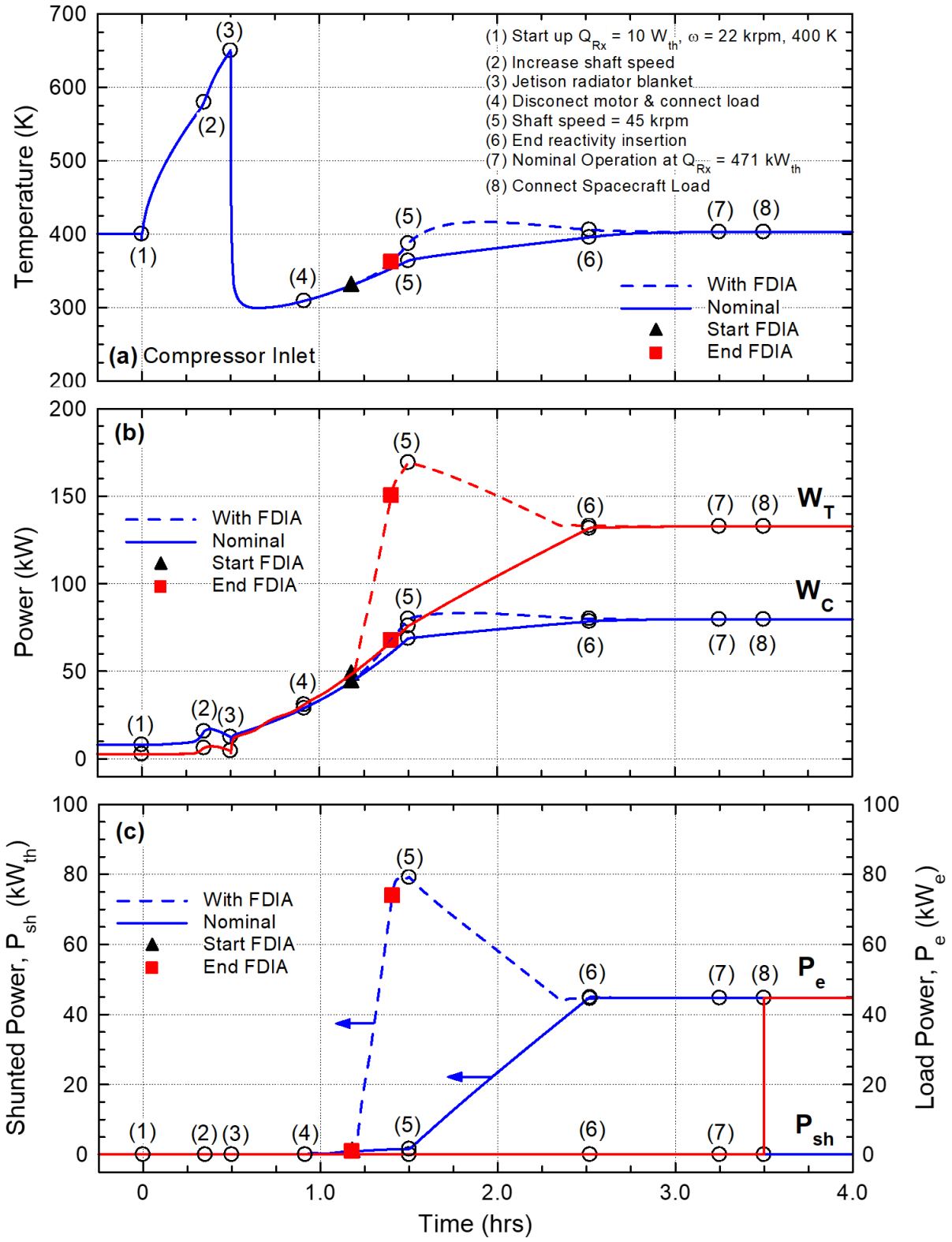


Fig. 5.10. CBC space nuclear power system state variables in the CBC loops during the system startup nominally and with a FDIA (El-Genk and Schriener 2022).

