SAND2021-2659C

AUTOMATED CYBER SECURITY TESTING PLATFORM FOR INDUSTRIAL CONTROL SYSTEMS

Andrew Hahn, Daniel R. Sandoval, Raymond E. Fasano, Christopher Lamb
Sandia National Laboratories
PO Box 5800 MS 0748
Albuquerque, NM 87185-0748
ashahn@sandia.gov; drsando@sandia.gov; refasan@sandia.gov; cclamb@sandia.gov

[Digital Object Identifier (DOI) placeholder]

ABSTRACT

Nuclear Power Plants (NPPs) are a complex system of coupled physics controlled by a network of Programmable Logic Controllers (PLCs). These PLCs communicate process data across the network to coordinate control actions with each other and inform the operators of process variables and control decisions. Networking the PLCs allows more effective process control and provides the operator more information which results in more efficient plant operation. This interconnectivity creates new security issues, as operators have more access to the plant controls, so will bad actors.

As plant networks become more digitized and encompass more sophisticated controllers, the network surface exposed to cyber interference grows. Understanding the dynamics of these coupled systems of physics, control logic, and network communications is critical to their protection. The research into the cybersecurity of the Operational Technologies of NPPs is developing and requires a platform that can allow high fidelity physics simulations to interact with digital networks of controllers. This will require three main components: a network simulation environment, a physics simulator, and virtual PLCs (vPLC) that represent typical industry hardware. A platform that incorporates these three components to provide the most accurate representation of actual NPP networks and controllers is developed in this paper.

Key Words: cybersecurity, simulation, emulation, PLC, network

1 INTRODUCTION

Industrial Control Systems (ICSs) are complex networks that interface with and control physical systems. Too often the control systems, the network, and the physics they control are treated as separate systems. In reality, network communications, controllers, and the physics of the process are highly coupled. Disturbing one will likely affect the others. This is especially true in diverse, complex networks of controllers governing a correspondingly complex system of coupled physics like those in nuclear power plants (NPPs). Understanding the full dynamics of such systems cannot be done with isolated analysis. All the system states that could lead to damage or dangerous conditions cannot be identified without considering the interactions of the whole system. This holistic approach to investigating the interrelated systems of physics, controllers, and networks of NPPs is a critical and novel area of research.

Currently, the methods used to analyze the cybersecurity, performance, and safety of industrial control systems only consider pieces of the whole system. There is no equivalent research that marries the simulations of plant networks with the high-fidelity controllers and physics of the NPP system. Additionally, the typical cybersecurity analysis does not take the time domain into account. When and in what sequence the communications between the Programmable Logic Controllers (PLCs) are manipulated can drastically change the effect on plant conditions. Adding a temporal aspect to the existing variables exponentially increases the fidelity of scenarios needed to perform more impactful research. This added time dimension significantly increases computational demands and calls for automated scenario generation, execution, iteration, and evaluation. This work is novel because it unites the emulation of networks and controllers with high fidelity physics simulations in an environment that enables automated scenario evaluation.

In this paper, we will show how a simulation platform and automated evaluation system were developed to analyze the complex dynamics of time-dependent control system manipulations. This paper will document how the research platform was created using the Sandia developed SCEPTRE emulation suite to recreate the control network of a nuclear power plant, coupled with the Asherah hypothetical Pressurized Water Reactor simulator and Siemens virtual PLCs [1][2]. The SCEPTRE platform enables the simulation of multi-node tiered networks by emulating network components (switches, firewalls, access points) and the connections between them. The virtual PLCs (vPLCs) allow implementation of dynamic control logic that responds as physical conditions change in the plant. This dynamic virtual analysis can be scaled to mimic an entire plant control structure and in addition hardware PLCs can be added in the loop to validate real PLC performance for commissioning.

With this platform, we can evaluate the cybersecurity, performance, and safety of NPPs at an unprecedented level. The full dynamics of control system actions originated from malicious network communications that cause manipulations of plant conditions can, for the first time, be investigated. We can identify sequences of events that bring NPP systems to dangerous conditions from the interaction of multiple control actions triggered simultaneously and temporally spaced. Not only is it necessary to identify time-dependent unsafe control actions, but it is also important to identify malicious actions that could result in plant damage. Our research will begin to enable more informed control system design and focus cybersecurity efforts on efficient and effective solutions. The outcome of this effort is to inform system and cyber defense design that can reduce the possibility of dangerous events that can evolve from malicious attempts to damage plants.

