SAND2023-05081C

Assessment and Experience Using Open-Source NPP Environments for Cyber-Security Training

Andrew Hahn[1*], Michael Rowland[1], Shannon Eggers[2], Christopher C. Lamb[1], Romuald Valme[1]

[1]Sandia National Laboratories, Albuquerque, NM
[2]Idaho National Laboratory, Idaho Falls, ID

[leave space for DOI, which will be inserted by ANS]

ABSTRACT

The use of high-fidelity, real-time physics engines of nuclear power plants in a cyber security training platform is feasible but requires additional research and development. This paper discusses recent developments for cybersecurity training leveraging open-source NPP simulators and network emulation tools. The paper will detail key elements of currently available environments for cybersecurity training. Key elements assessed for each environment are: (i) Management and student user interfaces, (ii) pre-developed baseline and cyber-attack effects, and (iii) capturing student results and performance. Representative and dynamic environments require integration of physics model, network emulation, commercial of the shelf hardware, and technologies that connect these together. Further, orchestration tools for management of the holistic set of models and technologies decrease time in setup and maintenance allow for click to deploy capability.

The paper will describe and discuss the Sandia developed environment and open-source tools that incorporates these technologies with click-to-deploy capability. This environment was deployed for delivery of an undergraduate/graduate course with the University of Sao Paulo, Brazil in July 2022 and has been used to investigate new concepts involving Cyber-STPA analysis. This paper captures the identified future improvements, development activities, and lessons learned from the course.

Keywords: Cybersecurity, opensource, education, advanced reactor, emulation

1. INTRODUCTION

Learning is a constructive process that requires students to interact with and apply knowledge in realistic contexts with authentic tasks [1]. Without experiential and interactive lessons, knowledge cannot be expected to transit from experts to future practitioners. Realistic and interactive environments are essential tools for the education of complex and nuanced subjects. Such educational tools for Operational Technology (OT) cybersecurity are lacking, especially those related to the unique operational environments in the nuclear industry. This gap is further compounded when considering the fidelity, deployability, export controls, and cost.

Simulators for Nuclear Power Plants (NPPs) fall into 2 major categories when evaluated for use in cybersecurity education: insufficient at representing cybersecurity and networking concerns (PCTRAN-Based), or export controlled (GSE, 3KEYSOFTWARE®). While PCTRAN is an excellent teaching and

*ashahn@sandia.gov

training tool for nuclear engineers, it lacks much of the Distributed Control System (DCS) elements that are fundamental to understanding NPP networks. GSE and 3KEYSOFTWARE® offer sophisticated and highly accurate simulations of NPPs and their DCS and are consequently export controlled. International cybersecurity capacity building being core to DOE-INS mission, export control forces a gap in the availability of tools, whereas domestic R&D is a core to the DOE-NE mission in developing and investigating new concepts and approaches for Cyber Informed Engineering.

Asherah fills the gap for an NPP simulator for a more open, realistic, NPP model for cybersecurity education and research [2]. Specifically developed to be a DCS model for cybersecurity research and exempt from export controls and expensive licenses, Asherah provided a unique opportunity to develop an opensource network emulation of an NPP DCS. Asherah is a work-in-progress solution, only providing the physics of the NPP and the I/O to connect it to a DCS. The emulation of the network, controllers, Human Machine Interfaces (HMIs), and student interfaces had to be integrated and developed. This paper documents the progress of the development of a research and educational environment, its deployment in the classroom, lessons learned, and future developments.

2. BENEFITS OF OPENSOURCE

OT cybersecurity is a highly complex issue that has had a significant lack in investment compared to IT cybersecurity. Complex problems require the efforts of many to solve, the multidisciplinary expertise required to address OT cybersecurity is a very scarce resource especially concerning the unique NPP cyber environment. Enabling collaboration is critical to reducing the gap in resources and expertise in a timely manner. Opensource is the most powerful tool to enabling widescale collaboration and rapid exchange and development of knowledge. Time is of the essence as cyberattacks on OT become more complex, sophisticated, and catastrophic. Securing infrastructure around the globe is far more important than copyright interests and mistaken beliefs that cybersecurity information obfuscation protects anything.

