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

DRAFT
ICONE28-POWER2020-14645

NICSIM: NUCLEAR INSTRUMENTATION & CONTROL SIMULATION FOR EVALUATING RESPONSE TO CYBER-ATTACKS

Mohamed S. El Genk, Timothy Schriener, Ragai Altamimi, Andrew Hahn.
Institute for Space and Nuclear Power Studies and Nuclear Engineering Department
University of New Mexico, **Albuquerque, NM**

Christopher Lamb, Raymond Fasano
Sandia National Laboratories
Albuquerque, NM

ABSTRACT

Digital Instrumentation and Control (I&C) systems in critical energy infrastructure, including nuclear power plants, raise cybersecurity concerns. Cyber-attack campaigns have targeted digital Programmable Logic Controllers (PLCs) used for monitoring and autonomous control. This paper describes the Nuclear Instrumentation and Control Simulation (NICSim) platform for emulating PLCs and investigating potential vulnerabilities of I&C systems in nuclear power plants. It is being developed at the University of New Mexico's Institute for Space and Nuclear Power Studies (UNM-ISNPS), in collaboration with Sandia National Laboratories (SNL), with high fidelity emulytics and modeling capabilities of a physics-based, dynamic model of a PWR nuclear power plant. The NICSim platform would be linked to the SCEPTRE framework at SNL to emulate the response of the plant digital I&C systems during nominal operation and while under cyber-attack.

Keywords: nuclear plant cybersecurity, digital instrumentation and control, PWR nuclear plant, modeling and simulation, programmable logic controllers

NOMENCLATURE

CHFR	critical heat flux ratio
CPC	core protection calculator
DOE	Department of Energy Nuclear Energy
NEUP	Nuclear Engineering University Program
ESF	engineered safety features
ESFAS	engineered safety features actuation system
I&C	instrumentation and control
ICS	industrial control system
IP	internet protocol
ISNPS	Institute for Space and Nuclear Power Studies
NICSim	Nuclear power plant Instrumentation & Control Simulation
PLC	programmable logic controller
PWR	pressurized water reactor
RTU	remote terminal unit
SG	steam generator
SNL	Sandia National Laboratories
TCP	transmission control protocol
UNM	University of New Mexico
Δt	simulation timestep
φ	PLC sampling frequency

1. INTRODUCTION AND BACKGROUND

Digital Industrial Control Systems (ICSs) are being used in many fields, including energy generation and transmission infrastructure. Examples are smart grids; aerospace and aviation; defense systems; oil and gas processing and refining; and manufacturing. Multiple cyber-attack campaigns have been executed in recent years against control systems worldwide. 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 [1,2]. The Stuxnet campaign targeted the specialized digital Programmable Logic Controller (PLC) computers. Unlike enterprise IT networks, ICSs frequently do not have the same levels of safeguards and defensive technologies against potential cyber-attacks.

Replacing the analog systems with digital Instrumentation and Control (I&C) in existing commercial nuclear power plants in the USA and abroad, has enhanced safety and reliability, and increased availability or load factor by minimizing scram events. In addition, it supported power uprates, increasing the electricity generating capacity and economics of the current plants. Current and future Generation III and III+ reactor designs would mostly use digital I&C systems for autonomous control and activation of safety and protection systems [3].

Unlike analogy systems, the digital IC systems are vulnerable to potential cyber-attacks. Therefore, it is imperative to evaluate the potential cyber-vulnerabilities of current and planned nuclear I&C architectures in nuclear power plants [4,5]. Nuclear power plants typically employ separate I&C systems for autonomous plant control and for plant safety and

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

protection by initiating a reactor trip and/or actuating the Engineered Safety Features (ESF) [3]. These systems operate mostly independent of the reactor operator's actions. Therefore, a cyber-compromise of the safety PLCs could potentially provide access to a hostile actor, significantly impacting the plant's operation and safety.

Figure 1 presents a layout of the autonomous reactor digital safety and protection trip system. The reactor trip function logic is performed by four independent PLCs, one for each of four protection system safety divisions (A, B, C, and D). Each reactor trip PLC receives measurement signals from a range of instruments throughout the plant. These include the reactor power based on ex-core neutron flux detectors, the positions of the control rod assemblies in the reactor core, temperatures in the hot and cold legs of the primary coolant loop, system pressure and water level in the pressurizer, the shell-side water level and pressure in the steam generators, and the rotation speed of the primary loop coolant pumps (Fig. 1). Each safety division has independent measurement instruments connected to its PLC. Each of the four PLCs then determines whether or not to vote for a reactor trip based on its logic programming and send a signal to a voting coincidence logic PLC. It combines the signals from the four reactor trip PLCs. A reactor trip will be initiated if at least 2 of 4 PLCs signal to the switchgear of control elements drives to trip the reactor (Fig. 1)

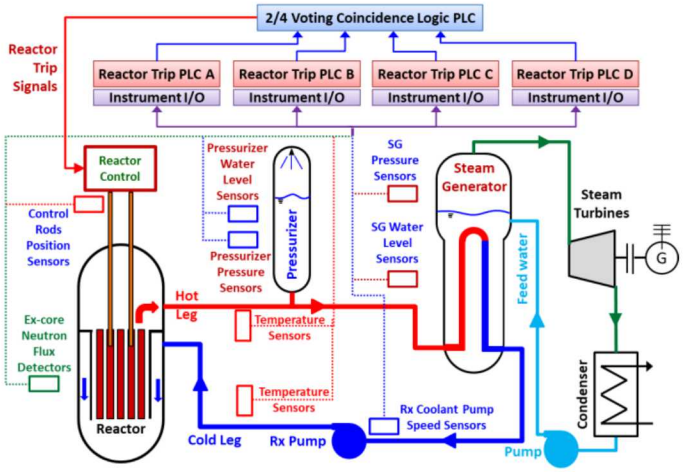

FIGURE 1: LAYOUT OF A PWR PLANT SAFETY AND PROTECTION I&C SYSTEM FOR AUTONOMOUS CONTROL AND REACTOR TRIP

Cyber-attacks on the safety and protection I&C system may manipulate the PLCs to report false signals that the plant is operating safely, while actively attempting to either force a reactor trip or the plant into an unsafe operating condition [2]. Cyber actors may attempt to attack I&C system to disrupt the transmission grid, forcing a plant blackout and incurring economic costs, similar to the Crashoverride campaign [1]. Given the high degrees of safety and reliability required for US nuclear power plants, such attacks could pose a major threat to the commercial nuclear fleet.