The feedback reactivity lags the external reactivity, so when the external reactivity insertion stops the negative reactivity feedback decreases reactor power approaching the nominal steady state value of 471 kW_{th} for the DynMo-CBC power system (point 7 in Figs. 5.8–5.10). At this point, the reactor core inlet and exit temperatures are 1,153 K and 985 K, respectively. At t = 3.5 hr. of the simulated startup, the spacecraft load is connected (point 8 in Figs. 5.8–5.10) with each of the three CBC turbomachine units in the power system supplying 43.6 kW_e (Figs. 5.3 and 5.10) to the load, for a total of 130.8 kW_e for the power system. Figs. 5.8–5.10 compare the results of the two simulated startup transients for nominal condition and when the Drum PLC subjected to an FDIA to speed the rotation rate of the control drums in the radial BeO reflector (Fig. 5.2). The obtained results of the latter discussed next.

5.5.2. Response to Simulated Cyberattack on Drum PLC

The simulated cyberattack during the startup transient of the DynMo-CBC space reactor power system (Fig. 5.2) attempts to disrupt the operation of the Drums PLC by subjecting it to a simulated FDIA. The FDIA increases the rotation rate of the control drums and hence the rate of external reactivity insertion into the reactor core beyond the nominal 0.005°/s. The ManiPIO FDIA generation program in the LOBO NCS platform (El-Genk, et al. 2021) writes a false high rotation speed of the control drums in the BeO radial reflector of 0.05°/s to the Modbus holding register for the drums PLC. This false value is ten times that during nominal startup without an FDIA (Figs. 5.8-5.10).

The faster drums rotation increases the rate of external reactivity insertion in the reactor core, causing large increases in the reactor power and temperatures and the coolant temperatures throughout the CBC loops. The simulated FDIA introduced after ~1.2 hrs. from the beginning of the startup transient (solid triangular symbol in Figs. 5.8- 5.10) and continues to overwrite the holding register of the drums PLC for 13.33 minutes (or 800 s) before ceasing (solid square symbol in Figs. 5.8- 5.10). The rotation angle of the drums to reach 77.79° at the end of the simulated FDIA (Fig. 5.8b). After the FDIA ceases, the Drum PLC returns to normal operation and guides the power system to resume normal startup.

During the applied FDIA the controller of the Drums PLC tries to return the position of the drums back to their nominal stopping position of 61.05°. As seen in the simulated scenario in Subsection 4.3, there are two instances of failure of the ManiPIO program to overwrite to the register in the OpenPLC program for the Drums PLC. In these instances, the register of the control Drums PLC attempts to rotate the drums inward at a rate of 0.005°/s to reduce their angle to nominal during the simulated startup scenario (Figs. 5.8a-b).

The high rotation rate and the large rotation angle of the control drums during the simulated startup with a FDIA applied increase the rate and the value of the external reactivity insertion, causing large increases in the reactor power, the temperatures in the reactor core and throughout the CBC loops, and the load electrical power (Fig. 5.9a). During the applied FDIA the reactor power peaks at 1,139 kW_{th}, compared to only 535 kW_{th} in the simulated nominal startup without a FDIA (Fig. 5.9b). In addition, the average temperature of the UN fuel in the reactor core peaks at 1,854 K, and the inlet and exit temperatures of the circulating He-Xe working fluid in the reactor core peak at 1,198 K and 1,460 K, respectively. The hot temperatures in the S^4 reactor and CBC loops could compromise the safety and reliability of the space power system should the FDIA continues for a sufficiently extended period.

Although calculated temperatures during the simulated FDIA are below the melting points of the UN fuel, the monolithic Mo-14%Re core structure and the piping in the CBC loops, the induced thermal stresses could be a concern. The calculated high average fuel temperature in the

reactor core during the simulated startup with a FDIA could increase the UN fuel swelling and mechanical interaction with the core structure. It is worth noting that the volumetric swelling of and the gas release from the UN fuel strongly dependent on temperature (Ross, El-Genk, Matthews 1990).

In the period when the simulated FDIA is active the increased reactor thermal power also increases the power supplied by the turbine and consumed by the compressor of the CBC turbomachines. The turbine power increases far more than the compressor power (Fig. 5.8b). This results in a substantial increase in the electric power supplied by the PMA of the CBC turbomachine unit, reaching a peak of 79.2 kW_e (Fig. 5.8c). In this scenario the power management and distribution system for the load needs to accommodate the increased electrical power during the simulated transient. In this transient, the PID controller of the CBC turbomachine manages to maintain the shaft rotation speed as in the nominal startup sequence without a FDIA (Fig. 5.8c).