1.1 Prior Work

The field of NPP simulators intended for cybersecurity investigation has only started to develop recently. The cybersecurity research of Operational Technology (OT) networks has been significantly lacking when compared to Information Technology (IT) networks [3]. NPP OT networks present additional complications as they constitute a complex and coupled control structure and represent a greater public risk.

The simulation tools to evaluate NPP cybersecurity are just being developed and as such few NPP simulators are designed to be integrated with external controllers in the efforts of evaluating cybersecurity. Two are currently identified to be available to the research community.

The Nuclear Instrumentation and Control Simulation (NICSim) platform was developed at the University of New Mexico's Institute for Space and Nuclear Power Studies (UNM-ISNPS) [4]. This platform incorporates a high-fidelity physics model developed in Matlab Simulink with external emulated PLCs. The PLCs are emulated in OpenPLC [5], an open-source PLC software. This platform is limited by the open-source PLCs that are not representative of real plant hardware. Additionally, the structure of the network has not been documented.

The University of Sao Paulo's Asherah Nuclear Power Plant Simulator (ANS) [6] is a physics simulator also based in Matlab Simulink. Asherah is built to support Hardware-in-the-Loop (HIL) integration of physical and emulated PLCs. The platform supports Modbus and OPCUA communication. Asherah has been used with HIL controller and as a physics engine to connect physical experimentation apparatus and PLCs [7][8]. The issue with these approaches is the scalability of using physical hardware. This can enable some experimentation on single control nodes but representing the whole control network becomes difficult and expensive. Expanding this to include the representation and relationship to other networks on site such as the enterprise network is cumbersome. It is important to include these related networks as they are most likely to be an entry point for malicious software.

2 SIMULATION METHODOLOGY

2.1 Network Simulation

The Sandia developed SCEPTRE environment allows the simulation of large-scale networks and their components [9]. SCEPTRE is built upon another Sandia developed Virtual Machine (VM) deployment suite, MiniMega [10]. MiniMega is an open-source tool that allows the generation of virtual networks and the deployment of VMs on that virtual network. SCEPTRE expands on the capabilities of MiniMega and provides more refined environment development controls and better physics integration support. It deploys VMs that are stored on large file servers and then ported to operate on high performance computing servers. The virtual networks are built by reading from storage and then populating into a predesigned virtual network. These designs constitute the network hardware such as switches and routers as well as the controllers, sensors, actuators, and in our case, virtualized PLC's and their control logic, and physics simulators. By using virtual machines, experiments can be duplicated, modified and regenerated as needed and is limited only by the computing resources available.