Prior nuclear cybersecurity research has largely focused on developing diagnostic tools to detect signs of a cyber-compromise and on analyzing potential consequences of a successful cyber-compromise. Sandia National Laboratories had investigated developing a methodology to integrate consequence analysis with the progression of a cyber intrusion in nuclear I&C systems [6]. Shin, et al. [7] have developed a cyber-security risk model for nuclear plant I&C systems. This model couples an activity-quality analysis, for evaluating human compliance to security regulations, to an architecture analysis model of system vulnerabilities. Hill, et al. [8] have investigated developing a FreeBSD-based simulation framework for modeling a research reactor control system. They used a computer network simulator that employs Transmission Control Protocol (TCP/IP) and Modbus/TCP communication protocols. For the verification and validation of the PLC's programming, Rankin and Jiang [9] investigated creating a platform using a hardware-in-the-loop implementation that links a physical Tricon v9 PLC from a CANDU reactor to a nuclear plant training simulator.

Therefore, it is desirable to develop an I&C system platform that could effectively investigate real vulnerabilities of nuclear plants to cyberattacks aimed at ICSs. Simplified functional models of plant components such as PLCs or communication buses within the plant and components simulation models would be useful for investigating responses of I&C system architectures. However, higher fidelity computer emulation models are required to understand cyber-vulnerabilities in the software and firmware on various devices. A platform with emulytics capabilities is therefore needed, which would allow cybersecurity researchers to investigate potential cybersecurity vulnerabilities in nuclear power plants I&C systems and understand plants' response to a successful cyber-compromise.

To address these needs, the University of New Mexico's Institute for Space and Nuclear Power Studies (UNM-ISNPS), in collaboration with Sandia National Laboratories (SNL) are developing a next-generation Nuclear Instrumentation and Control Simulation (NICSim) platform. The NICSim platform when coupled to the SCEPTRE emulytics framework at SNL, could investigate cybersecurity of ICSs [10].

2. NICSim PLATFORM

Fig. 2 outlines the elements of the NICSim platform. The emulated I&C system components are coupled to fast running, physics-based models of the nuclear power plant components and sensor instruments (Fig. 2) for direct feedback of the integrated I&C system's behavior. The physics-based dynamic models are developed using the versatile Matlab Simulink platform [11]. The SCEPTRE framework would emulate (via precise firmware and software execution within virtual machine environments) and simulate (via computational models) the plant's I&C system components. It handles intercommunication between devices across a virtual computer network using real ICS communication protocols. It is capable of embeding physical hardware components into its virtual network.

The physics-based dynamic nuclear plant model in NICSim is linked to the emulated, simulated, and/or physical PLCs and other I&C system components by a data transfer interface program which communicates with a data broker program [10]. The elements of the NICSim platform are designed to be adaptable to different reactor plant designs and I&C architectures. The coupling of an emulytics model of the plant I&C system and a dynamic model of the integrated nuclear power plant within the NICSim platform makes it possible to examine the effects of postulated cyber-attacks on the I&C system, the nuclear reactor operation, and the plant safety within a repeatable, sandboxed virtual testing environment.

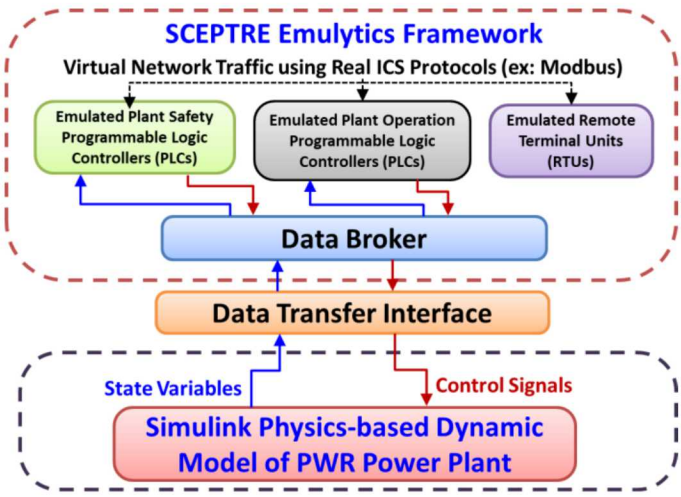

FIGURE 2: NUCLEAR INSTRUMENTATION AND CONTROL SIMULATION (NICSim) PLATFORM.

The NICSim platform includes a fast-running, physics-based dynamic model of a Pressurized Water Reactor (PWR) plant to provide direct feedback to the emulated components of the plant's digital I&C system. The Nuclear Plant Model in Simulink provides a modular environment with robust simultaneous solvers of series of differential equations for multitude of simplified physics-based models of different plant components. These include those of the reactor and primary coolant loop, the pressurizer, the steam generator, the primary feedwater pump, and the secondary loop. The modular Simulink platform would make it possible to add or change component models, enabling potential future expansions.

Fig. 3 presents a line diagram of the physics-based model of the PWR power plant. The plant model is comprised of: (a) a reactor model with coupled thermal-hydraulics and robust reactor point-kinetics, (b) a primary loop model, which solves the overall mass, momentum, and energy balance within the loop, (c) a steam generator model, (d) pressurizer model, (f) and a simplified model of the secondary loop. The NICSim plant model incorporates the dimensions, masses, and materials for the plant components, the reactor kinetics parameters, the reactivity control and temperature feedback parameters, the reactor coolant pump characteristic curves, and the secondary loop thermodynamic parameters.

The reactor model couples a point kinetics model to a thermal-hydraulic model. The point-kinetics model calculates the reactor fission power and change in the power in response to changes in reactivity due to movement of the control elements and various temperature reactivity feedback effects for the fuel, cladding, and the moderator, including the effects of soluble boron. It solves the 6-point kinetics equations using a robust and efficient exponential matrix technique approximated using the 7th order-accurate Padé(3,3) function [12]. This approximation is efficient, stable, and accurate independent of the timestep sizes used in the calculations.

The reactor thermal-hydraulics model is a lumped model of the core, represented by an average fuel rod, and includes the in-vessel coolant and core structure such as the reactor vessel and core internals. For given inlet 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. It is coupled to the primary loop thermal-hydraulic mode to calculate the coolant flow rate and inlet temperature in the core, after accounting for the effect of the steam generator.

The primary loop model includes physics-based models of the reactor core, the pressurizer, the steam generators, the primary coolant pumps, and the piping of the hot and cold legs. The calculated temperatures and system pressure are used to determine the thermophysical properties of the coolant, fuel, and structural materials. The primary loop model also accounts for the coolant volume due to changes in temperature and pressure, and the inflow and outflow through the charging and letdown valves in the cold leg, respectively. The coolant inventory in the primary loops is also used to determine the rates of in-surge and out-surge of coolant 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 rate in the primary loop is calculated from equating the total pressure losses in the primary loop to the pressure head generated by the primary coolant pumps.

