SAND2022-7654C

NPP Simulator Platform for Cyber Security Research and Training

Michael T. Rowland
Sandia National Laboratories

Andrew Hahn
Sandia National Laboratories

Ricardo Paulino Marques
University of Sao Paulo

Nichole White
Oak Ridge National

Christopher Spirito
Idaho National Laboratory

ABSTRACT

Department of Energy's Office of International Nuclear Security (INS) aims to expand cybersecurity capacity internationally by establishing sustainable training programs for cybersecurity of nuclear facilities through support for curriculum development and instructor training. To further this goal, INS has partnered with University of Sao Paulo (USP) Brazil to develop hands-on cybersecurity training for nuclear professionals and engineering students.

The lack of internationally available and low-cost nuclear power plant (NPP) emulation platforms to support cybersecurity research and training for NPPs has adversely impacted the progress of the domain. To address this challenge, the International Atomic Energy Agency (IAEA) commenced a coordinated research project (CRP) in 2016 that led to the development of the hypothetical Asherah Pressurized Water Reactor Simulator.

The Asherah NPP Simulator is a mature cybersecurity simulator developed by USP along with CRP collaborators from 17 organizations and 13 countries. Asherah was designed to function as a cybersecurity testbed with a critical feature of allowing real field equipment to be interfaced with the simulator (i.e., hardware-in-the-loop). Asherah provides a sophisticated platform that can support advanced training (e.g., undergraduate and post-graduate university courses) as well as research. The IAEA is committed to freely providing the simulator to organizations within IAEA Member States, upon request.

However, given the sophistication of the simulator, many organizations in newcomer NPP countries cannot support establishment, maintenance, and delivery of training using an on-premises installation of Asherah. This challenge has been addressed by the collaborative efforts of USP, Sandia National Laboratories, Oak Ridge National Laboratory, and Idaho National Laboratory through INS in the development of open-source software packages that simplify establishment, maintenance and use of Asherah for research and training in resource constrained settings. This paper discusses the development and application of the Asherah NPP Simulator Platform (ANSP) to advance international research and training in cybersecurity. ANSP will be used to train the current and future generation of cybersecurity professionals in Brazil and other international partners.

INTRODUCTION

"Modern Critical Information Infrastructure (CII) are increasingly dependent on the integration of digital technologies to provide functions that either autonomously or automatically control physical processes. Digital technologies that perform functions that control physical processes are generally categorized as Operational Technology (OT). A concurrent trend is the increased adoption of commercial of the shelf (COTS) Information Communications Technology (ICT) into OT systems. Whereas OT systems were once very customized and unique applications of digital technology, modern OT systems are an integration of COTS, ICT, and custom components. This integration has brought many advantages commensurate with leveraging the performance, economic, and interoperability gains of COTS and ICT equipment, however, it exposes modern OT systems to elements of common ICT attacks[1-3]. The potential consequences of a cyber-attack on an OT system extend beyond those consequences associated with cyber-attacks targeting traditional information and communications technology (ICT) environments[4]."[5]

To adequately face the challenges of cyber attacks on OT system requires continued education, training, and research. Greater understanding of protection and mitigation methodologies, as well as workforce training needs to be developed to build the knowledge base and preparedness to respond to cyber-attacks. The rapid pace of cyber attack development demands an agile and timely response from cyber defense research and training. OT cyber security is hampered by slow progress as each research and education entity is forced to assemble their own bespoke platforms to even begin the development of research. There is a great need for an accessible solution, especially within organizations and countries that cannot afford to develop these platforms.

This simulation platform seeks to answer the needs of a nuclear power plant cyber security platform for training, education, and research. All the tools and components discussed are freely available and intended to accelerate the advancement of the OT cyber security community. With less focus on the development of the basic tools, researchers and educators can focus on building solutions rather than develop platforms. Four components are presented that create a full simulation of a nuclear power plant, its control network, and a cyber-attack simulator.