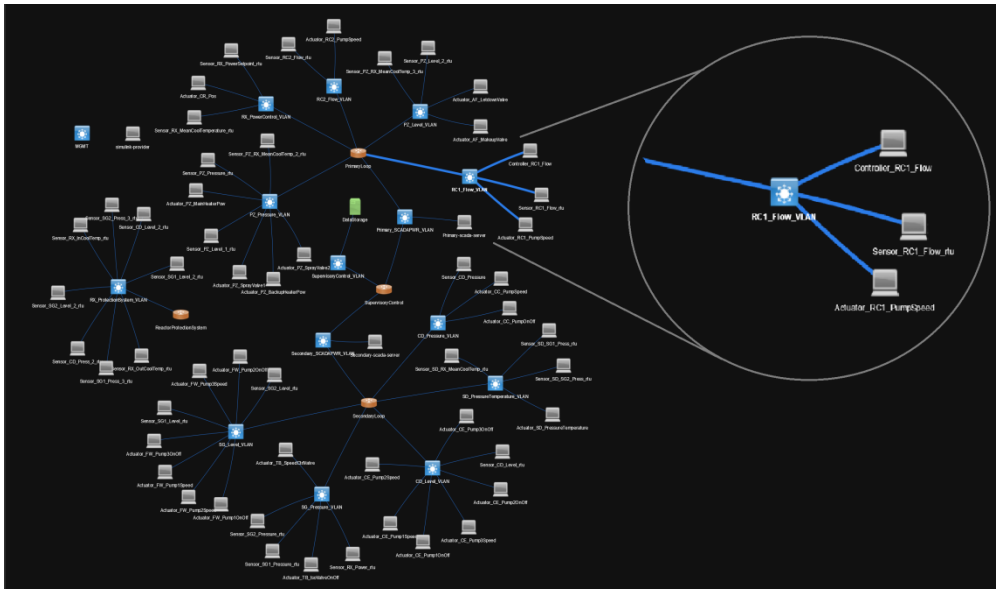

Figure 1. SCEPTRE simulation of Nuclear Power Plant control system network. Current working section is highlighted and enlarged.

The fully simulated NPP control network framework of both the primary and secondary systems is shown in Figure 1. Each grey icon represents a virtual machine. The blue icons are virtual LAN networks, or segmentations of the network that represent different groups of controllers and their sensors and actuators. Highlighted and enlarged is the current fully developed segment that consists of the Reactor Coolant Pump (RCP) vPLC and its sensors and actuators. Though the rest of the network is emulated, currently only this RCP controller and associated sensors and actuators are interacting with the physics simulation.

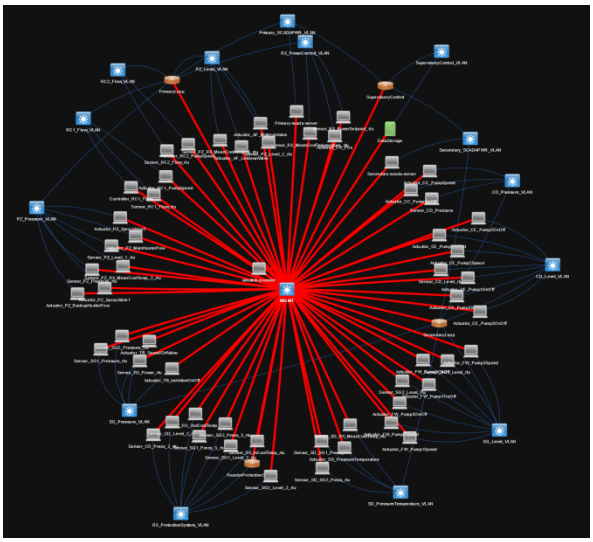

Figure 2. Network map of SCEPTRE simulation of Nuclear Power Plant control system network showing the management network.

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.
Sandia National Laboratories is a multimission 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. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Two networks compromise the SCEPTRE system, the top-level networks and the sub level management network. The top-level networks are comprised of all the plant level networks to be emulated. These are the experimental networks we are interested in monitoring and understanding. The management network is hidden from the top-level experimental system and is responsible for managing the VM operations. Through this network, smart sensors and actuators can communicate to the physics simulation. The management network allows physics values to be passed to the sensors while avoiding passing though the experimental top-level network. The extent of this management network is shown in Figure 2 by red lines.

2.2 Physics Simulator Integration

The physics are simulated by the Asherah Nuclear Power Plant Simulator (ANS) [6]. Sensor signals and control signals are routed via the management network to VMs of smart sensors and actuators. Asherah provides a high-fidelity physics simulation of a Nuclear Power Plant for the network and controllers to interact with. The controllers within the Simulink model provide a template of the vPLCs to be later created on our network. As vPLCs are programmed, the controllers in the Simulink model are commented out and the emulated PLCs take over. Figure 3 provides visual reference for how the Asherah NPP Simulator is positioned within the SCEPTRE simulation of the plant control network.

