ADVANCED REACTOR CYBER ANALYSIS AND DEVELOPMENT ENVIRONMENT (ARCADE) FOR UNIVERSITY RESEARCH

L.T. MACCARONE, A.S. HAHN, R. VALME, M.T. ROWLAND
Energy Security, Sandia National Laboratories
Eubank SE, 87185 Albuquerque – United States

A. KAPURIA, Y. ZHANG, D.G. COLE
Department of Mechanical Engineering and Materials Science, University of Pittsburgh
O'Hara Street, 15213 Pittsburgh – United States

Rigorous, repeatable, and evidence-based cybersecurity analysis and evaluations require complex modeling and simulation platforms. To address this need, Sandia National Laboratories has developed and implemented a suite of open-source network emulation tools capable of interfacing with nuclear power plant physics models. These tools have been applied to several projects supported by the U.S. Department of Energy's Office of Nuclear Energy (DOE-NE) and International Nuclear Security (DOE-INS) to develop advanced cybersecurity training and to conduct cybersecurity research and development (R&D). Given the cybersecurity needs of advanced reactors, these open-source tools are being leveraged to develop an Advanced Reactor Cyber Analysis and Development Environment (ARCADE). This work details collaboration efforts that integrate the University of Pittsburgh's Small Modular Advanced High-Temperature Reactor (SmAHTR) with ARCADE and presents the benefits of the collaboration for enhanced cybersecurity R&D and workforce development.

1. Introduction

Rigorous, repeatable, and evidence-based cybersecurity analysis and evaluations require complex modeling and simulation platforms. To address this challenge, the International Atomic Energy Agency (IAEA) commenced a Coordinated Research Project (CRP) in 2017 to develop an open-source pressurized water reactor (PWR) simulator, the Asherah nuclear power plant. Sandia National Laboratories (SNL) has developed and implemented a suite of open-source tools that integrate with the Asherah simulator.

After successful cybersecurity research and development (R&D) efforts using Asherah, SNL's suite of tools is now being applied to analyze the cybersecurity of advanced reactors. Given the cybersecurity needs of advanced reactors, these open-source tools are being leveraged to develop an Advanced Reactor Cyber Analysis and Development Environment (ARCADE). The aim of these efforts is to simplify secure-by-design (SeBD) analysis, evaluate Defensive Computer Security Architecture (DCSA) implementation, evaluate cyber-attack impacts, and provide a holistic hands-on training environment for advanced reactors.

These tools have been applied to several projects supported by the U.S. Department of Energy's Offices of Nuclear Energy (DOE-NE) and International Nuclear Security (DOE-INS) to develop advanced cybersecurity training and conduct cybersecurity R&D. These open-source tools are also being socialized with several universities with the benefits of conducting advanced cybersecurity R&D and strengthening the future cybersecurity workforce. This paper will detail efforts and status of these activities and the application of open-source software for the cybersecurity analysis of advanced reactors.

In particular, this paper presents collaboration efforts between SNL and the University of Pittsburgh on the development of cybersecurity analysis methods using advanced reactor modeling and simulation tools. The University of Pittsburgh developed a model of a Small Modular Advanced High-Temperature Reactor (SmAHTR) that was integrated with ARCADE for cybersecurity applications. This combination of the

SmAHTR physics model and the ARCADE network emulation environment enables the analysis of cyber-physical consequences of cyber-attacks on digital instrumentation and control (I&C) systems and the development of new cybersecurity analysis methods. Several cybersecurity simulation cases are presented using SmAHTR, and the impact of the collaboration is discussed.

2. Prior Modeling and Simulation Efforts for Cybersecurity Analysis

Many of the modeling and simulation tools developed by Sandia National Laboratories have been applied to projects supported by DOE-NE and DOE-INS to develop advanced cybersecurity training and to conduct cybersecurity R&D. This section provides a brief summary of these applications.

The physics model used in these modeling and simulation efforts is the Asherah nuclear power plant simulator [1]. Asherah is an open-source hypothetical PWR model developed and maintained by the University of Sao Paulo as part of an IAEA CRP. Asherah is a Simulink model of a 2,772 MWt two-loop PWR that was tuned using PARCS/RELAP. Asherah is a complete physics simulator, but does not contain simulation of all controllers, alarms, and annunciators found in a plant, nor does it contain a network emulation.