It must be acknowledged that the environment described in this paper could not be made possible without opensource tools and software, from which it is entirely constructed. Linux, Python, GCC, QEMU, OpenPLC, Minimega, etc.; all critical components that the environment could not be possible without and are all opensource. It is our responsibility to reciprocate the altruism of those that provided millions of hours of work to enable such lofty ventures. This is compounded by how critical it is that educational tools to rapidly advance NPP and critical infrastructure cybersecurity are accessible.

Access to education is a significant problem, domestically and abroad. Expensive or cumbersome licenses, expensive hardware and computational resources should not be barriers to entry if alternative paths exist. Socio-economic factors should not bar access to the knowledge to protect the critical infrastructure that lives depend on. It is essential for the success and safety of nuclear power that OT cybersecurity professionals are developed wherever possible. For these reasons the developers of the environment in this paper are committed to open-sourcing the full environment and all its tools, and optimizing the environment to run with limited hardware resources.

3. CYBER TRAINING ENVIRONMENT TECHNOLOGY STACK

To develop an environment that is truly dynamic, and representative of a real OT environment requires the key elements described in Figure 1. Each technology selected to fill key elements was carefully selected with these guiding principles in mind:

- The environment should be able to run on a low power college student laptop but also allow scaling up to a full highly accurate NPP DCS simulation.
- That scaling should smooth, ideally controlled by a single configuration file.

- The environment must be as transparent as possible. All communications and internal system operations must be visible and inspectable to students.
- The physics simulator should be swappable. Different NPP and especially Advanced Reactor physics simulations should be able to integrate easily into the environment.
- Everything that can be, should be opensource. There needs to be as low a barrier to entry as possible.