Physics Engine

At the center of the platform is the Asherah Nuclear Simulator (ANS) a dynamic, MATLAB/Simulink based, real time simulation of a Nuclear Power Plant (NPP) that has a strong likeness to (but not identical) Three Mile Island Unit 1 Pressurized Water Reactor (PWR) [6]. Asherah provides the physics of an NPP to the platform as well as internal control logic which we can base our external controller's logic. Alone, a Simulink simulation cannot provide the necessary network communications to drive external Programmable Logic Controllers (PLCs). To drive these network communications to the PLCs requires additional programs external to Simulink that can properly handle communications between many Operational Technology (OT) networks and controllers. Asherah does this through various modules that export control parameters via network communication pathways to external servers. Sandia sought to improve on this strategy and streamline the setup of the control system network with the OT Emulation Data Broker[7].

Asherah was developed by USP under IAEA CRP J02008, and is available on Member State Request to the IAEA.

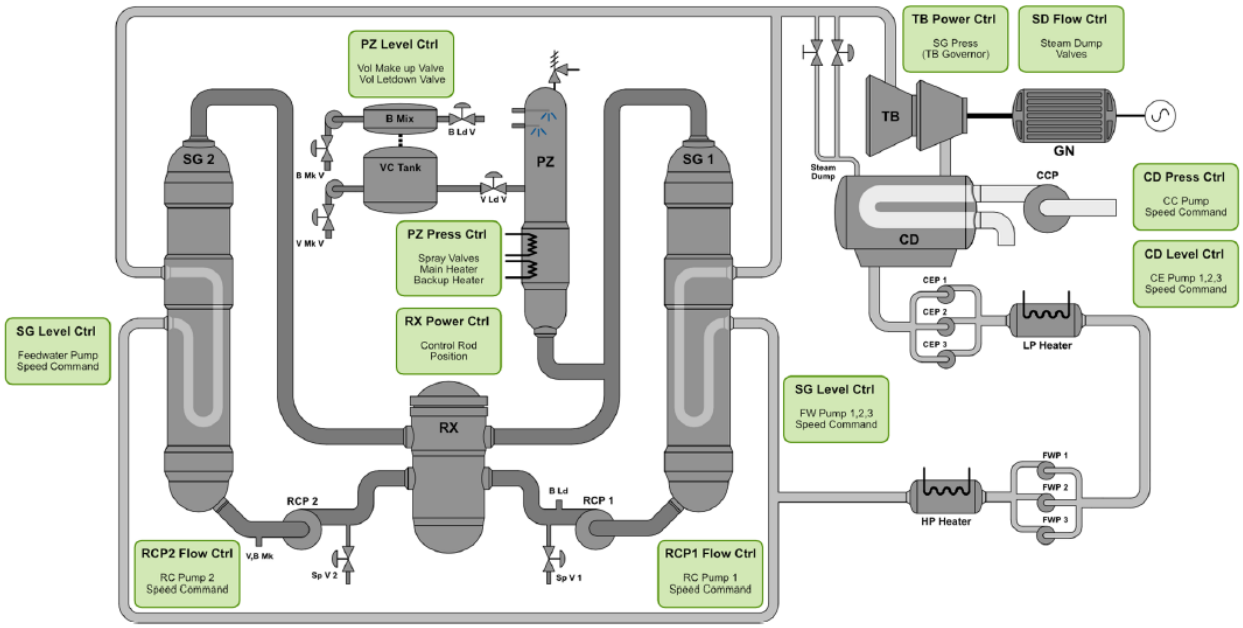

Figure 1: Basic diagram of the Asherah nuclear power plant simulator (ANS).[8]

Data Broker

The driving principles of the Data Broker system are modularity, flexibility, and centralized simulation control. It consists of three major components illustrated in Figure 2, the S-Function, Data Broker, and Endpoints. Each of which communicated in standardized methods, and contain modularly structured code, making each component and function exchangeable. A major advantage the system provides is the ability to compile the Simulink model into an executable and retain the data interface and simulation control that the Data Broker provides. This removes the need for Simulink to be present with the simulation, allowing the model to be run on any machine without the overhead of Simulink. This greatly reduces the computational and economic cost of running the simulator.