The development of a platform that incorporates a network simulation environment, a physics simulator, and virtual PLCs is presented in [2]. The network simulation in [2] was limited to a single controller, but the approach was soon applied to include networks of multiple controllers. These networks have been used to analyze combinations of multiple unsafe control actions (UCAs) and to develop new cybersecurity analysis tools [3, 4]. Insights included the impact of the timing of sequences of UCAs on plant process variables.

Asherah and SNL's network emulation tools have also been leveraged as part of cybersecurity training courses [5, 6]. The key benefits of these tools in training courses are that they accurately represent cybersecurity and networking concerns and are not export controlled. Building international cybersecurity capabilities is central to DOE-INS's mission, therefore the open-source nature of SNL's tools is highly valuable in developing training materials. The environment developed for these training courses is capable of being run on a low-power laptop of a college student and can also be scaled up to represent larger systems as needed [6].

3. Advanced Reactor Cyber Analysis and Development Environment (ARCADE)

ARCADE is a collection of tools designed to enable researchers to perform cybersecurity experiments on Defensive Cyber Security Architectures (DCSA) for Distributed Control Systems (DCSs). These tools have individually been useful in narrow scoped investigation, but together allow a complete view of a DCSA for cyber experiments. Using ARCADE, it will be possible to investigate the entire cyber-attack surface of a DCS from the physics of control, down to the firmware of individual components. A functional block diagram of ARCADE is shown in Figure 1. The remainder of this section describes ARCADE and is adapted from [7].