The three regions, non-equilibrium PWR pressurizer model calculates the transient changes in the system pressure and the water level in the pressurizer. The model tracks the mass and energy exchanges between the top saturated vapor region, the middle saturated water region, and a lower subcooled water region representing the insurge from primary loop coolant into the pressurizer. This physics-based model calculates the rates of evaporation and condensation due to pressurizer heaters and water spray, respectively, surface condensation due to heat losses through the pressurizer wall, and the changes in system pressure and the pressurizer water level. The pressurizer model utilizes control signals from PLCs to control the electric heaters located in the middle and lower regions of the pressurizer and the water spray nozzle in the top region.

The NICSim steam generator model determines the rate of heat removal from the primary loop in the steam generator's U-

tubes to the secondary water flow on shell side and the steam exit steam quality and flow rate to the turbine for electricity generation. This model calculated the changes in the internal water level and the exit steam quality at steady state and in operation transient due to a change in the load demand. It also calculates the change in the heat removal from the primary coolant due to changes in the steam demand to the turbine, the internal water level on the shell-side of the steam generator, the steam flow rate to the turbines, the recirculation rate within the steam generator, and the feedwater flow rate. The latter is controlled using an external PLC.

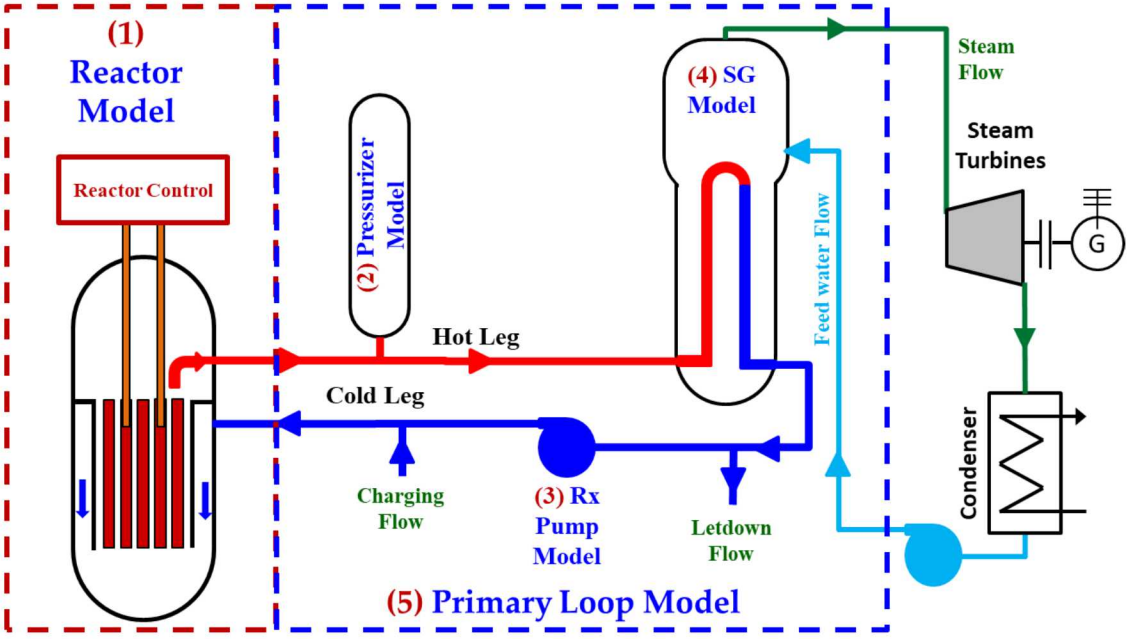

FIGURE 3: BLOCK DIAGRAM OF PHYSICS-BASED COMPONENT MODELS FOR A PWR PRIMARY LOOP IN NICSIM.

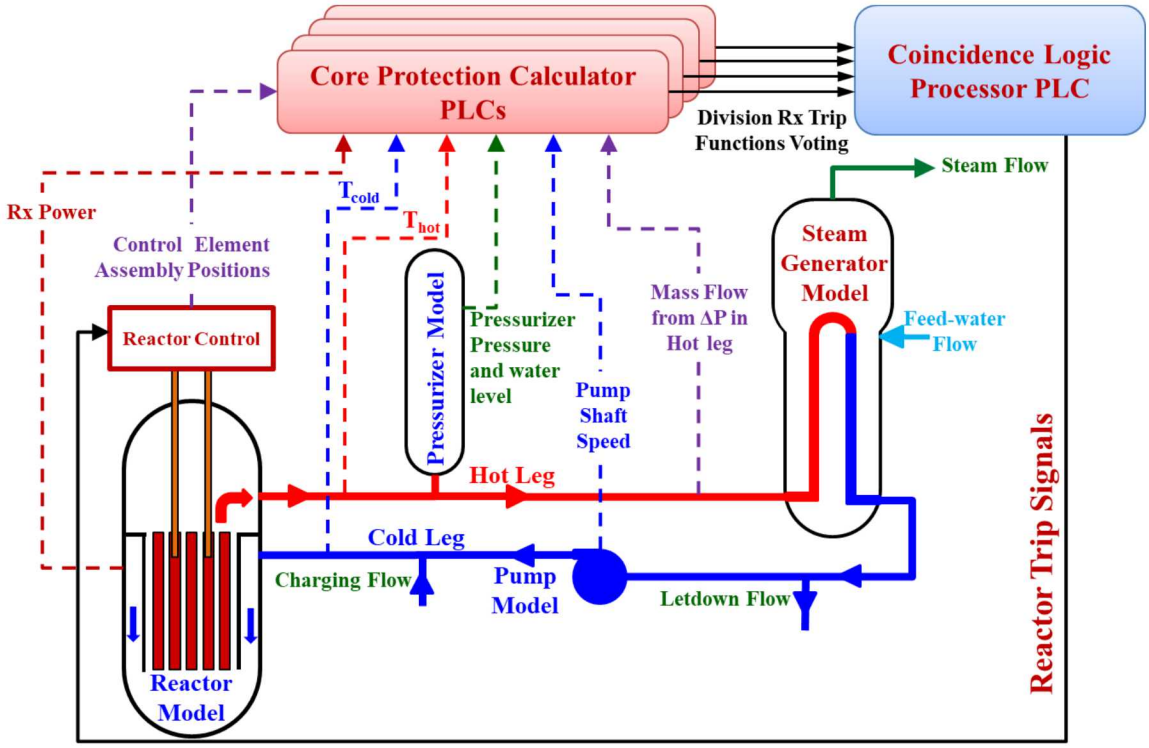

FIGURE 4: BLOCK DIAGRAM OF THE DIGITAL REACTOR SAFETY I&C SYSTEM FOR THE REACTOR TRIP FUNCTION.