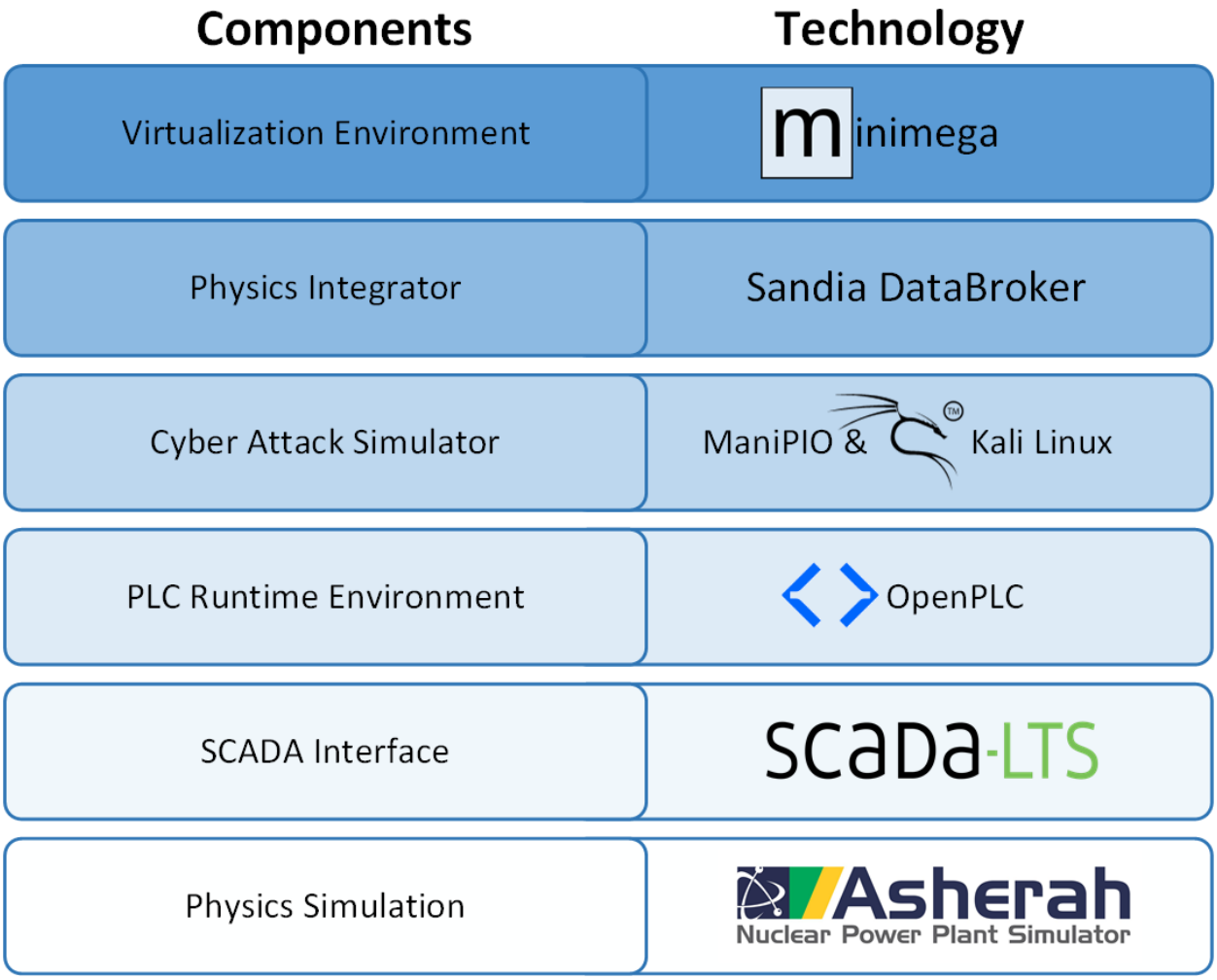

Figure 1: Key elements and technologies of the platform.

The foundation of the training environment is the virtualization environment; where all the Virtual Machines are instantiated, and which supports the emulated network. Principal to representing the cyber-physical nature of OT systems is the Physics Integrator which interfaces and drives the physical stimuli of control systems. Above these systems are the PLCs, SCADA system, and attack simulator which the students will interact with the most. Each of these systems is described below in detail.

3.1. Minimega

Minimega is a tool developed at Sandia to launch and manage large scale virtual machine-based experiments [3]. Minimega is scalable, allowing for the study of small or very large VM networks. Minimega has a number of novel technologies and capabilities:

- Open source, available at minimega.org
- Rapid, turnkey deployment on general purpose computers and clusters
- Very fast experiment description and launch
- Hardware-in-the-loop
- Scales to at least 100,000 endpoints
- Integrated command and control layer for endpoints
- VNC-based framebuffer and keyboard/mouse record and replay
- Supports QEMU/KVM and container-based VMs
- Ephemeral network connection support
- Feature-rich, real-time experiment visualizations

Minimega is the key enabling technology for the SNL Open-Source Emulation Platform. Particularly, the integrated command and control layer for endpoints (i.e., every single VM within the emulation platform) allowing for "controllers" or "researchers" to interact directly with each VM and automate actions and tasks within these VMs without contaminating the experiment (controlled network). This integrated command and control exposes all VMs to a single management node.

3.2. DataBroker

The SNL DataBroker is the key "adapter" component that connects a Matlab-Simulink simulator to the emulation platform [4]. Currently, the DataBroker works with any Matlab-Simulink and has a default configured mapping to the Asherah compiled binary. The DataBroker uses an S-Function (and POSIX Inter Process Communication shared memory spaces) to export values from Asherah and send them to the Endpoints via a UDP broadcast on 255.255.255.255. This UDP packet contains the physical information, actuator and sensor values, and other control signals necessary for the Hardware in the Loop (HiL) (i.e., SG and RCP controllers) to communicate and interact with the model.

3.3. ManiPIO

Manipulate Process I/O (ManiPIO) is a SNL developed python script that takes as an input a text file that can automate writing to a PLC register via Modbus TCP communication [5]. ManiPIO is open-source software provided by SNL to allow for research on OT cyber-attacks. However, ManiPIO requires a change to the controller logic to latch the setpoint change value, otherwise the PLC controller would overwrite this change with actual values determined by the controller algorithm.

3.4. OpenPLC

OpenPLC is an open-source programmable logic controller emulator [6]. Within the Emulation Platform that leverages Asherah simulator, the Reactor Coolant Pump (RCP) and the Steam Generator (SG) PLCs have been "exported" from the Asherah model executable. This allows for the Emulation Platform to attack the information/communication that is exchanged between the PLCs and the Asherah model executable, via the DataBroker. OpenPLC and the DataBroker both support Modbus TCP communications.

3.5. Scada-LTS

Scada-LTS is an Open Source, web-based, multi-platform solution that provides Supervisory Control and Data Acquisition (SCADA). Within the Emulation Platform, Scada-LTS is the Operator HMI for both the SG and RCP controllers. Scada-LTS is the key interface to demonstrate the effects of Man-in-the-Middle attacks.