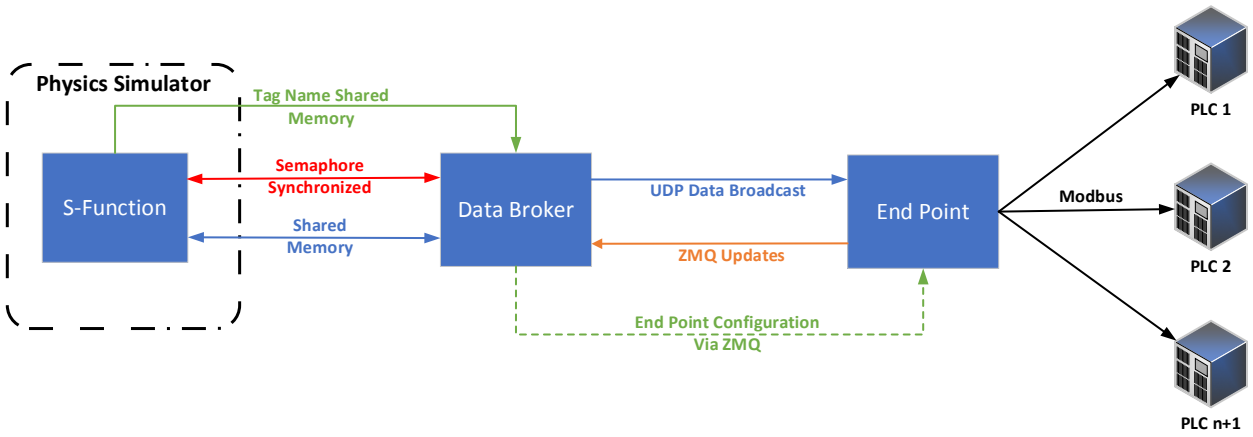

Figure 2: Sandia National Labs OT Emulation Data Broker functional schematic.

Starting at the source of physics data, the S-Function resides in a Simulink simulation. S-Functions are a Simulink method to incorporate custom C code into models, which require a very particular structure to interface with the time dependent equation solver. This allows the custom Sandia developed low latency interface using shared memory and synchronization semaphores to be integrated into any Simulink model. The S-Function generates three shared memory locations for initialization data, input data, and output data. The shared memory locations are latched on to by the external Data Broker Program.

The Data Broker is the multithreaded central processor for system which handles controlling the simulation, real time synchronization, Endpoint setup, and network communications. A user writable JSON configuration file instructs the Data Broker which executable to control or to connect to Simulink and how to set up the Endpoints. Using UDP the system broadcasts ground truth physics values every simulation timestep, initial setup information and actuation signals are exchanged via ZeroMQ (ZMQ). This allows a low latency network solution to allow the Endpoints to have the most up to date physics values and be able to return actuation values to the Data Broker in a timely manner.

The Endpoints are the agents responsible for handling communications with the actual PLCs or control system network. Based in python, they provide a modular platform to build communication methods that fit with to the needs of the control network being emulated. Currently the Endpoints use Modbus/TCP to communicate with the control system and were recently updated to enable multithreading allowing connections to numerous devices simultaneously. Though a single Endpoint can now handle the entirety of the Asherah platforms current allocation of PLCs, multiple Endpoints enable unique capabilities. Distributing communications responsibilities across multiple Endpoints allows integration into complex and diverse networks with many communication standards and hardware-in-the-loop (HITL) while also reducing computational load on the simulation machine.

The DataBroker, Endpoints, and logic files are available on the Sandia SMARTT GitHub repository.

