M.S. El-Genk, T.M. Schriener, C.C. Lamb, "1.Nuclear Instrumentation and Control Simulation (NICSim) Platform for Investigating Cybersecurity Risks," Trans. ANS 2020, Cyber Security for Nuclear Power Installations-II, Phoenix, AZ, June 7-11, 2020.

Nuclear Instrumentation and Control Simulation (NICSim) Platform for Investigating Cybersecurity Risks

Mohamad S. El-Genk*, Timothy M. Schriener*, Christopher C. Lamb**

*Institute for Space and Nuclear Power Studies and Nuclear Engineering Department, University of New Mexico, Albuquerque, NM 87131, mgenk@unm.edu
**Sandia National Laboratory, Albuquerque, NM, 87185

INTRODUCTION

Cyber-attack campaigns executed against energy control systems worldwide in recent years have directly targeted digital Programmable Logic Controllers (PLCs) used in Industrial Control Systems (ICS) for monitoring and autonomous control. Digital instrumentation and control (I&C) systems in nuclear power plants offer high efficiency and performance in process control applications, compared to analog systems, but raise potential cybersecurity vulnerabilities. Therefore, there is a need to develop a platform for emulating PLCs and investigating potential vulnerabilities of I&C architectures in nuclear power plants.

This paper introduces the Nuclear Instrumentation and Control Simulation (NICSim) platform, currently being developed at the University of New Mexico's Institute for Space and Nuclear Power Studies in collaboration with Sandia National Laboratories. It offers high fidelity emulytics of I&C systems and physics-based, dynamic modelling capabilities of a PWR power plant. The NICSim platform when interfaced to the DOE SCEPTRE[1] framework at Sandia National Laboratories would emulate the digital I&C systems in nuclear power plants, both during nominal operation and while under a cyber-attack. This platform could also enable cybersecurity researchers to assess the effects of potential cyber-attacks on the digital I&C systems, on nuclear plants operation and safety, within a repeatable, sandboxed virtual testing environment.

APPROACH

Figure 1 outlines the NICSim platform for high fidelity modeling of the ICS computers and network communication. It would make it possible for cyber-security researchers to examine real responses of these systems to malicious software attacks in a repeatable virtual testing environment. In this platform, the SCEPTRE framework would emulate (via precise firmware and software execution within virtual machine environments) and simulate (via computational models) the components of I&C systems in a Pressurized Power Reactor (PWR) plant. SCEPTRE handles intercommunication between PLCs, Remote Terminal Units (RTUs), and networking devices, such as gateways, routers, and firewalls, across a virtual computer network. This is carried out using ICS communication protocols such as Modbus, DNP3 over TCP, ICCP, and IEC-104. SCEPTRE could also embed physical hardware components into its virtual network[1].

The emulated ICS components within SCEPTRE would be interfaced to fast running, physics-based transient models of the nuclear power plant components for direct feedback. The physics-based models, developed on the versatile Matlab Simulink platform[2], are linked to the emulated, simulated, and/or physical PLCs and other I&C system components by a suitable data transfer interface program[3]. This program communicates with the data broker within SCEPTRE. The developed data transfer interface[3] would link the Simulink PWR plant model with a number of ICS emulation frameworks for testing and analysis. The elements of the NICSim platform are designed to be adaptable to different plant designs and I&C architectures.

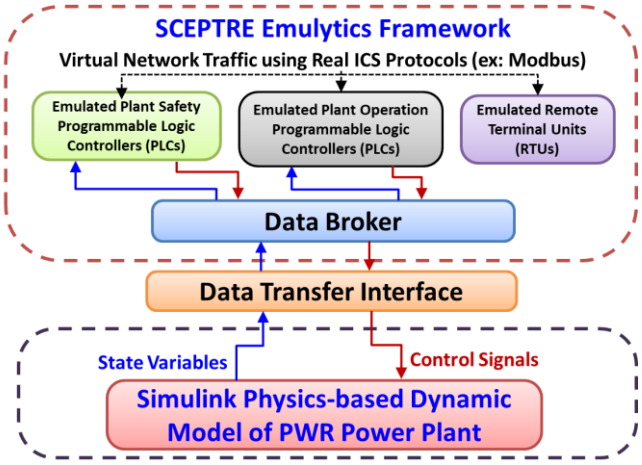

Fig. 1. Components of the Nuclear Instrumentation and Control Simulation (NICSim) platform

The NICSim platform includes a fast-running, physics-based dynamic model of the primary loop of a PWR plant. In addition to solving the overall mass, momentum, and energy balance equations for the primary coolant loop, the PWR plant model includes physics-based models of various components. The phenomenological models of the plant components capture the relevant physics associated with steady state and transient operation, and support fast-running operation while linked with the plant's PLCs. The developed plant model can be configured for different dimensions, materials, and reactor kinetics parameters to represent different PWR plant designs and configurations.