3.6. Kali Linux

Kali Linux is an open-source Linux-based operating system that provides for a suite of cyber evaluation tools, such as penetration testing, password cracking, and red team emulation. Within the Emulation platform, Kali Linux provides the capability for students and researchers to launch actual attacks against PLCs, Scada-LTS and other elements of the Emulation Platform.

3.7. Asherah

The experiments in this report relied upon the Asherah Nuclear Power Plant Simulator (ANS) [2] to provide values for DH and Physical Information Harm (PIH). ANS was developed by the University of Sao Paulo as part of an IAEA Coordinated Research Project J02008. The key advance with ANS is the design allowed for hardware in the loop. Hardware in the loop allows for Commercial Off the Shelf (COTS) OT equipment to be interfaced with the simulator. This allows for actual cyber-attacks to be launched against COTS equipment and the follow-on impacts to the system and the reactor can be investigated. ANS consists of the major systems and components necessary to control the core (for operations), cool the core, and transfer the heat to the turbines and finally the atmosphere/environment (ultimate heat sink).

4. ACTIVITIES

The developed environment has evolved with each activity it has been used for to better fulfill roles in research and education. Research developments have expanded its capabilities and toolsets. Educational developments have focused on ease of use and resource optimization. Each of these activities have produced valuable feedback and lessons learned that are incorporated in future development.

4.1. Education - Brazil Cybersecurity Course

A pilot weeklong university course for OT cybersecurity for NPPs using the environment was delivered in July 2022 at the University of Sao Paulo. The environment was optimized and packaged to run on student laptops that were expected to have 2 cores and 16Gb of ram. Students were presented with a flat network with 2 PLCs, a SCADA HMI, and an embedded attacker (Figure 2). The students first task was to develop a simple HMI for the 2 PLCs and become familiarized with the OT environment from the role of an engineer. The second task put the students in the role of the attacker, they would perform a predeveloped Man in the Middle (MitM) attack against the HMI and malicious packet injection attacks against the PLCs and observe the effects. The final task and capstone of the course put students in the role of a system designer and asked them to redesign the network to prevent the attack by incorporating the previous days lecture material.

The course demonstrated that the environment excels in its setup simplicity and operational ease. The Minimega built in C2 channel provided rapid and consistent environment establishment. A single Wireshark instance could capture traffic from any interface in the environment, allowing students to easily analyze the environment and eliminating any jarring context switching. Most importantly the

environment proved to be remarkably stable, with over a dozen student laptops of varied configuration and poor computational ability, only 1 machine had a failure (hardware related).