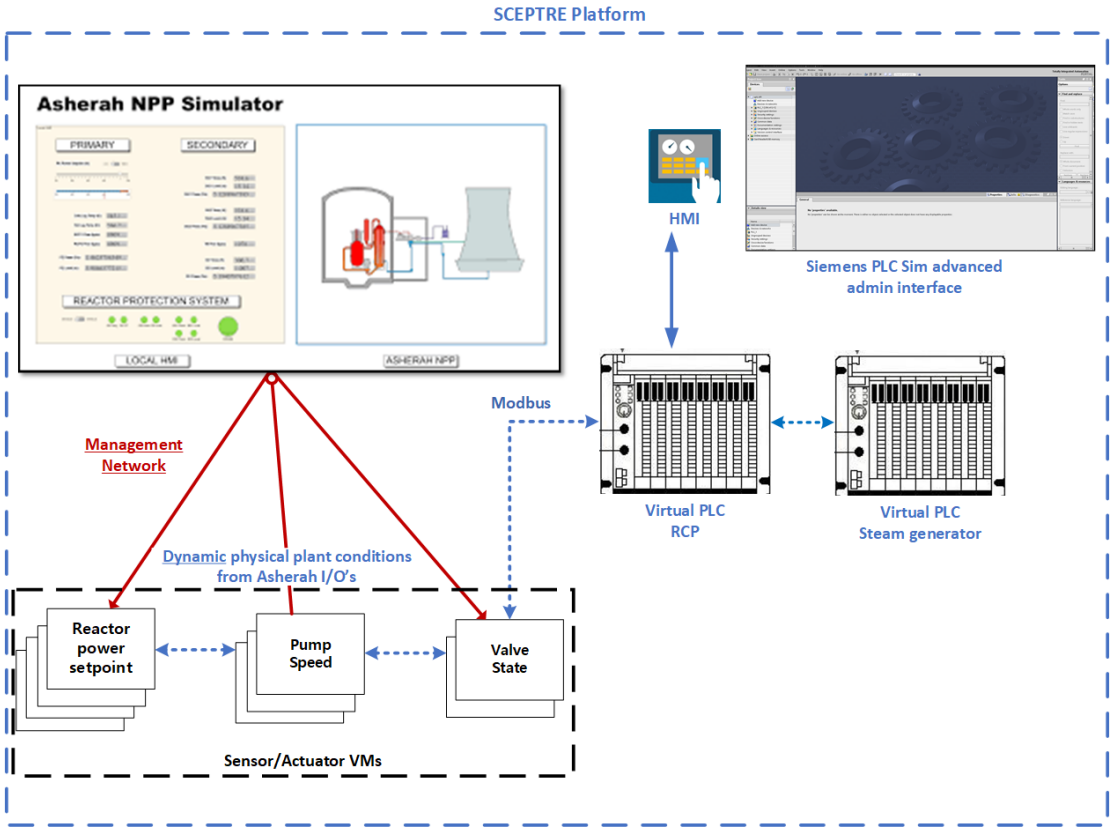

Figure 3. Asherah Nuclear Power Plant Simulator I/O communications within SCEPTRE.

To facilitate the communication from the Asherah model to the virtual sensors and actuators it was necessary to modify the Asherah model. The Asherah Simulink model was compiled to an executable and the variable tags associated with sensor and actuator values were linked to a separate program. This allows the management network to access and change these model process variables. To properly access these variables, sensor and actuator programs were developed that interface with the management network and communicate these via Modbus to the PLCs. These sensor and actuator programs can be easily modified to adapt the system to use other communication protocols to investigate the cybersecurity of the system using protocols such as OPCUA.

2.3 Emulating Programmable Logic Controllers

Programmable Logic Controllers are somewhat difficult to fully emulate currently. Few manufactures of hardware that would be found in a real plant have dedicated the effort to develop emulations of their products. Emulation of hardware that is dependent on the accuracy of time measurement is a difficult task on modern computers. Siemens offers the PLCSIM Advanced emulation software which allows Siemens S7-1500 PLCs to be virtually emulated [11]. High fidelity emulations of PLCs can be run from Windows 10 VMs and provides accurate virtual representations of real PLC hardware.

The Siemens PLCSIM Advanced software presents some challenges to overcome for utilization in the NPP simulation. Since the experimental platform has no internet connection, license management becomes difficult. Offline licenses can be generated, but the license management software will still attempt to contact the Siemens license server. Offline licenses that initially indicate an unlimited license period will sometimes expire on the experiment and require pulling the VM off of experimental servers and rechecking out the licenses locally. The cause of this is unknown, and mitigation strategies are being investigated.