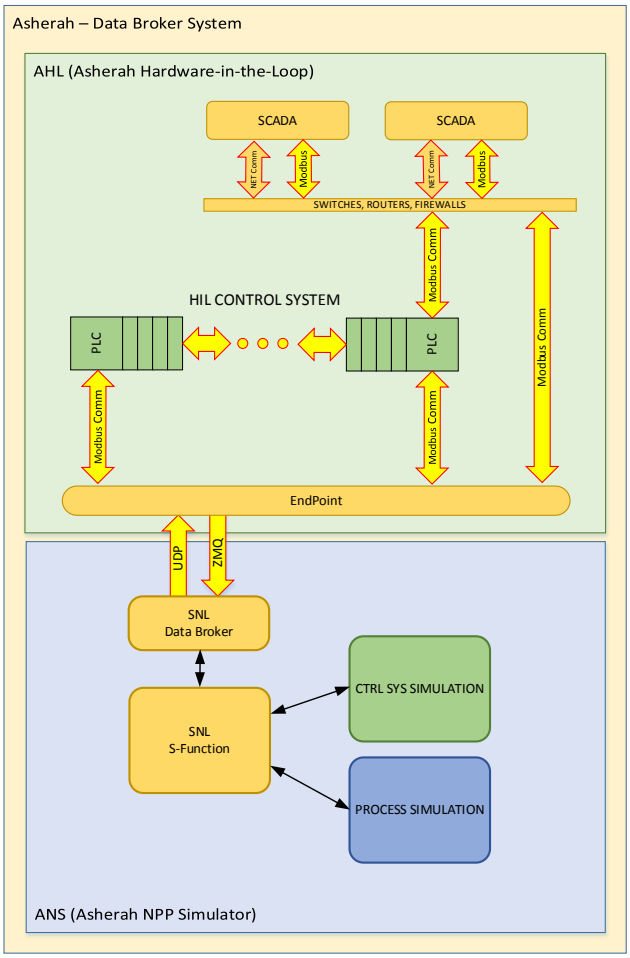

Figure 3: Asherah integration with SNL Data Broker system.

Integrating the Data Broker into Asherah extends its capability as a platform for emulating the control system of an NPP. Shown in Figure 3, the Data Broker takes control of the internal simulated PLCs in Asherah and allows on the fly automatic switching between internal and external control. In this manner the entire I/O for the simulation can be broken out to the external interface, but only switched to external control when needed eliminating the need to recompile the simulation executable for every change in the control network. For flexible and automatic instantiation of control network emulations, this feature is critical. Together the Data Broker and Asherah form a highly flexible physics engine for an emulated NPP control system, but they require a network and machines to operate on.

Network Emulation

The Asherah Data Broker system is network agnostic, it will run on physical or virtual networks alike, but cybersecurity training and research require both. For cybersecurity training in a classroom, it is more practical to have a fully virtual network, in live training exercises it may be highly advantageous to have HITL. Cyber security research will have similar demands. The solution is a blended network with a network emulator that can facilitate both. MiniMega[9] was the primary candidate for the platform as it allowed this blended network and is opensource and freely available.