The integrated plant model within NICSim platform couples individual models of the various plant components. These are of the reactor with coupled thermal-hydraulics and robust reactor point-kinetics, the pressurizer[4], the steam

generator[5], the primary loop and coolant pumps. The physics-based integrated plant model incorporates the dimensions, masses, and materials for the various components, the reactor kinetics parameters, the reactivity control and temperature feedback parameters, the reactor coolant pump characteristic curves, and the secondary loop thermodynamic parameters. In addition to steady-state operations, this fast running PWR plant model simulates operational transients, including startup and shutdown, and changes in the electrical load demand.

The reactor point kinetics model, which is coupled to lumped thermal-hydraulic models of the reactor core and the primary coolant loop, calculates the change in fission power in response to a movement of the control elements, injection of soluble boron, and a temperature reactivity feedback for the fuel, cladding, and the moderator. The reactor 6-point kinetics equations are solved using an exponential matrix technique with its accuracy being independent of the simulation timestep size[6]. The lumped thermal-hydraulics model of the reactor core is based on an average fuel rod, and includes the in-vessel coolant and core structure such as the reactor vessel and core internals. This model calculates the average temperatures of the fuel, cladding and coolant, as well as the core pressure losses as functions of the reactor thermal power during nominal and transient operations.

The three region non-equilibrium pressurizer model[4] calculates the transient changes in the system pressure and the water level in the pressurizer. It tracks the mass and energy exchanges between the top saturated vapor region, the middle saturated water region, and a lower subcooled water region in case of a surge in of the coolant from the primary loop. This model also accounts for the evaporation and condensation due to pressurizer heaters in saturated water region and water spray in the saturated vapor region. It also account for condensation and liquid film evaporation at the inner surface of the pressurizer wall.

The steam generator model determines the rate of heat removal from the primary loop to the secondary loop water flow, and the flow rate to the turbine for electricity generation[5]. It calculates the internal water level and the exit steam quality at steady state and following an operation transient, e.g., due to a change in the load demand. The performance of the reactor coolant pumps connected to the primary loop cold legs is determined using homologous pump curves. They are coupled to the overall momentum and energy balance equations of the primary loop to calculate the pump pressure head and coolant flow rate.

The PWR nuclear plant model in Simulink is linked to emulation models of the digital components within the plant's I&C system. The calculated state variable values by the physics-based models of the plant components are communicated to the inputs of the digital I&C system components, representing sensor measurements. An emulated representative I&C system architecture is being developed for a reactor safety and protection system to help demonstrative the NICSim platform. This representative I&C system includes autonomous reactor trip[6] and engineered safety features actuation functions. Additional PLCs within the digital I&C system are developed for the autonomous control of the plant.[4,5] Each PLC is emulated using a virtual machine with the open-source OpenPLC software running its control logic program[3]. The OpenPLC software runs IEC 61131-3 standard PLC programming languages and communicates using the Modbus ICS communication protocol.

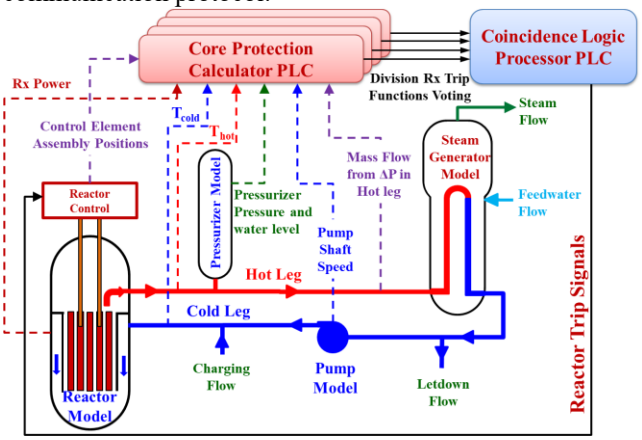

Fig. 2. Block diagram of the digital reactor safety I&C system for the reactor trip function.

Figure 2 presents a functional diagram of a representative autonomous reactor trip function in the plant protection system. The Core Protection Calculator (CPC) PLC receives state variables from the various plant component models and calculates key safety parameters.[7] These include the critical heat flux ratio and the margin to the saturation temperature of the water coolant in the hot leg. The CPC PLC compares these parameters to safety setpoints and, if exceeded, votes to trip the reactor. The voting signals of four independent CPC PLCs are combined in a Coincidence Logic Processor PLC. At least 2/4 of the PLCs need to vote trip before sending a reactor trip signal.

In addition to the PLCs of the plant protection system, the representative I&C system architecture in the NICSim platform includes PLCs for the autonomous operation of the components within the reactor primary loop (Fig. 3). These are the reactor power regulation PLC, the pressurizer pressure control PLC, the pressurizer water level control PLC, and the steam generator feedwater control PLC (Fig. 3). These PLCs receive the calculated state variables by the physics-based models of these components and send signals back to the integrated plant model.