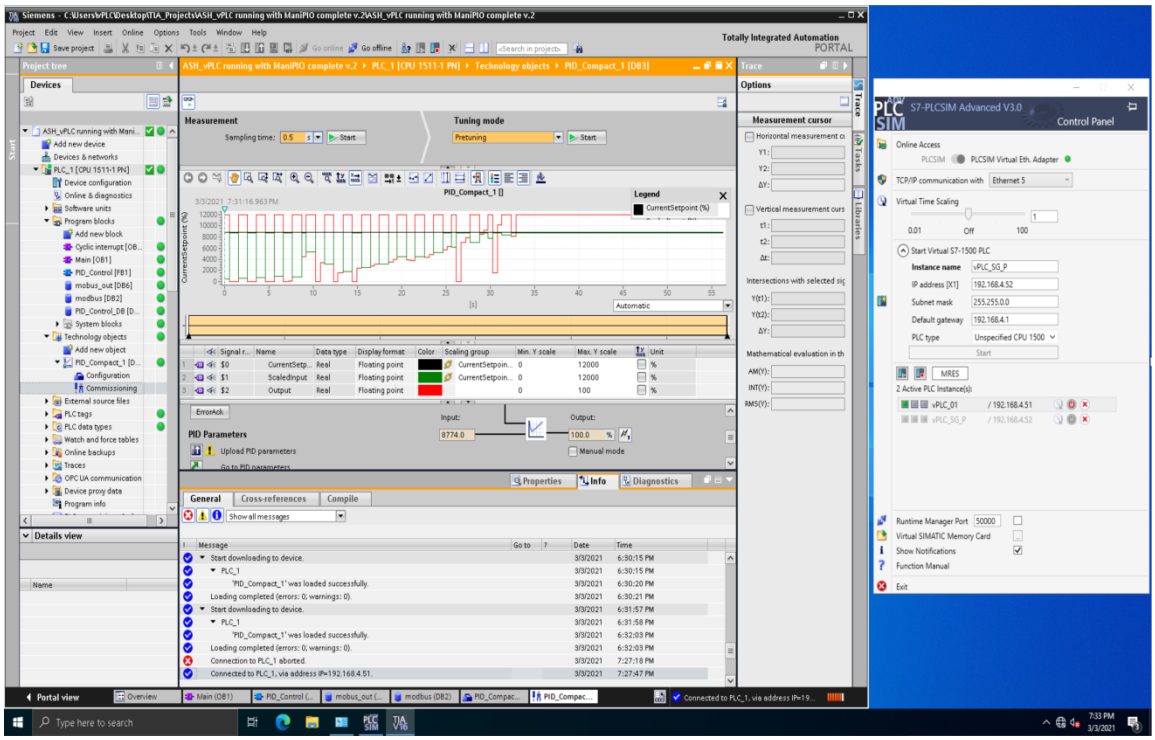

Figure 4. Windows 10 VM running a Siemens virtual PLC connected to the Asherah NPP Simulator. The PLC is controlling the reactor coolant pump and is showing a successful tuning of PID process control.

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.
Sandia National Laboratories is a multimission 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. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Modbus is the primary Industrial Control System (ICS) communication protocol for this simulation which provides additional complications. Siemens vPLCs have the ability to communicate over Modbus by including Modbus server blocks in the ladder logic. These blocks allow Modbus clients to connect to the vPLC and read or write values. Typically, Modbus servers allow multiple clients to connect simultaneously, the Siemens Modbus server blocks only allow one client connection at any time. Instantiating multiple Modbus server blocks allows multiple client connections, but each server must have a unique port. Modbus communications are designated as using port 502 [12]. To mitigate the limitations of the Siemens PLC Modbus blocks, additional client connections are routed to ports 503, 504, 505 + [number of clients]. This non-standard port specification may create future issues with Modbus components that only allow communication on port 502 as specified in the Modbus standard.

After mitigating the issues with the Siemens Modbus servers and while the license remains stable, the simulation successfully connected to and controlled the RCP in the Asherah Simulation. Figure 4 shows the virtual PLC running in the Siemens PLCSIM Advanced program on the right. TIA Portal, Siemens PLC programming software, is running on the left showing the tuning application on the Proportional Integral Derivative (PID). The PID tuning has successfully optimized the operation of RCP as it would if connected to a real physical process. This groundbreaking virtual dynamic physical process interacting with a virtual dynamic control process is a critical stepping point in our research.