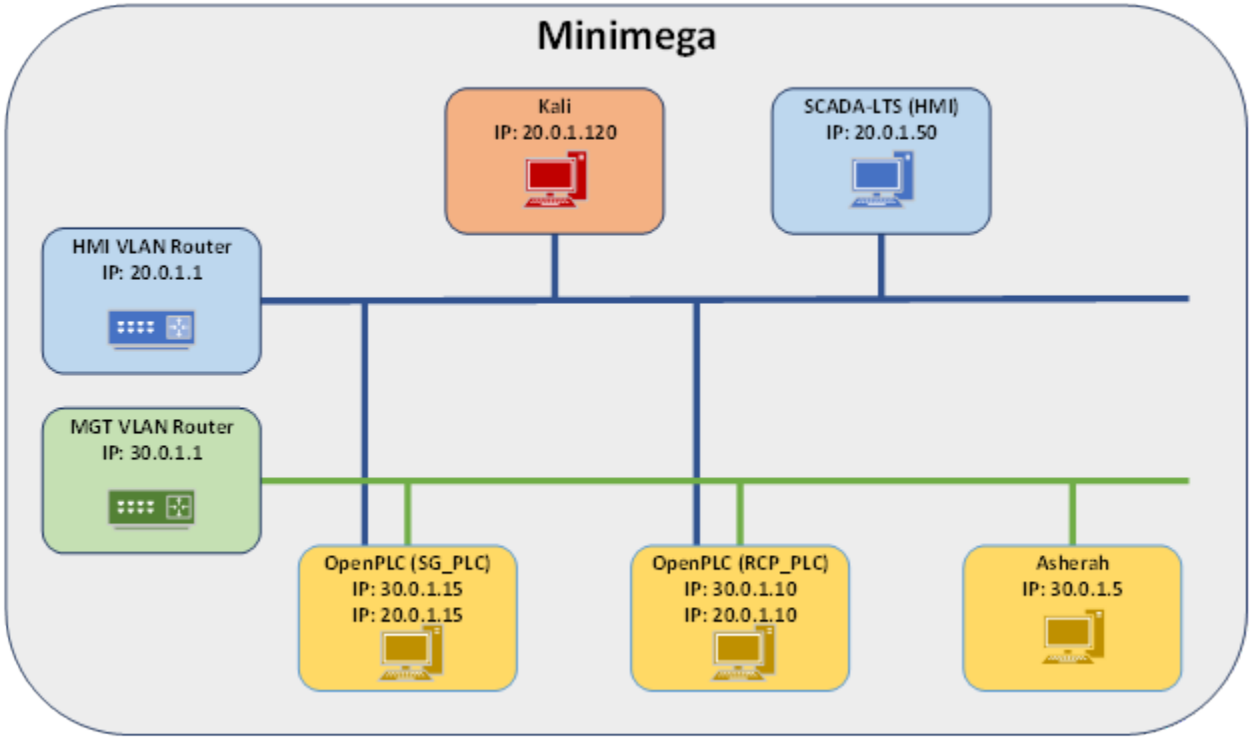

Figure 2: Emulation platform initial flat network configuration.

While the technology of the environment proved highly effective, the course illustrated some issues. The concepts needed to understand the complex environment of OT networks is broad and more extensive than previously estimated. The students gathered for the course were mostly engineering students and professionals that did not have any education on networks and their analysis. Much of the time in practical part of the course was spent covering how to use Wireshark and how OT network's function. During the capstone portion, editing the configuration files of Minimega for students to design their own DCS network proved to be too far reaching.

4.2. Cybersecurity Fundamental Research – Information Harm Triangle

The Information Harm Triangle (IHT) attempts to formalize metrics of harm to cyber-physical systems to understand the underlying fundamental qualities of cyber-attacks against OT [7]. Through this lens, cyber attacks can be measured and graded on consequence and detectability. The IHT seeks to simplify the implementation and improve the impact of defense in depth of NPP I&C. By expressing cyberattacks as two orthogonal components, Data Harm (digital information harm) and Physical Information Harm (real-world harm), their magnitude difference can differentiate attack risk and detection adequacy.

Figure 3 shows the experimental data from investigations on the IHT using the environment to test cyber attacks on the Steam Isolation Valve in Asherah [8]. The valve was forced to rapidly change position with a malicious change in the programming of the PLC that controls the valve. However, it was discovered that even though the valve position demand changed rapidly the valve could not physically change position rapidly. The valve is mechanically governed and therefore inherits some significant resilience to

certain types of cyber-attacks. Using the IHT this resilience inherent in control systems can be identified and credited to the defense in depth of a design.