When the FDIA ends, the Drums PLC returns to normal operation by slowly rotating the control drums in the radial BeO reflector of the S^4 reactor inward. This decreases the external reactivity and rapidly decreases the reactor power (Fig. 5.7a-b) and the temperatures of UN fuel and He-Xe working fluid commensurate with the reactor power. The reactor power and temperatures eventually reach their nominal steady state values when P_{Rx} = 471 kW_{th}. The simulation results show that following a FDIA the nuclear power system recovers to the same nominal values as at the end of the simulated startup without a FDIA.

5.6. Summary

The presented results demonstrate the capabilities of the LOBO NCS platform for simulating and investigating effects of cyberattacks on a space reactor power system. It also shows how pre-existing Matlab Simulink models of power systems can be integrated into the LOBO NCS platform with a minimum of modifications to couple the models with external emulated or physical hardware control systems. In addition to supporting cybersecurity analysis, the LOBO NCS platform can also support developing autonomous operation and control technology for terrestrial nuclear plants and space nuclear power systems. It can also aid in to optimizing the numbers and placement of the measurements sensor in the integrated power systems to promptly detect components malfunctions and identify their nature. The autonomous control system will then devise a course of action to mitigate undesirable long-term consequences on the system.

6. SUMMARY AND CONCLUSIONS

This final report details the efforts conducted at UNM-ISNPS in collaboration with SNL as part of the DOE NEUP to develop Nuclear Instrumentation and Control Simulation (NICSim) capabilities. The objective of this project is to develop platform to assess the resilience and cybersecurity risks of digital I&C systems in nuclear power plants. The uses of digital I&C systems in nuclear power plants raise concerns of potential cyber vulnerabilities that needs investigated. Currently, the regulators require all US commercial nuclear plants to develop and implement a cybersecurity protection plan for its essential I&C systems. PWR plants employ a combination of protective equipment and administrative controls to prevent unauthorized access to their secure systems. These protect against potential cyber-vulnerabilities of the I&C systems and consider the potential consequences of a successful cyber-compromise of a given component. Cybersecurity modeling and simulation tools are developed to help identify potential vulnerabilities of nuclear power plants' I&C systems architecture and inform security designers of needed protections.

UNM-ISNPS in collaboration with SNL have developed the LOBO NCS platform as part of the NICSim effort to provide a modular and versatile testing and simulation platform for cybersecurity investigations of digital I&C systems of commercial PWR plants. This platform incorporates physics-based dynamic models of a representative PWR plant primary loop, capable of running synchronous with real time and is compatible with the SCEPTRE framework developed by SNL. The LOBO NCS platform incorporates fast running and robust data transfer and communication interfaces and a GUI for displaying real time data of the calculated values of the state variables in the plant. It also incorporates the ManiPIO program which simulate a wide range of cybersecurity events on the emulated and physical PLCs and other devices within the I&C systems. The emulated PLCs in the LOBO NCS platform developed using open-source OpenPLC runtime that uses the Modbus TCP ICS communication protocol.

The results of a series of investigations using the LOBO NCS platform for a representative PWR plant model linked to the emulated PLCs in the operation I&C system demonstrated the functionality of the LOBO NCS and the PLCs in simulated transients. Presented results are for a series of cybersecurity investigations using the LOBO NCS platform linking emulated PLCs to the developed dynamic simulation models of a representative PWR plant and components and of a space nuclear reactor power system with multiple CBC loops. Results for scenarios for nominal operation transients are compared to those when one PLC subjected to a simulated FDIA.

The investigation of a representative PWR SG model coupled to an emulated Feedwater PLC simulated an operation transient following a 10% increase in stream demand. During nominal operation, the Feedwater PLC maintains the water level in the SG close to its preprogramed setpoint. A simulated FDIA using the ManiPIO program succeeded in manipulating this PLC to maintain a constant feedwater injection during the simulated transient. This caused a rapid decline in the SG water level until reaching the safety setpoint for starting the emergency Auxiliary Feedwater Actuation System.