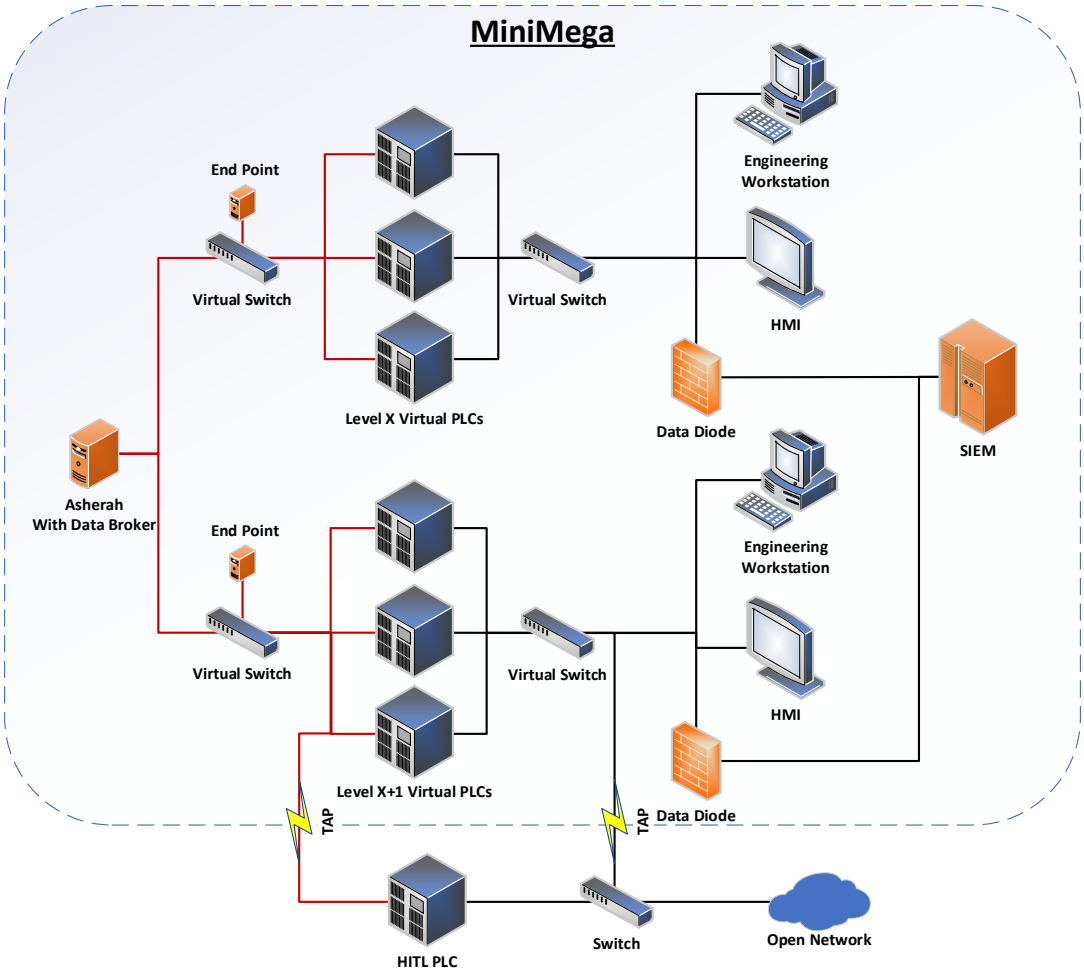

Figure 4: Asherah Data Broker blended network emulation in MiniMega.

With a blended physical and virtual network, the platform can accommodate all manner of research and training. The network shown in Figure 4 can be though to have a permeable barrier between the virtual and physical. Any device and network in the virtual can be tapped out to a physical environment and vice versa. At the core of this capability is MiniMega, which allows the emulation of networks, the machines in those networks, and allows those networks and Virtual Machines (VMs) to be linked to the physical network hardware of the machine they are emulated on.

Coordinating the instantiation and management of the emulated networks is critical to setting up the environment and scenarios for training and research. MiniMega uses a back-channel communication paths into each of the virtual machine through a command and control system, miniplumber[10]. This allows automatic setup and configuration of network devices and virtual machines. By using generalized VM images and configuring them at boot, a minimal package can be used to automatically assemble the network of the whole plant, or sections of the plant network at the discretion of the user.

Cyber Attack Simulation

A whole NPP network can now be established with the tools thus described but missing is a critical element of a training platform for cyber security, simulated attacks. A safe and repeatable mechanism to simulate a cyber-attack on a control system is required. For this purpose the Manipulate Process I/O[11] (ManiPIO) was developed by Sandia.