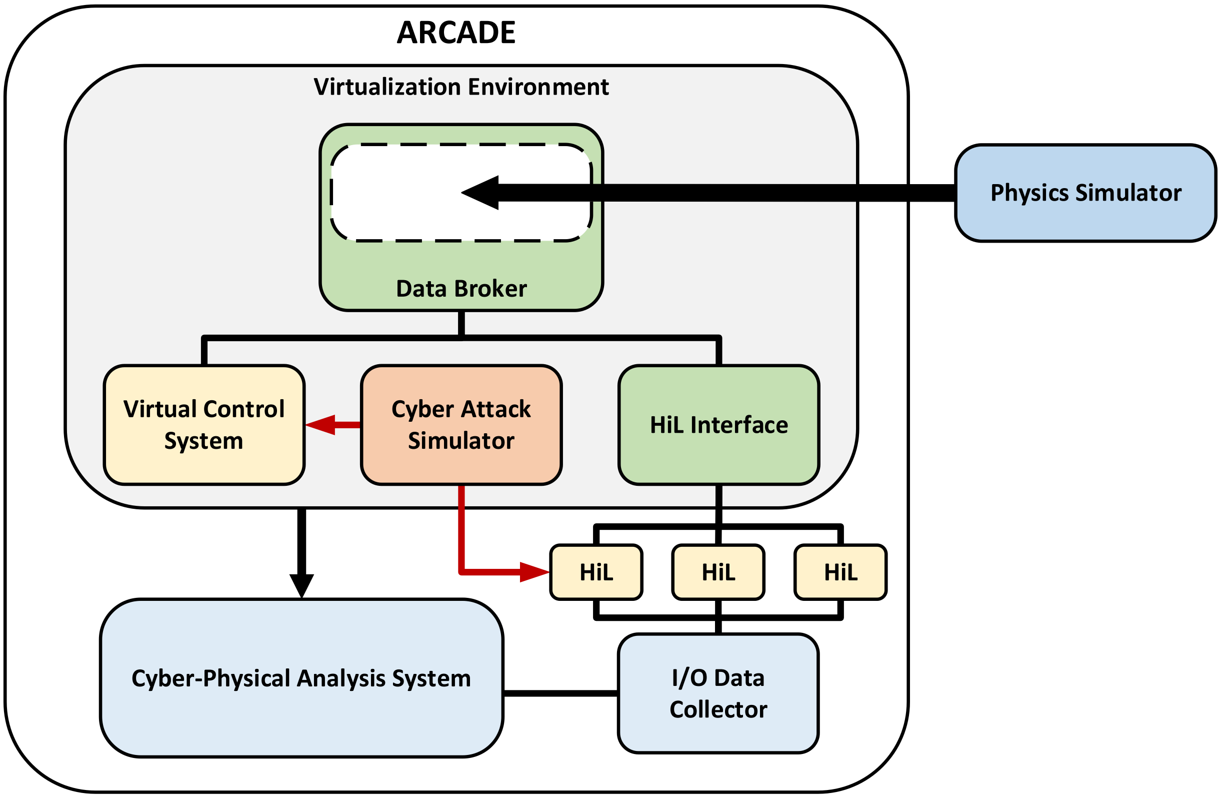

Figure 1: Advanced Reactor Cyber Analysis and Development Environment (ARCADE) Functional Block Diagram [7]

The foundation of ARCADE is the virtualization environment that supports the system's virtual machines. Minimega was selected as the virtualization environment primarily because of its transparency and data capturing abilities [8]. The file systems of the virtual machines and all network traffic are visible, inspectable, and recordable. The full scope of the effects and indicators of cyber-attacks can be deeply inspected with this level of system visibility. Availability of virtualized or emulated hardware is the only limitation, as some manufactures have not produced emulations of their control systems. Other systems are not conducive to emulation, such as field-programmable gate array (FPGA) control systems which operate as discrete logic. The solution for machines that cannot currently be emulated is a hardware-in-the-loop (HiL) approach.

Minimega allows taps to bridge virtual network interfaces to the host machine, but HiL integration with the physics simulator required the development of the Data Broker [9]. Most physics simulators do not have the capability to integrate with HiL, and those that do are often only able to connect to a single controller. The Sandia Data Broker is a distributed computing solution to connecting a physics simulator to a DCS. It was developed as a modular and universal solution for connecting physics simulators to virtual or physical control systems. Its companion tool is ManiPIO, which shares ICS communication libraries and allows the simulation of control system cyber-attacks [10]. ARCADE incorporates ManiPIO into its cyber-attack simulation suite that is hosted on a Kali Linux VM.

While ARCADE does not include a physics simulator, it is important to understand how some key tools were developed around the Asherah NPP Simulator [1]. The Data Broker, ManiPIO, and many elements of the virtual control system were first developed using Asherah as the physics simulator [9, 10]. Key features of Asherah critical to DCSA modeling include simulated control surfaces (e.g., valves, pumps, actuators), separation of the process simulation and the control system, and a solver that allows external data injection. These features are key to enabling control systems to be separated from the rest of the simulator and replaced with external controllers.

ARCADE must be able to support cybersecurity analysis throughout the advanced reactor decision process. One framework for the design process was developed by the World Nuclear Association (WNA) to describe the development of small modular reactors (SMRs) [11]. These benefits of ARCADE are summarized for the WNA design phases in Table I. For greater detail, readers are encouraged to refer to [7].

Table I: ARCADE Benefits By Design Phase [7]

Design Phase	**Phase Description**	**ARCADE Benefits**
Concept	Reactor concept	N/A: focused exclusively on reactor design
Plant-Level	Requirements of key systems, structures, and components (SSCs) are identified	Preliminary evaluation of I&C architecture interaction with reduced-order physics models to evaluate efficacy of SeBD features to eliminate or mitigate accident sequences caused by a cyber-adversary
System-Level	Requirements of key SSCs are refined, and additional systems are defined	Evaluation of DCSA interaction with high-fidelity physics models to evaluate attack sequences not mitigated or eliminated by security-by-design features
Component-Level	Engineering details are finalized for SSCs	Testing of integration of specific ICS devices through emulation or HiL and denial of adversary's ability to conduct specific tasks

4. Small Modular Advanced High-Temperature Reactor (SmAHTR)

SmAHTR is a fluoride-salt-cooled reactor that can be easily transported to and assembled at remote sites and is designed to deliver safe, affordable, and reliable high-temperature process heat and electricity [12]. SmAHTR uses tri-isotopic (TRISO)-coated particle fuel and graphite as a moderator. The following SmAHTR description and model development is based upon a pre-conceptual design report written by researchers at Oak Ridge National Laboratories [12].