The LOBO NCS platform linking the integrated dynamic model of a representative PWR plant and emulated PLCs of its digital I&C systems is used to simulate a reactor startup transient. Two simulated FDIAs are investigated; one targeted the Pressure PLC of the PWR pressurizer in the Operation I&C system, and the second targeted one of the four CPC PLCs in the PMS performing the reactor trip safety function. The simulated FDIA on the Pressure PLC manipulated the controller by writing a low system pressure to its memory register prompting it

to turn on the submerged proportional and backup heaters and raise the system pressure. This caused significant increase in the system pressure as the submerged heaters increased flash evaporation. The second simulated FDIA manipulated the CPC to vote to trip the reactor by writing a false high reactor exit temperature to the PLC to make it calculate a value of the CHFR below its trip setpoint and vote to trip the reactor.

Results show that the simulated FDIAs on the emulated PLCs failed to consistently overwrite the true state variable value during every timestep. Intermittently during the simulated FDIA the LOBO NCS communication interface succeeded to write the true state variable value to the register of the PLC. Research detailed in previous reports and publications (see List of Publication on p. 7) have shown that this behavior also observed for a commercial grade Allen-Bradley PLC.

The versatility of the LOBO NCS platform is demonstrated by employing it to simulate a startup of the S^4 CBC space reactor power system for nominal operation and when the PLC for the control drums within the BeO radial reflector targeted by a simulated FDIA. The FDIA attempted to write a false higher value of the rotation rate of the control drums to the PLC's memory register. This application is an example of how the LOBO NCS platform can be extended beyond commercial PWRs to be applied to advanced reactors, SMRs and microreactors, and space nuclear power systems.

Digital I&C systems and cybersecurity investigations are growing fields within the nuclear industry. Platforms such as the LOBO NCS can play a key role in the development of robust, secure digital I&C systems for current and advanced nuclear power plants. They can help investigate cyber-vulnerabilities of I&C system architectures and analyze potential effects of upgrades and modifications and help researchers evaluate different protective measures and train professionals on detecting signs of a potential cyber-compromise within the plant.

Future research plans for the developed LOBO NCS platform include using its capabilities to research advanced control technologies such as AI smart controllers and digital twins for SMRs and space nuclear power systems. Advanced controller concepts could be integrated into an emulated I&C system in the platform to quantify their performance while linked to real-time dynamic models of the nuclear power plants and I&C systems.

6. ACKNOWLEDGEMENTS

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 funded this research. 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.

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. The views expressed in the article do not necessarily represent the views of the U.S. DOE or the United States Government.

We would like to acknowledge the contributions of Christopher Lamb, Raymond Fasano, and Andrew Hahn at Sandia National Laboratories. They collaborated and contributed to the conduct and completion of this DOE NEUP NICSim project. We would also like to acknowledge the contributions of graduate students Ragai Altamimi, Asmaa Salem, and Quac Duong at UNM-ISNPS and Nuclear Engineering Department, in assisting with some of the research tasks. The invaluable contributions of these collaborators contributed to the completion and the successful outcome of this research effort.

7. REFERENCES

Agarwal, V., Ballout, Y. A., Gehin, J. C. (2021). Fission Battery Initiative: Research and Development Plan. Idaho National Laboratories technical report INL/EXT-21-61275, Idaho Falls, ID.

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

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

Blank, E. (2007). I&C Program: Nuclear Steam Supply System Engineered Safety Features Actuation System (NSSS/ESFAS). Palo Verde Nuclear Generating Station Document NID18C000103.

Brown, C., Gabbar, H. A. (2014). Fuzzy logic control for improved pressurizer systems in nuclear power plants. Annals of Nuclear Energy, 72, 461-466.

Busquim e Silva, R. A. (2021). Cybersecurity Assessment Framework for Digital Interface between Safety and Security at Nuclear Power Plants. International Journal of Critical Infrastructure Protection, 34, 100453.

Camacho-Lopez, T. R. (2016). SCEPTRE. Electricity Subsector Coordinating Council & Government Executives Meeting. Technical Report SAND2016-8095C, Sandia National Laboratory, Albuquerque, NM, USA.

Cetiner, S. M., Muhlheim, M. D., Guler-Yigitoglu, A., Belles, R. J., Greenwood, S. M., Harrison, T. J., Denning, R. S., Bonebrake, C. A., Dib, G., Grabaskas, D., Brunett, A. J. (2016). Supervisory Control System for Multi-Modular Advanced Reactors. Oak Ridge National Laboratory technical report ORNL/TM-2016/693, Oak Ridge, TN.