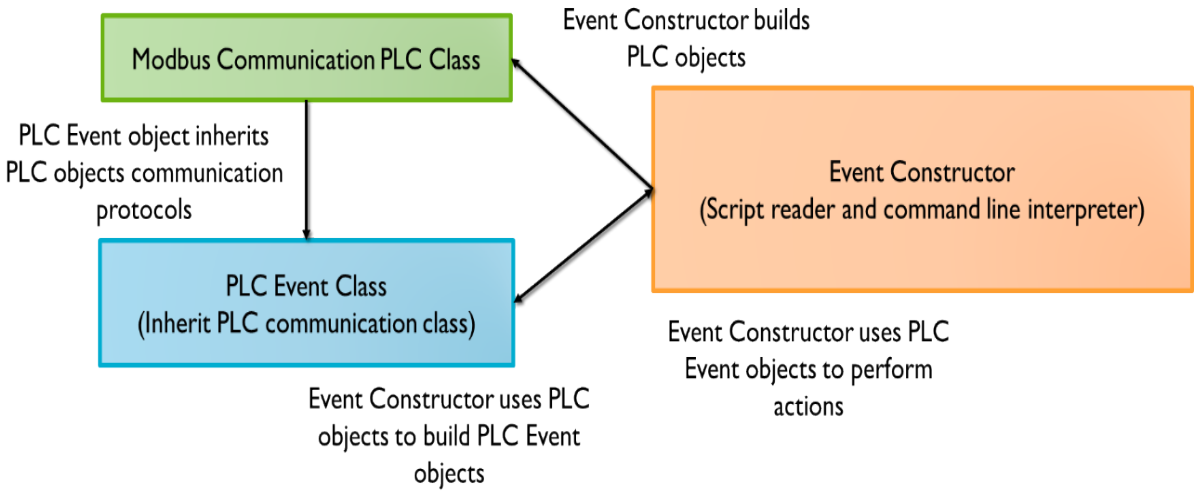

Figure 5: ManiPIO functional block diagram of internal structure.

With ManiPIO, users can setup complex and varied events to take place across the control system network. These events can be timed in sequences or triggered off conditions read from the PLCs. These events and triggers are all configured in human readable input scripts. Like the Data Broker, ManiPIO is highly modular to allow future improvements and shares a component with the previously discussed Endpoint. The Modbus Communication PLC Class depicted in Figure 5 is the same communication class as used in the Endpoint and forms the exemplar of interchangeable communication classes for ManiPIO and the Endpoint. When one is updated to use a new communication protocol, the other inherits it, streamlining future development.

Of concern is the security and safety of providing a cyber attack simulator in a training platform and as an opensource tool which ManiPIO is. Careful consideration was made to ensure that we did not contribute a cyber risk to the world through efforts to educate and reduce cyber risk. By its nature ManiPIO cannot be used as a viable threat, the system requires mechanisms in the PLC logic to allow it to actually change process control information. The program is essentially a packet crafting tool that allows users to make sequences of OT protocol packets as they see fit. For ManiPIO to change anything first requires it to be exposed to the network, and it must also be given a hook in the internal PLC Logic to allow it to change the information in the memory. Otherwise ManiPIO would be in a race condition with the PLC CPU, which over the network is a race it cannot win.

Future Work

The Asherah physics engine, MiniMega network emulation, and ManiPIO cyber-attack simulator form a cyber security training and research platform that is flexible to many applications. Currently this system has use cases in cyber security research on control system networks, as the control system emulation behind cyber security exercises, and as an educational tool in the universities. Though this platform has succeeded in providing valuable tools to the international community of OT cyber security research and education, it has many areas of needed improvement to continue providing critical tools to an underserved sector of cyber security. Analyzing the pros and cons of the components of this system, Table 1, provides context for future developments and outlines a roadmap for improvement.