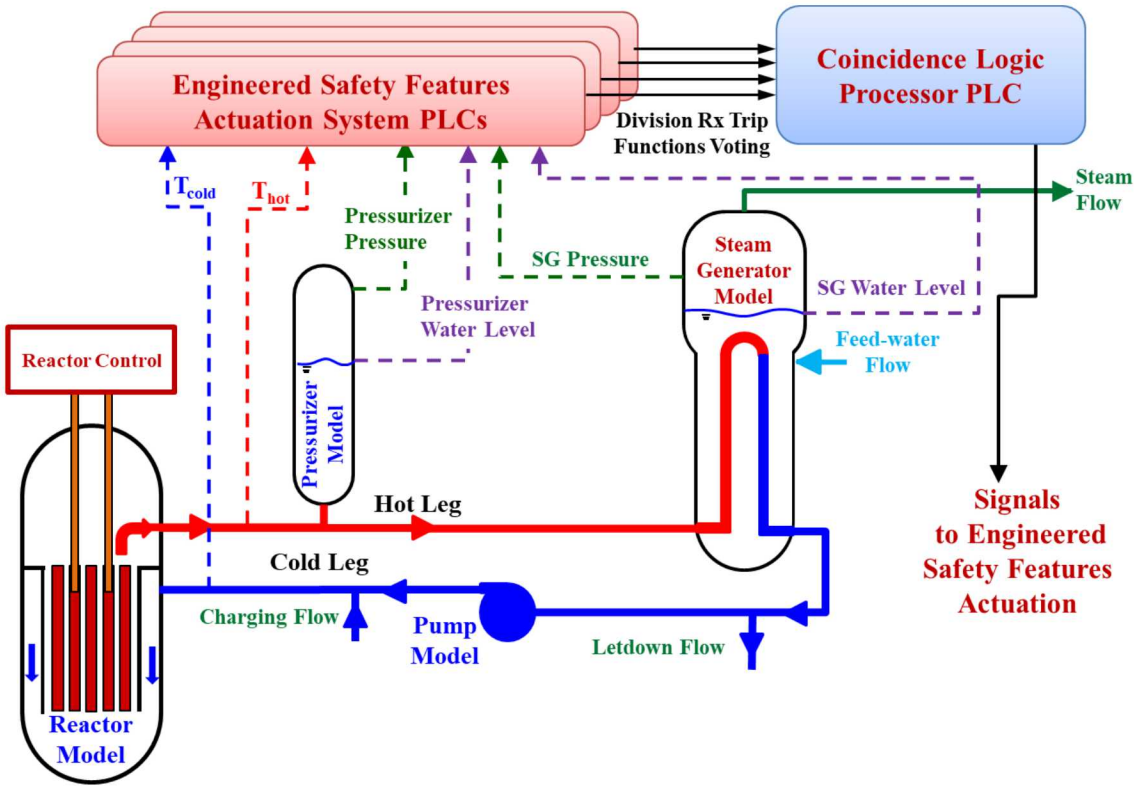

FIGURE 5: BLOCK DIAGRAM OF THE DIGITAL REACTOR SAFETY I&C SYSTEM FOR THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

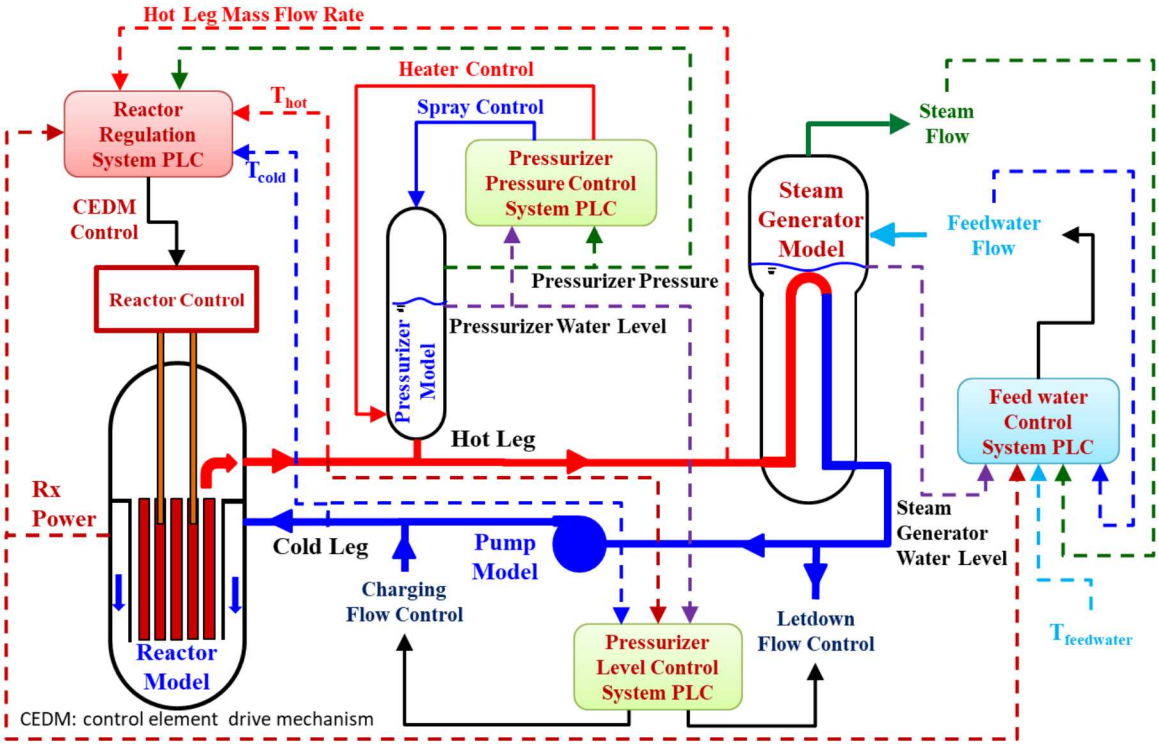

FIGURE 6: BLOCK DIAGRAM OF PRIMARY LOOP OPERATIONAL I&C SYSTEM PROGRAMMABLE LOGIC CONTROLLERS

The primary coolant pump model calculates the performance of the coolant pumps connected to the cold legs of the primary loop. It is partially based on the pump model used in the RELAP5 system code [13], and uses homologous pump curves to calculate the pressure head and hydraulic torque as a function of the operating conditions. The pump pressure head is used within the primary loop overall momentum balance to determine the coolant flow rate. This model uses the calculated pump hydrodynamic and shaft torque to determine the thermal energy dissipation, deposited directly in the primary coolant as well as the required pumping power. Different pump rated parameters and homologous head and torque curves could be input by the user to allow the model to simulate the performance of different coolant pump designs.