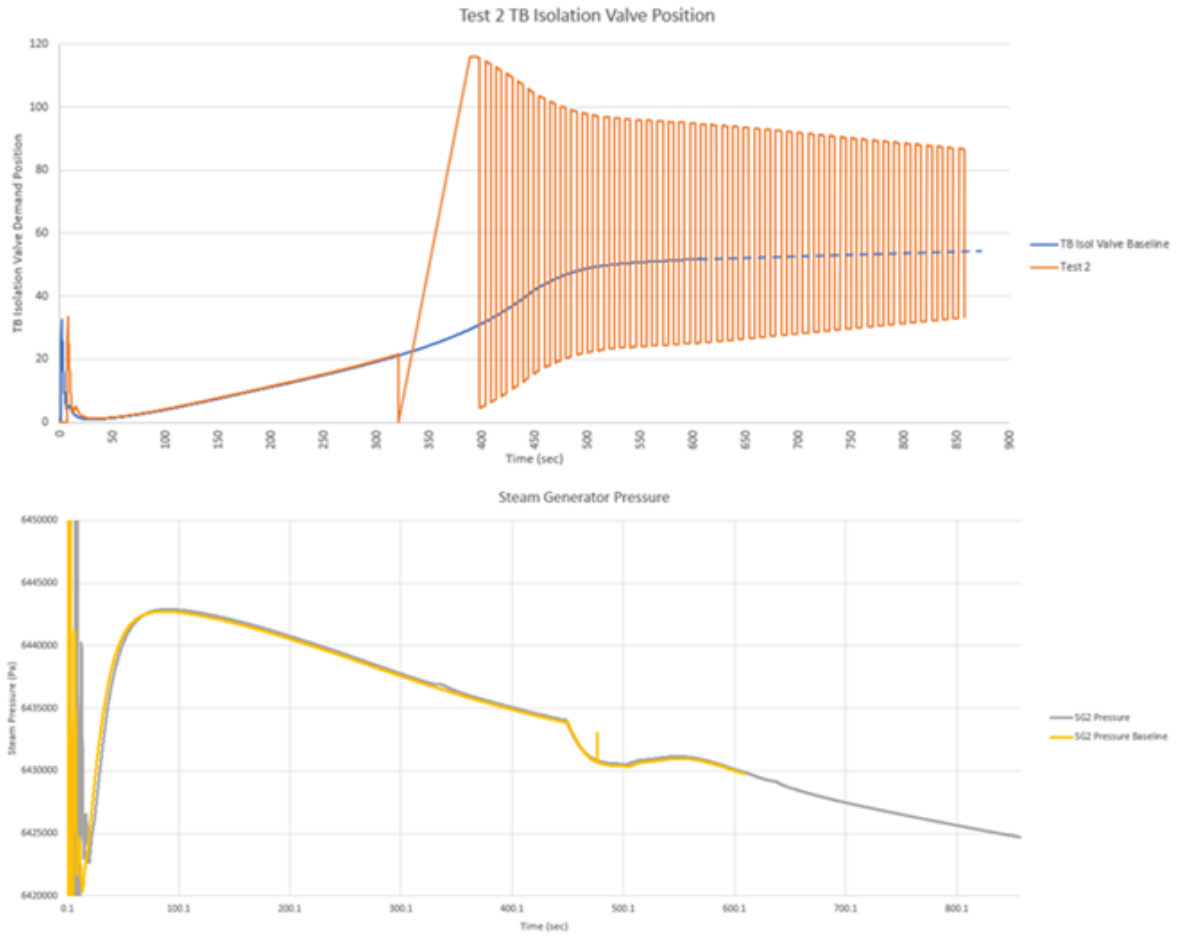

Figure 3: IHT steam isolation valve experimental data. [8]

The environment was used to perform many experiments to test the IHT theory and continues to be used to inform research on IHT theory application. Critically it provided the evidence to support the discovery that harm is a rate rather than a sum, a core understanding of the IHT theory. To continue to drive physical harm, harm to data must on going. This was demonstrated with Man in the Middle attacks against the HMI, showing that to preventing physical harm intervention from operators required a continuous stream of data being altered (data harm). All the experiments on the system pointed to the underlying property of the IHT, though the MitM example is most illustrative.

The environment continues to provide valuable data for fundamental OT cybersecurity research like the IHT. A scaled-up version of the Brazil environment has been developed that incorporates the full Asherah control system in a multi-layer security network. The limits of useful research possible for the IHT have nearly been reached with Asherah, being that it is a fictional NPP. Since the environment and DataBroker have been developed specifically for modularity, new high-fidelity models of advanced reactors are being integrated with the environment through its next evolution discussed in Section 5.

4.3. Lessons Learned

The Brazil course demonstrated the gaps in the environment that needed to be addressed to adequately address its use in the classroom environment. The design of a DCS with cybersecurity defense in depth is a highly advanced activity that needs more lead up. The MitM attack was not realistic enough to be fully effective on the HMI, the values did not change once the attack began and thus the HMI simply stopped updating. Pre-written DCS architectures, a more realistic MitM attack, more materials that discuss defensive measures, and pre-course study materials are being incorporated for the next iteration of the course.

The environment currently only runs on Linux distributions due to Its dependency on QEMU for virtualization in Minimega. To solve this a full Docker implementation is being investigated, though virtualizations within containers present limitations that are time intensive to solve. Primary focus for current development is scripting to auto-assemble the environment's VMs and container images to improve deployment. The original distribution was 12Gb in size even highly compressed, which makes opensource distribution difficult, the intent is to reduce this to sizes that can be hosted on GitHub. The intent is for students to be able to run a single command and the environment will self-install, and with another single command the environment will start. This was achieved with 12Gb distribution but is now being developed for the opensource release.