SmAHTR employs three in-vessel primary heat exchangers (PHXs). Each PHX is coupled with a main circulating pump that directs primary coolant salt from the common riser region above the reactor core down through the shell side of the PHX into a common downcomer region. The coolant flows down through the downcomer region to the lower head of the reactor vessel, up through the core, and back to the common riser region, thus completing the main cooling loop. SmAHTR can operate at full power with only two of three cooling loops by increasing the pump flow in the two operational cooling trains. SmAHTR employs three passive direct reactor auxiliary cooling system (DRACS) cooling loops to remove shutdown decay heat from the reactor. Only two of the three loops are required for safe operation. During nominal operation, the DRACS removes 1% core heat.

The secondary side of each PHX is an integral element of a companion intermediate cooling loop. Each intermediate cooling loop includes the secondary side of the PHX, a companion intermediate loop pump, and an intermediate heat exchanger that transfers the heat to the ultimate load (either the electrical power conversion system or the process heat storage system). During normal operations, all three main and intermediate cooling loops are active, each removing one-third of the heat produced by the reactor. This is accomplished by adjusting the in-vessel main circulating pump flow and the companion intermediate circulating pump flow.

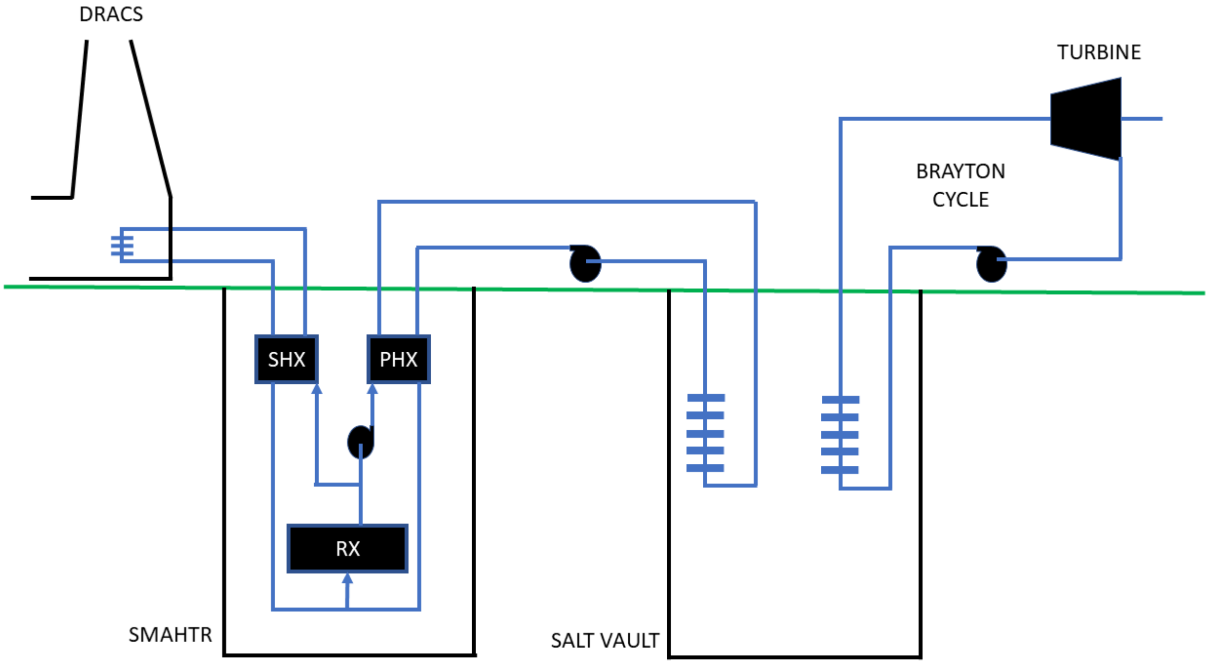

Figure 2: SmAHTR Simulink model includes the reactors, salt vault, and Brayton cycle.