Chae, Y. H., Lee, C., Choi, M. K., & Seong, P. H. (2022). Evaluating attractiveness of cyberattack path using resistance concept and page-rank algorithm. Annals of Nuclear Energy, 166, 108748.

Chatzidakis, S. (2021). Exploring Quantum Key Distribution for Nuclear I&C Cybersecurity. In proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), virtual meeting, June 14-17, 2021, 1383-1391.

Crew, A. W. (2011). AP1000 I&C Data Communication and Manual Control of Safety Systems and Components. Technical Report WCAP-166674-NP, rev 4, APP-GW-GLR-087, rev 2, Westinghouse Electric Company LLC, Cranberry Township, PA.

de Oliveira, M. V., & de Almeida, J. C. S. (2013). Application of artificial intelligence techniques in modeling and control of a nuclear power plant pressurizer system. Progress in Nuclear Energy, 63, 71-85.

Derr, K. W., Becker, C. D. (2011). Securing Wireless Technologies in Nuclear Facilities. In proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), virtual meeting, June 14-17, 2021, 626-637.

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

El-Genk, M. S. (2008). Space Reactor Power Systems with No Single Point Failures. J. Nuclear Engineering and Design, 238(9), 2245-2255.

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., Schriener, T., Hahn, A., Fasano, R., Lamb, C. (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), virtual meeting, June 14-17, 2021, 1417-1426.

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

El-Genk, M.S., Schriener, T.M., (2022), Modeling and Simulation Capabilities for Nuclear Cybersecurity Investigations of a Representative PWR Plant and a Space Reactor Power System," in Nuclear Power Plants: Recent Progress and Future Directions, J.K. Compton (Ed.), Nova Science Publishers, Hauppauge, NY, 2022.

El-Genk, M. S., Tournier, J. M. (2007). Noble Gas Binary Mixtures for CBC Space Reactor Power Systems. J. Propulsion and Power, 23(4), 863-873.

El-Genk, M. S., Tournier J. M. (2016). A Point Kinetics Model and Dynamic Simulation of Next Generation Nuclear Reactor. J. Progress in Nuclear Energy, 92, 91-103.

El-Genk, M. S., Tournier, J. M., and Gallo, B. M. (2010). Dynamic Simulation of a Space Reactor System with Closed Brayton Cycle Loops. Journal of Propulsion and Power, 26(3), 394-406.

Electrical Power Research Institute (EPRI) (2011). Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems. EPRI technical report 1022983, Palo Alto, CA

Fanning, T. H., Cahalan, J. E. (2017). The SAS4A/SASSYS-1 Safety Analysis Code System, Version 5, Argonne National Laboratory technical report ANL/NE-16/19, Argonne, IL.

Fasano, R., Lamb, C., El-Genk, M. S., Schriener, T. M., Hahn, A. (2020). Emulation methodology of programmable logic controllers for cybersecurity applications. 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-POWER2020-11150.

Gallier, S. (2021). U.S. nuclear capacity factors: Reliable and looking for respect. Nuclear News, 64(6), May 2021, 28-36.

Gallo, B. M., El-Genk, M. S. (2009). Brayton Rotating Units for Space Reactor Power Systems. J. Energy Conversion and Management, 50(9), 2210-2232.

Garcia, I. L. (2021). Nuclear Energy Agency's Consensus Position on the Impact of Cyber Security Features on Digital Instrumentation and Control Systems Important to Safety at Nuclear Power Plants –Evaluation Framework. In proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), virtual meeting, June 14-17, 2021, 1437-1444.

Gauntt, R. O., Cole, R. K., Erickson, C. M., Gido, R. G., Gasser, R. D., Rodriguez, S. B., Young, M. F. (2000). MELCOR computer code manuals. Sandia National Laboratories, Albuquerque, NM, NUREG/CR 6119.

Hahn, A., Sandoval, D. R., Fasano, R. E., Lamb, C. (2021). Automated Cyber Security Testing Platform for Industrial Control Systems. In proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), virtual meeting, June 14-17, 2021, 915-924.

Hahn, A., Schriener, T. M., El-Genk, M. S. (2020). 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.