Research use of the environment has shown some gaps in the toolset, such as limited communication protocols, few satisfactory emulations of commercial PLCs, and Asherah's limitations on DCS complexity. These limitations are being addressed on multiple fronts. The protocols are limited only by the PLCs and DataBroker, recently development of new protocols has begun and OPCUA is expected to be introduced in the next year. Few emulations of PLCs meet the requirements for use in cybersecurity research, currently HitL is the best solution and FPGA integration is also being investigated.

Asherah's limitations are 2-fold, one being reduced complexity, but most significant are the license limitations. Asherah may be the closest to opensource of any NPP simulation, but it is not fully opensource due the rights held by the IAEA. Though free to any IAEA member country, not being opensource means it cannot be hosted openly, massively impedes open collaboration, and nearly eliminates the incentive for continued development support external to the IAEA. This limitation is not shared by any other component in the environment which was ultimately developed to allow swapping of the physics simulator. Development is on-going to produce standardized DataBroker connectors to high fidelity physics simulators of advanced reactors with various code bases.

5. FUTURE DEVELOPMENTS

As an educational tool the environment has proven to be capable of providing support for moderately advanced students. It has the capabilities of spanning the breadth of the educational spectrum, bridging the educational tool gap from novice to scientist. This is exactly the intent of future developments. The educational tool is being honed to provide better support to beginning OT cybersecurity classes. While more advanced class resources are being developed to include better, more complex, defensive measures (firewalls, intrusion detection systems, Security Information and Event Management, etc.). The developments for research can be directly applied in the classroom, drastically improving the efficiency for which novel research can be translated to the classroom.

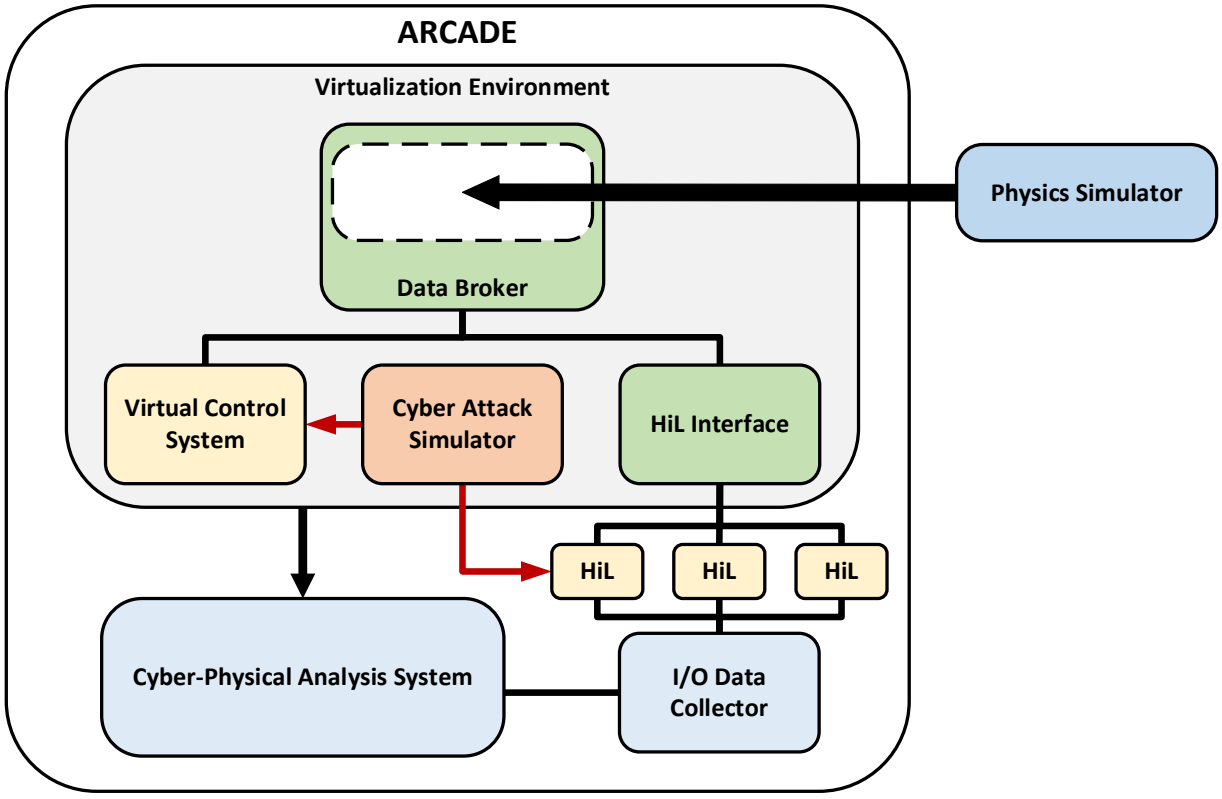

Figure 4: Advanced Reactor Cyber Analysis and Development Environment (ARCADE) functional block diagram.