3. Emulated Nuclear Plant I&C System Architecture

A representative I&C system architecture is developed for the PWR plant model in the NICSim platform. An I&C system for a representative PWR plant includes a number of emulated PLCs within the safety and protection and the plant operation I&C systems. The PLCs within the safety and protection I&C system perform the reactor trip initiation function (Fig. 4) and the ESF actuation function (Fig. 5). The PLCs in the plant operation I&C system provide for the autonomous regulation of the reactor power, system pressure, the pressurizer's water level, and the feedwater flow to the steam generators. Each PLC is emulated using a virtual machine running the open-source OpenPLC software running its control logic program [15]. The OpenPLC software runs IEC 61131-3 standard PLC programming languages and communicates using the widely used Modbus ICS communication protocol. These emulated PLCs are validated using the PLC emulation methodology established as part of this research effort.

The Core Protection Calculator (CPC) PLCs perform the reactor trip voting function (Fig. 4). The four independent CPC PLCs each receive values of state variables from the physics-based PWR plant model. These include the reactor thermal power, control element assembly positions, water temperatures in the hot and cold legs, and the pressure and water level in the pressurizer. Two separate state variables are used by the CPC to determine the coolant flow rate through the reactor primary loop; from the shaft speed of the primary coolant pumps and the primary loop pressure loses demand and the pump supply curves, as well as the measured pressure differential across a section of the hot leg. The logic programming of the CPC uses the plant state variables to calculate safety parameters, including the minimum Critical Heat Flux Ratio (CHFR) for the identified hot channel in the reactor core, and the temperature margin of the hot leg coolant from the saturation temperature at system pressure, and potential discrepancies between the different measurements of the coolant flow rate.

The CPC PLC's program compares the received state variables and the calculated parameters to safety setpoints for the reactor trip functions, to determine if any of the limits have been exceeded. In this case, the CPC's programming communicates a signal to the coincidence logic processer PLC that the division has voted to trip the reactor (Fig. 4). The coincidence logic processer PLC compares the voting signals of the four separate safety divisions' CPC PLCs. The coincidence logic processer PLC generates a reactor trip signal if the required 2/4 voting coincidence is satisfied. This signal is then communicated back to the nuclear plant model to trip the reactor (Fig. 4).

The PLC of the Engineered Safety Features Actuation System (ESFAS) performs the automatic actuation function for the plant's ESF. The four independent ESFAS PLCs receive values of the state variables from the component submodels of the PWR plant model. These are the hot and cold leg coolant temperatures, the system pressure, the water levels in the pressurizer, and the water level and internal pressure in the steam generators (Fig. 5). These values are compared to setpoints programed within the PLCs for the different ESF systems of the plant. If the PLCs' programming determines that any of the plant state variables exceeds the safety setpoint for an ESF system, the PLC sends a voting signal to actuate that system. The Coincidence Logic Processor PLC receives the voting signals from the four ESFAS and sends an actuation signal to the systems components.

In addition to the PLCs of the plant protection and safety monitoring system, the representative I&C system architecture includes PLCs for the autonomous operation of the plant components within the reactor primary loop. These are a reactor regulation PLC, a pressurizer pressure control PLC, pressurizer water level control PLC, and steam generator feedwater control PLC (Fig. 6). These PLCs receive state variables for the physics-based models of these components and send signals back to the plant model for direct control feedback.

The reactor regulation PLC provides autonomous control of the reactor's control rods in order to maintain the reactor thermal power at a level specified by the operators. It monitors the reactor power both from the nuclear instrumentation and the calculated values of the reactor thermal power from the primary loop energy balance. It then adjusts the insertion of the control rods in the core to maintain the desired steady reactor thermal power. The pressure control PLC monitors maintain the primary loop system pressure within programed setpoints. The system pressure is adjusted by controlling the level of the pressurizer proportional and backup heaters and the water spray valve.

The level control PLC regulates the water level in the pressurizer in order to regulate the total water volume in the primary loop. It accommodates changes in water volume due to thermal expansion and contraction during a heatup/cooldown of the primary loop and helps maintain the primary coolant inventory in the event of a leak. This PLC adjusts the water inventory by controlling the rates of inflow from the charging pumps and outflow through the letdown valves. The steam generator feedwater control PLC controls the water inventory within the plant's steam generators to ensure that the U-tube bundles are adequately covered with water. This PLC also

monitors the water level measured in the steam generator's downcomer and adjusts the feedwater flow rate into the secondary side to accommodate changes in the steam flow due to changes in the electrical load demand.

4. I&C SYSTEM EMULATION

The developed PWR nuclear plant model is linked to emulation models of the digital components within the plant's I&C system (Fig. 2). The calculated state variables by the physics-based models of the plant components are input to the developed and implemented digital I&C system of these components within SCEPTRE framework. These components are the digital PLCs in the reactor safety and protection system and operational I&C system described in Section 3 (Figs. 4-6).

Emulations of the digital programmable logic controllers in the representative I&C system are developed to support future cybersecurity investigations and analyses. These controllers emulate the PLCs operating system kernel and control software, and communicate using the same ICS communication protocols. They are developed using a PLC emulation methodology established by the NICSim project team to characterize the key physical and digital signatures of the PLC and validate these signatures against those of an emulated PLC [14]. Validation testing of the PLC emulation methodology is conducted to determine the settings required to ensure that the emulated PLCs replicate the performance and network traffic behavior of the physical devices.

4.1 DOE SCEPTRE Emulytics Framework

SCEPTRE is an emulation, modeling, and simulation framework developed by DOE which creates a test environment that links together control system models and process simulation models [10]. This environment can be comprised of emulated, simulated, and physical hardware control system devices, such as PLCs, Remote Terminal Units (RTUs), and networking devices such as gateways, routers, and firewalls. This framework is capable of starting up large numbers of virtual machines emulating different I&C computer devices and creating virtual networks on which they can communicate.