3 EXPERIMENTAL SETUP

The entire simulation platform is run by a single node on a local High-Performance Computing (HPC) center. The node has two Intel Xeon E5-2683v4 32 core processors, and 512 Gb of ram. This allows the 62 VMs in the topology to be emulated while utilizing only 57 Gb of the available memory. The VM images are stored on a data storage server and loaded into memory on the compute node. The SCEPTRE environment requires only 3 images to build this experiment, a generic Linux based image, the Windows VM for the Siemens vPLC emulators, and a Linux based data collection image. The generic Linux image can be used for all the sensors and actuators, the SCEPTRE system injects files and scripts that automatically setup these images to be the appropriate sensor or actuator they represent. This efficiently streamlines resource utilization and experiment initiation.

4 EMULATION PROOF OF CONCEPT

The simulation network shown in Figure 1 consists of a total of 62 VMs: 27 sensor VMs, 26 actuator VMs, 4 router VMs, 2 SCADA server VMs, a historian server VM, the Asherah Simulator VM, and the Siemens PLC VM. These constitute the devices across the primary and secondary coolant loops of the NPP simulator and are segregated into virtual LANs (VLANs) that represent each subsystem. The 12 VLANs separate out the individual process control systems, such as the pressurizer control group, on to their own subnets [Figure 5]. These VLANs are connected to the router VMs that connect the networks of each side of the coolant loop, primary and secondary. The primary and secondary coolant loop control networks are temporarily connected to each other through a separate router to allow the historian to record both sides. The reactor safety system network is instantiated as a separate network with its own router isolated from the rest of the control network. This whole network of VMs is operational and communicating across the virtualized ethernet connections. Only the remaining PLC emulations are required to complete a fully functional control system network. The one controller that is fully implemented provides proof that the system will function as intended.

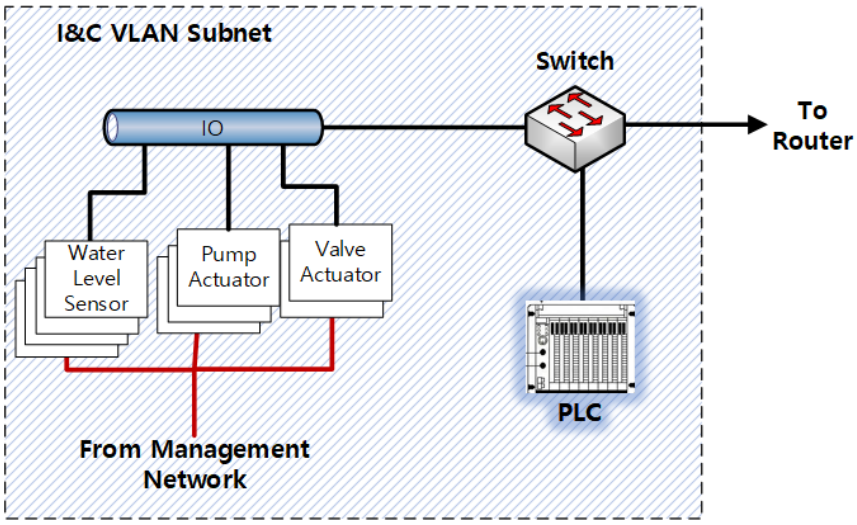

Figure 5. VLAN Node with controller and sensor/actuator group within a subnet.

Currently one VLAN subnet has been completed with an emulated PLC, the Reactor Coolant Pump (RCP) controller. As seen in Figure 4, the Siemens virtual PLC is connected to the Asherah Simulator and controlling the RCP. This vPLC is connected to Siemens TIA portal and has been tuned to the process it is controlling. As far as the Siemens TIA portal is concerned it is connected to a physical PLC that is controlling a physical process. Using industry standard PLC tools with high-fidelity emulations running actual firmware from physical PLCs is significant to the efforts of simulating these control networks. This happens within a large-scale simulation of the NPP control network that is reproducible, scalable, and enables iterative and parallel investigation of the dynamics of these systems. To the NPP physics simulation and the network, this platform is indistinguishable from a physical Hardware-in-the-Loop controller.