For research the environment has provided the basis and foundational tools to enable the Advanced Reactor Cyber Analysis and Development Environment (ARCADE) (Figure 4). This new toolset seeks to enable the analysis of cyber risk on advanced reactor designs from a system-level design to a component-level design. ARCADE will also allow the development and validation of cybersecurity design strategies. Highly instrumenting emulations and HIL in a high-fidelity representation of the entire DCS of an Advanced Reactor with integrated physics will allow an exceptional level of introspection. Intrusion detection, prevention, and mitigation research can be conducted on the DCS while the physics simulation allows a measure of the physical consequence of the cyber-attacks. ARCADE is currently under development and its tools and discoveries will have direct pathways to improve the quality of its educational counterpart.

CONCLUSIONS

The developed environment described here has proven to be a highly valuable tool in research and in education. It has been demonstrated that it can be used to support advanced courses on OT cybersecurity, and students will be able to run a research environment from their own homes. A paradigm shift that will drastically expand the potential for innovation by delivering tools and capabilities beyond the laboratory. Though, gaps were identified in course material, being that this is the first time students have been presented with the real task of synthesizing new architectures and security approaches. Development on the course and environment will continue to close these gaps and allow a depth of applied learning previously only possible in the laboratory.

Within the laboratory the environment had originally proved itself with the investigation of the combinatory effects of multiple Unsafe Control Actions (UCAs) [9]. Physical and digital harm being rates in the context of the IHT was supported and tested using this environment. Without Asherah and the environment, investigation of IHT could not have discovered inherently protective phenomena like the mechanical governing of valves. Though the constant motion of the valve would cause excess long-term stress and wear on the system, the short-term failure is prevented via this governing of the valve. Modeling of this stress and wear is an ongoing effort, and these more complete models will allow a greater resolution of rate of harm analysis.

The development of this environment began because some experimental tools could not be shared with a university research partner. It has exceeded initial expectations and will continue to develop into more refined opensource research and education tools. Such tools are essential to accelerating cyber defense for nuclear to match the pace of cyber adversaries. Cybersecurity will continue to be a concern for nuclear security for as long as digital systems exist. Continued investment in the development of tools to understand cyber risks and educate engineers to mitigate these risks is critical to the success and safety of nuclear power.

REFERENCES

1. S. O. BADA, "Constructivism Learning Theory: A Paradigm for Teaching and Learning," *IOSR Journal of Research & Method in Education,* **5** (6), pp. 66-70 (2015).
2. R. Silva, K. Shirvan, J. R. C. Piqueira and R. P. Marques, "Development of the Asherah nuclear power plant simulator for cyber security assessment," in *Proceedings of the International Conference on Nuclear Security*, Vienna, Austria (2020).
3. J. Crussell, J. Erickson, D. Fritz and J. Floren, "minimega v. 3.0," Sandia National Labs, Albuquerque, NM (2015).
4. A. Hahn and R. Fasano, "OT Emulation Data Broker," Sandia National Labs, Albuquerque (2021).
5. A. Hahn, "ManiPIO - Manipulate Process I/O," Sandia National Labs, Albuquerque, NM (2021).
6. T. Alves and T. Morris, "OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research," *Computers & Security,* **78**, pp. 364-379 (2018).
7. M. T. Rowland, L. T. Maccarone and A. J. Clark, "Using the Information Harm Triangle to Identify Risk-Informed Cybersecurity Strategies for Instrumentation and Control Systems," *Nuclear Technology,* **209** (3), pp. 471-487 (2023).
8. M. T. Rowland, "Investigation of Data Harm and its Relevance to Unsafe Control Actions of Control Systems through Application of the Information Harm Triangle," (2023).
9. A. S. Hahn, C. Lamb, R. E. Fasano and D. Sandoval, "AUTOMATED CYBER SECURITY TESTING PLATFORM FOR INDUSTRIAL CONTROL SYSTEMS," in *12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, Providence, Rhode Island (2021).