The emulation virtual machines run software images containing the same operating system and software programs as the physical ICS devices they are representing. SCEPTRE handles the communication between these devices on the virtual networks using standard ICS communication protocols such as Modbus, DNP3 over TCP, ICCP, and IEC-104. Such high fidelity modeling of the ICS computers and network communication allows cyber-security researchers to test the real responses of these systems to malicious software attacks in a repeatable virtual environment. This virtual testing environment can be configured and modified with much greater ease, and lower cost, than a comparable ICS computing hardware testing lab.

SCEPTRE could be linked to a transient, physics-based simulation model of a power plant or an electrical transmission system. The process simulation model within the SCEPTRE framework is referred to as a Provider. The control system devices are linked to the process simulation models by means of a data broker program and a model-specific interface program (referred to as a Wrapper within the SCEPTRE framework). The data broker handles the data transfer between the virtual machines emulating the PLCs, simulation models of I&C components, and the provider's interface programs ('wrapper') using a fast message passing protocol.

4.2 Data Transfer Interface

The NICSim platform employs an efficient and fast-running data transfer interface, which could be used for linking the Matlab Simulink model of a PWR power plant to the broker program (Fig. 7) [14]. The developed data transfer interface program functions as the 'wrapper' within the SCEPTRE framework (Fig. 2). A specialized Simulink S-function written in the C programming language is developed to communicate the simulation state variables to an external interface program written in the python programming language (Fig. 7).

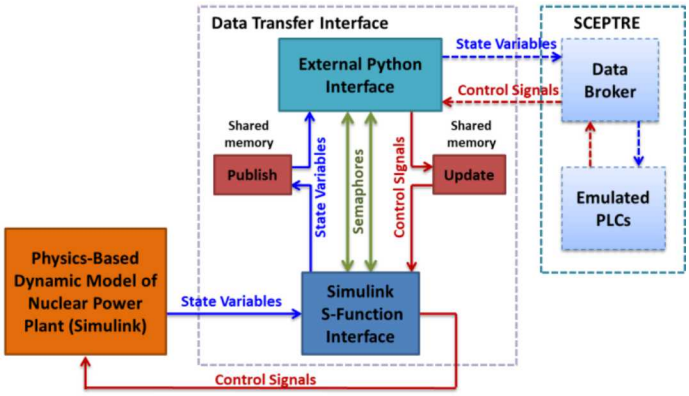

FIGURE 7: BLOCK DIAGRAM OF DEVLOPED NICSim DATA TRANSFER INTERFACE PROGRAM

The state variables calculated by the physics-based nuclear power plant model are communicated to the external python interface using shared memory inter-process communication [14]. The state variables are written and read from a shared memory location named 'publish' (Fig. 7). The control signals determined by I&C system's emulated PLCs are passed back to the Simulink model through a second shared memory location named 'update'. Inter-process communication semaphores are used to control access to the two shared memory locations, ensuring that only one side of the interface can access a given shared memory location at a time. This ensures reliable communication and avoids instabilities caused by attempts to simultaneously access the memory location.

The data transfer interface program also includes a time synchronization routine to ensure that the NICSim nuclear power plant model running in Matlab Simulink runs in the same time scale as the emulated PLCs' control programming. For controllers using real-time clocks, this will ensure that the response timing of the nuclear plant model is in tune with that expected by the controllers' software.

5. PRELIMINARY RESULTS

This section presents preliminary results of some of the developed Simulink-based PWR component models that are linked to the emulated PLC using the data transfer interface in Fig. 7. Fig. 8 shows transient results of the reactor model linked to the safety CPC PLC performing the trip protection function (Fig. 4). The reactor model simulates a transient initiated by a positive reactivity insertion, decreasing the CHFR and eventually causing a reactor trip. The time delay in the response of the emulated PLC is determined by comparing its performance to that of an 'ideal' logic controller with no delay. The latter is built into the Simulink model.

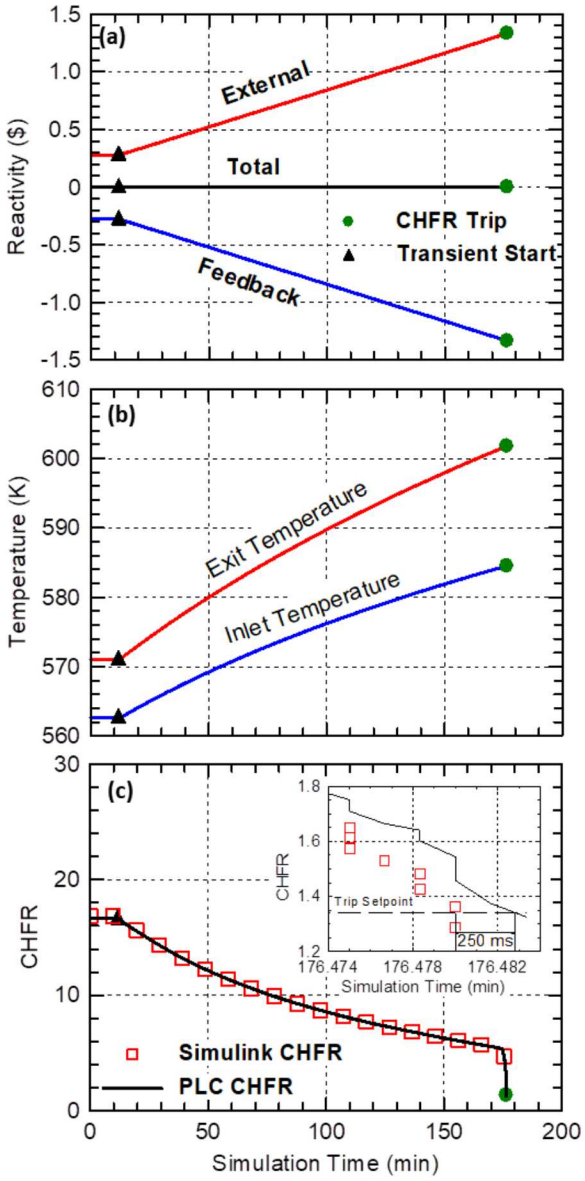

FIGURE 8: SIMULATION RESULTS OF A REACTOR TRANSIENT INITIATED WITH A REACTIVITY INSERTION AND RESULTED IN REACTOR TRIP.