Hemsley, K. E., Fisher, R. E. (2018). History of Industrial Control System Cyber Incidents. Idaho National Laboratories report INL/CON-18-444111-Revision-2, Idaho Falls, ID.

Hung, P. L. (2010). Core Protection Calculator System: Past, Present, and Future. In proceedings 18th International Conference on Nuclear Engineering (ICONE18), May 17-21, 2010, Xi'an, China, ICONE18-29001.

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).

Isermann, R., Balle, P. (1997). Trends in the Application of Model-Based Fault Detection and Diagnosis of Technical Processes. Control Eng. Practice, 5(5), 709-719.

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.

Kim, J., Lee, D., Yang, J., Lee, S. (2020). Conceptual design of autonomous emergency operation system for nuclear power plants and its prototype. Nuclear Engineering and Technology, 52, 308-322.

King, J. C., El-Genk, M. S. (2007). Temperature and Burnup Reactivities and Operational Lifetime for the Submersion Subcritical Safe Space (S^4) Reactor. J. Nuclear Engineering and Design, 237, 552-564.

King, J. C., El-Genk, M. S. (2009). Thermal-Hydraulic and Neutronic Analyses of Submersion-Subcritical, Safe Space (S^4) Reactor. J. Nuclear Engineering and Design, 239(12), 2809-2819.

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.

Lew, R., Poresky, C. M., Ulrich, T. A., Boring, R. L. (2019). Integrated Approach to Advanced Reactor Operations. In proc. 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019), Orlando, FL, February 9-14, 2019, 507-521.

Lin, L., Athe, P., Rouxelin, P., Avramova, M., Gupta, A., Youngblood, R., Lane, J., Dinh, N. (2021). Development and assessment of a nearly autonomous management and control system for advanced reactors. Annals of Nuclear Energy, 150, 107861.

Marriott, A. T., Fujita, T. (1994). Evolution of SP-100 System Designs. In proc. Space Nuclear Power and Propulsion: Eleventh Symposium, AIP Conference Proceedings Vol. 301, No. 1, 157-169.

McNelles, P., Lu, L. (2013). A review of the current state of FPGA systems in nuclear instrumentation and control. In proc. of the 2013 21st International Conference on Nuclear Engineering (ICONE21), July 29 - August 2, 2013, Chengdu, China, paper ICONE21-16819.

Metzger, J. D., El-Genk, M. S. (1992). Application of a Model-Reference Adaptive Controller with Selective State-Variable Weighting to an SP-100 Space Nuclear Power System. J. Propulsion and Power, 8(5), 1093–1102.

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, 171-187.

National Research Council (1997). Digital Instrumentation and Control Systems in Nuclear Power Plants. Safety and Reliability Issues, Final Report, 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 Safety Analysis Division (2001). RELAP5/MOD3.3 Code Manual Volume II: User's Guide and Input Requirements. Information Systems Laboratories, Inc., Rockville, Maryland.

Oka, Y., Suzuki, K. (2013). Nuclear Reactor Kinetics and Plant Control (Vol. 10, pp. 978-4). Springer, Tokyo, Japan.

Palo Verde Nuclear Generating Station (2017). Palo Verde Nuclear Generating Station Units 1, 2, and 3 Updated Final Safety Analysis Report, Rev. 19 Corrected (Redacted per RIS 2015-17).

Pelowitz, D. B., et al. (2010). MCNPX 2.7.C Extensions. Los Alamos National Laboratory, Los Alamos, LA-UR-10-00481.

Perlroth, N. (2019). Hackers are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say. New York Times, June 19, 2019.

Raimbault, S. (2019). Libmodbus v3.1.6., https://github.com/stephane/

Ramuhalli, P., Cetiner, S. M. (2019). Concepts for Autonomous Operation of Microreactors. Oak Ridge National Laboratory technical report ORNL/TM-2019/1305, Oak Ridge, TN.

Ross, S. B., El-Genk, M. S., Matthews, R. B. (1990). Uranium Nitride Fuel Swelling Correlation. J. Nuclear Materials, 170, 169-177.

Sabharwall, P., Gibb, J., Ritter, C., Araújo, K., Gupta, A., Ferguson, I., Rolston, B., Fisher, R., Gehin, J., Ballout, Y. (2021). Cyber security for microreactors in advanced energy systems. Cyber Security: A Peer-Reviewed Journal, 4(4), 345-367.