5 FUTURE WORK

Developing the single controller network in the SCEPTRE suite with the Siemens virtual PLC operating with the Asherah NPP Simulator lays the groundwork to complete the entire NPP control network. License issues and Modbus communications present complications that are being investigated and will be resolved. The next system to be completed is the steam generator pressure control network. The Asherah internal controllers will incrementally be replaced with high fidelity vPLCs. Relationships with other vPLC vendors are being developed to explore product diverse multivendor control networks. After the controller network includes more systems, complex interference on these networks will be investigated.

6 CONCLUSIONS

This work presents the current development of a platform to evaluate the coupled nature of NPP physics, controllers, and the control network. This network simulation is limited to a single controller, but this will quickly expand to the whole system. This will allow experimentation on a full NPP control system network. The virtual nature of this platform allows safe, relatively inexpensive, and repeatable experimentation, culminating in the ability to perform highly iterative experimentation to discover the underlying dynamics of these coupled systems. Using industry developed emulations of PLCs, high fidelity simulations of networks, and advanced physics simulations enables the most accurate and complete representation of Nuclear Power Plant control system networks.

7 REFERENCES

1. Sandia National Laboratories, *SCEPTRE*, SAND2016-8095C, Albuquerque, NM (2016).
2. R. A. Busquimesilva, D. A. Correa, F. R. Antunes, F.C. S. Souza, J. R. C. Piqueira, R. P. Marques, "The Asherah Nuclear Power Plant Simulator (ANS) as a Training Tool at the Brazilian Cyber Guardian Exercise," *IAEA*, (2020).
3. Seungmin Kim, Gyunyoung Heoa, Enrico Zioa, Jinsoo Shinc, Jae-gu Song, "Cyber-attack taxonomy for digital environment in nuclear powerplants," *Nuclear Engineering and Technology*, **52**, pp.995-1001 (2020).
4. Mohamed S. El-Genk, Timothy Schriener, Andrew Hahn, Ragai Altamimi, "A Physics-based, Dynamic Model of a Pressurized Water Reactor Plant with Programmable Logic Controllers for Cybersecurity Applications," *DOE-NEUP Project Report* (2020).
5. T. R. Alves, M. Buratto, F. M. de Souza, T. V. Rodrigues, "OpenPLC: An open source alternative to automation," *IEEE Global Humanitarian Technology Conference (GHTC 2014),* San Jose, CA, USA, 2014, pp. 585-589, doi: 10.1109/GHTC.2014.6970342
6. Silva, RA BUSQUIM E., Koroush Shirvan, José Roberto Castilho Piqueira, Ricardo Paulino Marques. "Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment." *International Conference on Nuclear Security (ICONS),* 10-14 Feb 2020, Vienna Austria. 2020.
7. Song, Jae-Gu, Jung-Woon Lee, Cheol-Kwon Lee, Chan-Young Lee, Jin-soo Shin, In-koo Hwang, Jong-gyun Choi. "Development of Hardware In the Loop System for Cyber Security Training in Nuclear Power Plants." *Journal of The Korea Institute of Information Security & Cryptology 29*, Vol. 4 (2019): 867-875.
8. Chanyoung Lee, Cheol Kwon Lee, Jong Gyun Choi, Poong Hyun Seong, "Development of a Demonstrable Nuclear Cyber Security Test-Bed and Application Plans," *Korean Nuclear Society Spring Meeting*, Jeju, Korea, May 23-24, 2019.
9. Nicholas Joacobs, Jay Johnson, *SCEPTRE: Power System and Networking Co-Simulation Environment*, SAND2018-5328PE, Albuquerque, NM (2018).
10. Jonathan Crussell, Jeremy Erickson, David Fritz, John Floren. *minimega v. 3.0*. Report No. 004619MLTPL00. Sandia National Laboratories Albuquerque, NM, 2015.
11. Siemens, *PLCSIM Advanced V3.0*, (2021).
12. International Electrotechnical Commission, *IEC 62453-315*, Geneva, Switzerland (2009).