Initially the reactor is at steady state operating at 50% of its nominal thermal power. The transient is initiated by inserting reactivity at a ramp rate of 0.01 cents/s (Fig. 8a), increasing the reactor power and the core exit temperature, and subsequently the core inlet temperature (Fig. 8b). As the coolant temperature in the core increases, CHFR in the designated hot channel decreases. When CHFR decreases to the programed safety setpoint, the CPC PLC signals for a reactor trip (Fig. 8c). The insert in Fig. 8b shows that the emulated CPC PLC responses with 250 ms time delay compared to the internal Simulink controller. The PLC response time is factored into determining the CHFR trip setpoint to ensure that the CHFR does not decrease below the lowest value allowed.

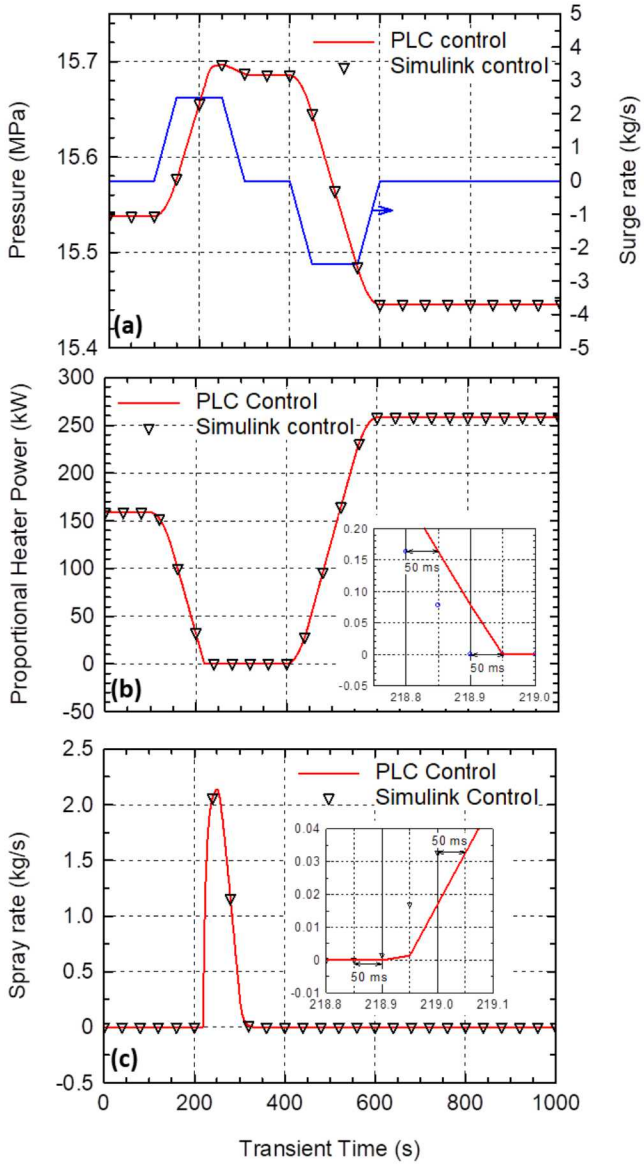

FIGURE 9: SIMULATION RESULTS OF A PRESSURIZER TRANSIENT INITIATED BY WATER INSURGE FROM THE REACTOR PRIMARY LOOP.

Figure 9 presents transient results of the Pressurizer model that is linked to the emulated pressure control PLC (Fig. 6). The simulated transient is of an insurge of coolant from the primary loop. During the transient, the pressure control PLC actuates the proportional heaters and pressurizer spray, as needed, to maintain the system pressure within desirable values. The response time of the emulated PLC linked to the Simulink pressurizer model is compared to that of the internal logic controller built in Simulink, with no delay in response. The emulated pressure control PLC in this case is operated with a sampling frequency, φ = 20 Hz (or 20 samples per second).

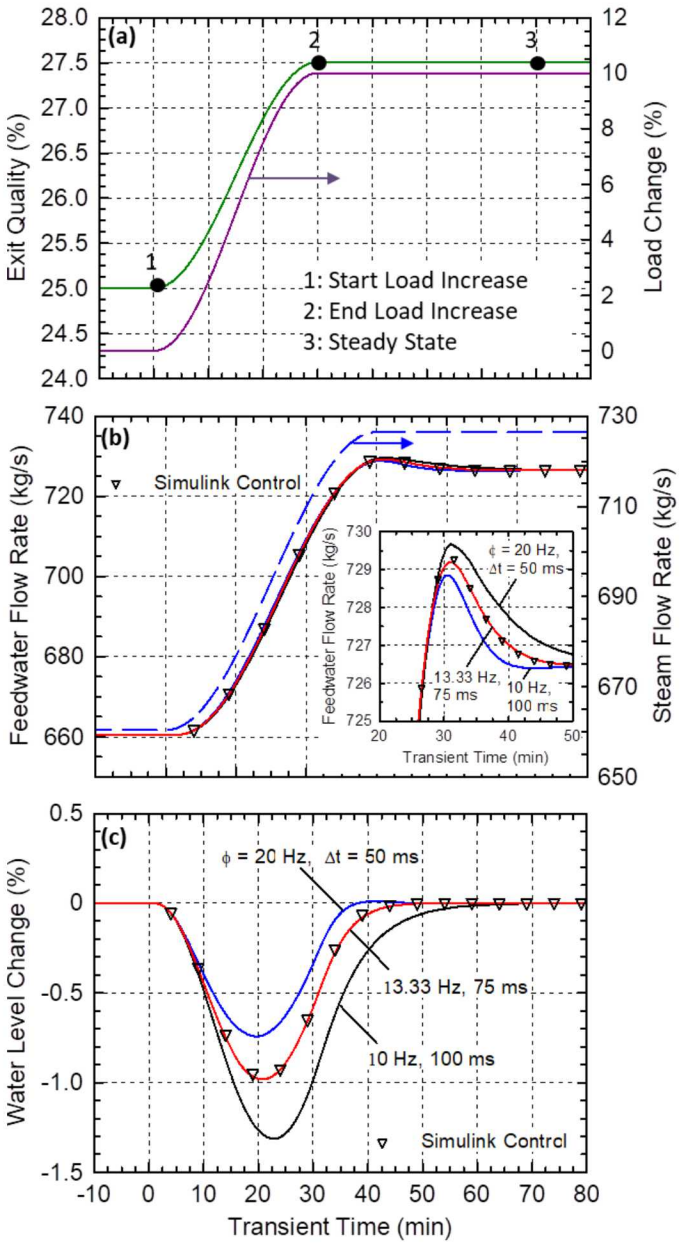

FIGURE 10: RESULTS OF SIMULATED TRANSIENT OF STEAM GENERATOR IN RESPONSE TO A 10% INCREASE IN LOAD DEMAND.