Schindhelm, E. P., Single, R. E. (2010). AP1000 Protection and Safety Monitoring System Architecture Technical Report. Technical Report WCAP-16675-NP, APP-GW-GLR-147, rev 2, Westinghouse Electric Company LLC, Cranberry Township, PA.

She, J., Jiang, J. (2011). On the speed of response of an FPGA-based shutdown system in CANDU nuclear power plants. Nuclear Engineering and Design, 241(6), 2280-2287.

Shin, J., Son, H., Khalil ur, R., Heo, G. (2015). Development of a cyber security model using Bayesian networks. Reliability Engineering & System Safety, 134, 208-217.

Siemens Power Corporation (2000). TELEPERM XS: A Digital Reactor Protection System. Technical Report EMF-2110(NP) rev 1, Richland, WA.

Southern Nuclear Operating Company (2018). Vogtle Electric Generating Plant 3 and 4 Updated Final Safety Analysis Report, Revision 6, ND-18-0656, Southern Nuclear Operating Company, Inc., Birmingham, Alabama.

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

Tournier, J. M., El-Genk, M. S. (2006). Bellows-Type Accumulator for Liquid Metal Loops of Space Reactor Power Systems. In proc. of Space Technology and Applications Inter. Forum (STAIF-06), AIP Conference Proceedings No.813, 730-742.

Triplett, B. S., Loewen, E. P., & Dooies, B. J. (2012). PRISM: a competitive small modular sodium-cooled reactor. Nuclear Technology, 178(2), 186-200.

Uhrig, R. E., Hines, J. (2005). Computational intelligence in nuclear engineering. Nuclear Engineering and Technology, 37(2), 127-138.

US Department of Homeland Security (2015). Nuclear Sector Cybersecurity Framework Implementation Guidance, Department of Homeland Security report, Washington, DC.

VMware (2019). VMware Workstation 15 Pro.

Wang, P., Yan, X., & Zhao, F. (2019). Multi-objective optimization of control parameters for a pressurized water reactor pressurizer using a genetic algorithm. Annals of Nuclear Energy, 124, 9-20.

Westinghouse Electric Company (2003). Common Qualified Platform Digital Plant Protection System. Technical Report WCAP-16097-NP-A Appendix 3, Westinghouse Electric Company LLC, Cranberry Township, PA.

Westinghouse Electric Company (2011). AP1000 Design Control Document Revision 19, Westinghouse Electric Company LLC, Pittsburgh, PA.

Wheeler, T., Denman, M., Williams, R. A., Martin, N., Jankovsky, Z. (2017). Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis. Sandia National Laboratories Technical Report SAND2017-10307, Albuquerque, NM.

Wierman, T. E., et al. (2001). Reliability Study: Combustion Engineering Reactor Protection System 1984-1998. Idaho National Engineering and Environmental Laboratory Report NUREG/CR-5500, Vol. 10, Idaho Falls, ID.

Wood, R. T., Upadhyaya, B. R., Floyd, D. C. (2017). An autonomous control framework for advanced reactors. Nuclear Engineering and Technology, 49, 896-904.

Word, J. L., Fischer, R. L., & Ingle, B. D. (1967). Static Parasitic Speed Controller for Brayton-Cycle Turboalternator. NASA technical report NASA TN D-4176, Lewis Research Center, Cleveland OH.

Wright, S.A, Lipinski, R.J., Vernon, M.E., Sanchez, T. (2006). Closed Brayton Cycle Power Conversion Systems for Nuclear Reactors: Modeling, Operations, and Validation, Sandia National Laboratories Report SAND2006-2518, Albuquerque, NM.

Yi, J., Ye, J., Xue, Y., Yang, X., & Qian, H. (2009). Research on pressurizer water level control of nuclear reactor based on CMAC and PID Controller. In proc. 2009 International Conference on Artificial Intelligence and Computational Intelligence (Vol. 3, pp. 8-11). Shanghai, China, Nov 7-9, 2009.

Zhang, F., Payne, T., Childress, B. (2021). Developing a Compact Cybersecurity Testbed Using Raspberry Pi Emulated PLC. In proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021), virtual meeting, June 14-17, 2021, 905-914.