Component	Pros	Cons
Asherah	• Openly available for IAEA members • Allows collaborative development of an NPP physics and control system simulation • Sophisticated, modular, real-time physics system of full plant. • Continuous development benefits from international community of researchers	• Requires Simulink • Needs complex setup to establish connection to external PLCs • Each OT communication protocol needs a separate system to be developed
Data Broker	• Opensource and freely available • Enables a large and tiered control systems to be connected to the physics of Asherah • Allows scripted control network configuration • Works with compiled and uncompiled Simulink models • Highly modular, easily customizable	• Data Broker and S-Function only work on Linux systems • Difficult initial S-Function integration • Complex configuration file • Only uses Modbus/TCP
MiniMega	• Scalable emulation of networks • Opensource and freely available • Back-channel control and configuration system • Allows bridging internal networks to external physical networks	• Complex configuration scripts • Command line interface
ManiPIO	• Allows complex cyber-attack simulation • Opensource and freely available • Safe, no cyber risk • Highly modular	• Complex configuration scripts • No graphical user interface • Only uses Modbus/TCP

Table 1: Evaluation of pros and cons of simulation platform components.

The future development of the platform will be primarily focused on easing deployment, improving user interfaces, and expanding use cases. Asherah and the Data Broker present the most difficult set up case for the system and have the most requirements to deploy. A containerized Asherah and Data Broker are being developed that will eliminate the complex setup for these components and allow deployment on any operating system. User interfaces to assist configuration of MiniMega, the Data Broker, and ManiPIO will eliminate the hurdle of complex configuration files. New protocols are planned to be developed for ManiPIO and the Data Broker to expand their connectivity and use cases.

CONCLUSIONS

Cyber security will continue to be a constantly evolving concern for the critical infrastructure of the world for the foreseeable future. The cyber security of OT systems is just starting to gather attention, and no single solution exists. Education, training, and continued research on OT cyber security are essential to addressing the safety and security of the most critical and sensitive infrastructure. This platform seeks to reduce the development burden across the community of nuclear cyber security to help focus on the solutions to these complex problems. For this reason, the development of this platform has been committed to providing and utilizing opensource tools whenever possible.

REFFERENCES

1. Case, D. U., Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 2016**,** *388*, 1-29.
2. Lee, R. M.; Assante, M. J.; Conway, T., German steel mill cyber attack. *Industrial Control Systems* 2014**,** *30* (62).
3. Lamb, C. *Advanced Malware and Nuclear Power: Past Present and Future*; Sandia National Lab.(SNL-NM), Albuquerque, NM (United States): 2019.
4. Rowland, M. T.; Maccarone, L. T.; Clark, A. J., Using the Information Harm Triangle to Identify Risk-Informed Cybersecurity Strategies for Instrumentation and Control Systems. *Nuclear Technology* 2022.
5. Rowland, M. T. Investigation of Data Harm and its Relevance to Unsafe Control Actions of Control Systems through Application of the Information Harm Triangle. University of London, To Be Published, 2022.
6. SILVA, R. B. E.; Correa, D.; Antunes, F.; Souza, F.; Piqueira, J.; Marques, R., The Asherah Nuclear Power Plant Simulator (ANS) as a Training Tool at the Brazilian Cyber Guardian Exercise.
7. Hahn, A.; Fasano, R. *OT Emulation Data Broker*; Sandia National Lab.(SNL-NM), Albuquerque, NM (United States): 2021.
8. e Silva, R. B.; Piqueira, J.; Cruz, J.; Marques, R., Cybersecurity Assessment Framework for Digital Interface Between Safety and Security at Nuclear Power Plants. *International Journal of Critical Infrastructure Protection* 2021**,** *34*, 100453.
9. Crussell, J.; Erickson, J.; Fritz, D.; Floren, J. *minimega v. 3.0*; Sandia National Lab.(SNL-NM), Albuquerque, NM (United States): 2015.
10. Fritz, D. J. *Introducing miniplumber*; Sandia National Lab.(SNL-NM), Albuquerque, NM (United States): 2017.
11. Hahn, A. S. *ManiPIO-Manipulate Process I/O for Industrial Control Systems*; Sandia National Lab.(SNL-NM), Albuquerque, NM (United States): 2021.