The water insurge into the pressurizer, increases the internal pressure (Fig. 9a), signaling the pressure control PLC to reduces the power to the proportional heaters in response in an attempt to reduce the increase in pressure (Fig. 9b). When the pressure increases beyond the actuation setpoint for the spray, the pressure control PLC opens the spray valve to condense the steam in the vapor bubble of the pressurizer and reduce the pressure (Fig. 9c). Once the pressure levels off, a water outsurge removes some of the accumulated water from the pressurizer into the primary loop. To halt the resulting decrease in system pressure, the pressure control PLC increases the electrical power to the proportional heaters (Fig. 9a,b).

The inserts in Figs. 9b and 9c show the response delay of the emulated PLC compared to the internal Simulink control logic. For both the proportional heaters and water spray, the emulated PLC responds with a 50 ms delay compared to the Simulink model internal controller. This delay in response has only a minor effect on the simulated transient. This is indicated by the close agreement of the system pressure values in Fig. 9a.

Figure 10 present the resulted of a simulation transient of the Steam Generator (SG) model, which is linked to the emulated Feedwater control PLC (Fig. 6). The simulated transient is in response to a 10% increase in the electrical load demand. The feedwater control PLC adjusts the water rate to the steam generator in an attempt to maintain the internal water level at the desirable setpoint (Fig. 6). The response of the emulated PLC that is compared to that of the internal control logic built in Simulink model of the SG. The emulated PLC sampling frequency, φ, and simulation timestep, Δt, are varied. This is to determine the settings which allow the emulated PLC response to match that of the internal Simulink controller.

The increase in load demand, increases the steam flow rate exiting the SG, by increasing the exit stem quality (Figs. 10a,b). The increased steam flow rate reduces the water inventory in the SG, decreasing the water level in the SG downcomer (Fig. 10c). The feedwater control PLC responds to the deceasing water level by adjusting the throttle valve to increase the feedwater rate to SG (Fig. 10b). The increased feedwater rate halts the drop in the water level in the SG, and eventually returns it to the programmed setpoint.

The proportional-integral controller within the feedwater PLC is sensitive to the timestep size. Therefore, the sampling frequency and simulation timestep size are varied to determine the setting for the emulated controller to match the internal control logic in Simulink. The insert in Fig. 10b and water level results in Fig. 10c show that increasing φ and decreasing Δt results in a faster response to slow the change in the water level in SG. With a φ = 13.33 Hz and Δt = 75 ms the response of the emulated PLC nearly matches that of that the Simulink controller with no response delay.

These preliminary results in Figs.8-10 demonstrate some of the capabilities of the NICSim platform to link emulated PLCs running within virtual machines to Simulink-based dynamic models of PWR plant components (Fig. 2). These capabilities would support cybersecurity investigation into the emulated

I&C systems and potential impacts on the power plant operation.

6. CONCLUSION

The UNM-ISNPS in collaboration with SNL is developing the NICSim platform with emulytics capabilities. This platform combines a physics-based model of a commercial PWR power plant with high-fidelity emulations of the plant's digital I&C system architecture. The DOE SCEPTRE framework developed at SNL would emulate the nominal response of the plant digital I&C systems and while under cyber-attack.

A fast-running, dynamic model of the primary loop of a PWR power plant is developed using the Matlab Simulink platform. It consists of physics-based models of the major components, which can be configured to represent different PWR reactor designs. An emulated digital I&C system for a representative PWR plant is also developed. This includes emulated PLCs in the safety and protection I&C system for the autonomous reactor trip and ESF actuation safety functions. The emulated I&C system also includes PLCs for automatic control of the plant's operation. The PLCs within the emulated I&C system are linked to the Matlab Simulink PWR plant model using a robust data transfer interface.

One completed, the NICSim platform will enable cybersecurity researchers to assess the effects of potential cyber-attacks on the digital I&C systems, which may influence reactor operation and/or the plant safety, within a repeatable, sandboxed virtual testing environment. It could also support upgrade activities at existing nuclear facilities as well provide for testing the effectiveness of different cyber-defense strategies, under consideration for use in next generation plants digital I&C systems, against real malicious attacks.

ACKNOWLEDGEMENTS

This research is being performed using funding received from the DOE Office of Nuclear Energy's Nuclear Energy University Program under Contract No. Nu-18-NM-UNM-050101-01.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.

REFERENCES

[1] Dragos, Inc., 2017. "CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations version 2.20170613," www.DRAGOS.com.

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

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

[4] US Department of Homeland Security, 2015, "Nuclear Sector Cybersecurity Framework Implementation Guidance."

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

[6] Wheeler, T., Denman, M., Williams, R.A., Martin, N., and Jankovsky, Z., 2017, "Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis," Sandia National Laboratories Technical Report SAND2017-10307.

[7] Shin, J., Son, H., Khalil ur, R., and Heo, G., 2015, "Development of a cyber security model using Bayesian networks," Reliability Engineering & System Safety, 134, pp. 208-217.

[8] Hill, Z., Chen, S., Wall, D., Papa, M., Hale, J., and Hawrylak, P., 2017, "Simulation and analysis framework for cyber-physical systems," Proceedings of the 12th Annual Conference on Cyber and Information Security Research CISRC '17, Oak Ridge, Tennessee, April 4-6, 2017.

[9] Rankine, D. J., and Jiang, J., 2011, "A Hardware-in-the-Loop Simulation Platform for the Verification and Validation of Safety Control Systems," IEEE Trans. Nuclear Science, 58(2), pp. 468-478

[10] Sandia National Laboratories, 2016, "SCEPTRE," Sandia Document SAND2016-8095C.

[11] The MathWorks, Inc., 2018, Simulink Version 9.2 (R2018b).

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

[13] Nuclear Safety Analysis Division, 2001, "RELAP5/MOD3.3 Code Manual Volume II: User's Guide and Input Requirements," Information Systems Laboratories, Inc., Rockville, Maryland

[14] M. S. El-Genk, et al., "NICSim: Nuclear Instrumentation and Control Simulation for Evaluating Response to Cyber-attack," Albuquerque, NM, 6 August 2019. https://digitalops.sandia.gov/Mediasite/Play/d54f41efcc0241afbce2c027403e6ab41d

[15] Alves, T. R., Buratto, M. M., Mauricio de Souza, F., and Rodrigues, T. V., 2014. "OpenPLC: An open source alternative to automation," IEEE Global Humanitarian Technology Conference (GHTC 2014), San Jose, CA, USA, DOI: 10.1109/GHTC.2014.6970342