The representative emulated nuclear power plant I&C system emulates the PLCs' operating system kernel and control software, and communicate using the same ICS communication protocols. Representing digital I&C components with high fidelity emulation would make it possible to investigate cyber-attacks targeting PLCs' programming and network communication. A PLC emulation methodology is developed to characterize the key

physical and digital signatures and validate them against those of an emulated PLC. Validation testing within this emulation methodology determines the settings required to ensure that of the emulated PLCs replicate the performance and network traffic behavior of the physical devices.

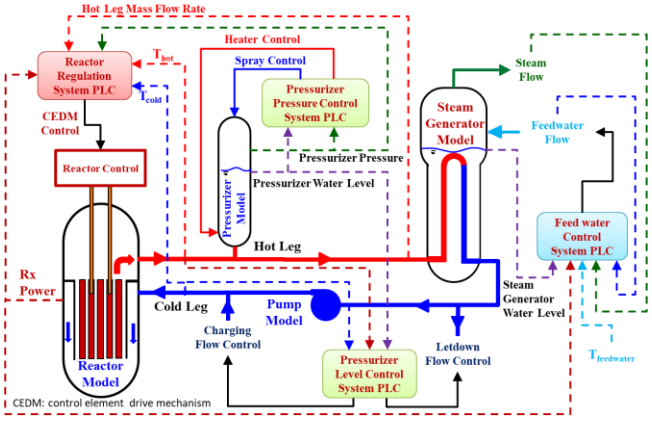

Fig. 3. A block diagram of a PWR primary loop with the operational I&C system programmable logic controllers.

The NICSim platform employs an efficient and fast-running data transfer interface for linking the Simulink physics-based transient model of the PWR power plant to the emulated ICS components (Fig. 3)[3]. The data transfer interface uses Modbus over a TCP/IP network connection to communicate with the emulated PLC's input and output signal register values. The state variables calculated by the physics-based PWR plant model are communicated to an external python interface using shared memory inter-process communication within a developed Matlab S-function[2]. The calculated state variables are written and read from a shared memory location named 'publish' (Fig. 4).

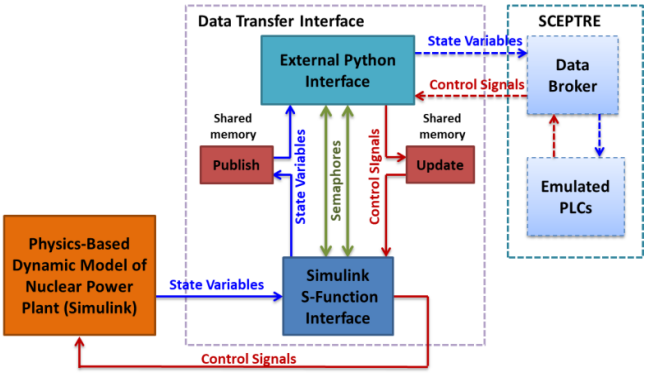

Fig. 4. Developed and validated data transfer interface for linking Simulink to external PLCs.[3]

The determined values of the control signals by emulated PLCs are communicated back to the Simulink model through a second shared memory location named 'update' (Fig. 4). Inter-process communication semaphores control access to the two shared memory locations, and ensure timely, reliable communication (Fig. 4). The data transfer interface can also be used to synchronize the timing of the Simulink PWR plant model with that of the PLCs. Example of the results of the behavior of the emulated PLCs, which are linked to the various components of the PWR plant simulation model components using this data transfer interface, are presented in companion papers in these proceedings[4,5,6].

The NICSim platform would provide a next-generation capability for investigating cybersecurity of digital I&C systems in nuclear plants. Once completed, it could be used by cybersecurity researchers to investigate and analyze risks to existing I&C systems as well as evaluate the resilience and vulnerabilities of proposed systems' upgrades. It could also assist the development of cybersecurity protective measures in next generation digital I&C systems, and test the effectiveness of different cyber-defense strategies against real malicious attack programs.

ACKNOWLEDGEMENT

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. SANDIA NATIONAL LABORATORIES, "SCEPTRE," SAND2016-8095C, Sandia National Laboratories (2016).
2. MATHWORKS, Matlab Simulink ver. 2019b, (2019)
3. 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
4. R. ALTAMIMI, M. EL-GENK, T. SCHRIENER, "Pressurizer Model and PLCs for Investigation of Cybersecurity of PWR Plants." Trans. ANS 2020, Phoenix, AZ, June 7-11, 2020.
5. T. M. SCHRIENER, M. S. EL-GENK, "Steam Generator Controller for Cybersecurity Analyses of Digital I&C Systems in PWR Plants." Trans. ANS 2020, Phoenix, AZ, June 7-11, 2020.
6. M. S. El-Genk, J.-M. Tournier, "A Point Kinetics Model and Dynamic Simulation of Next Generation Nuclear Reactor," J. Progress in Nuclear Energy, **92**, 91-103 (2016).
7. A. HAHN, M. S. EL-GENK, T. M. SCHRIENER, "Programmable Logic Controller of a Pressurized Water Reactor Core Protection Calculator." Trans. ANS 2020, Phoenix, AZ, June 7-11, 2020.