A SmAHTR model has been developed and used in research at the University of Pittsburgh [13, 14]. An offline model was developed for the SmAHTR using Matlab and Simulink. In this model, the SmAHTR is coupled to a salt vault and a Brayton cycle, as shown in Figure 2. Four SmAHTR reactors operate together to transfer energy to the salt vault through three integral PHXs per reactor. The salt vault is the primary heat storage unit. The energy stored in the salt vault is used to make steam to generate mechanical power in the turbines. There are three turbines that receive heat from the salt vault.

The reactor system is modeled in Simulink, and consists of the reactor core, the PHXs and DRACS with secondary heat exchangers (SHXs). The reactor core is modeled as a spatially lumped-parameter point-kinetics model. The core thermodynamics model relates reactor power and reactor temperature. A PI controller regulates reactor outlet temperature using reactivity control. The total reactivity of the system includes the reactivity due to the control rods and the temperature feedback. Reactor power is controlled by manipulating the primary mass flow rate, subsequently controlled using a PI controller. The reference for the controller is the desired primary flow rate for nominal operation.

Although the University of Pittsburgh's SmAHTR model was originally developed for other applications, the model has been repurposed for cybersecurity R&D with SNL. The aim of the collaboration between the University of Pittsburgh and SNL is to develop novel approaches for characterizing the cyber-physical effects of cyber-attacks on I&C systems and their mitigations. The approach being developed is called the Information Harm Triangle (IHT). The IHT decomposes cybersecurity harm into two orthogonal vectors: data harm and physical information harm. Data harm is harm to information stored on digital systems and physical information harm is harm to a physical process. Attacks on I&C systems cause data-harm, which can lead to physical information harm through a UCA [3, 15, 4, 16]. This research is enabled by coupling SmAHTR with ARCADE, to study both the cyber and physical consequences of cyber-attacks on the plant.

5. Application and Discussion

To demonstrate potential cybersecurity applications for SmAHTR and ARCADE, two cybersecurity scenarios were investigated. In both scenarios, it is assumed that the adversary has the capability to manipulate the power demand signal used to operate the pumps of the first reactor's PHXs. In Scenario 1, the adversary decreases the power demand of the first PHX. In Scenario 2, the adversary sequentially decreases the power demand of all three PHXs.

5.1. Scenario 1 Results: Manipulation of One PHX

In this scenario, the adversary reduces the power demand of one of Reactor 1's PHXs from 42 MW to 1 MW at a time of 100 seconds. The results of this simulation are shown in Figure 3. The results shown were selected because of their relevance for heat transfer from the reactor to the salt vault. The results shown in Figure 3 are grouped by reactor, with the first column corresponding to Reactor 1 and the second column corresponding to Reactors 2, 3, and 4. Reactors 2, 3, and 4 behave identically when Reactor 1 is manipulated. The mass flow rates of the secondary side of the PHX are shown in Figure 3a and Figure 3b, the temperatures of the secondary side of the PHX are shown in Figure 3c and Figure 3d, and the temperatures of the primary side of the PHX are shown in Figure 3e and Figure 3f.

5.2. Scenario 2 Results: Manipulation of Three PHXs

In this scenario, the adversary sequentially reduces the power demand for each of Reactor 1's PHXs from 42 MW to 1 MW. The power demand for the first PHX is reduced at a time of 100 seconds, the power demand for the second PHX is reduced at a time of 200 seconds, and the power demand for the third PHX is reduced at a time of 300 seconds. The results of this simulation are shown in Figure 4. Figure 4 has the same structure as Figure 3.

5.3. Discussion

In both scenarios, the secondary coolant mass flow rate through the Reactor 1 PHXs were reduced as the power demand was decreased (Figure 3a and Figure 4a). In Scenario 1, the mass flow rate is approximately halved while in Scenario 2, the mass flow rate sequentially decreases until it approaches zero.

As the mass flow rate of the Reactor 1 PHX secondary coolant decreases, the temperature of the PHX secondary coolant inlet decreases because the Brayton cycle is converting the same amount of heat from the salt vault to power while the salt vault receives less heat from the PHXs (Figure 3c and Figure 4c). The temperature of the secondary coolant at the outlet of the PHX increases to attempt to maintain the same heat transfer with a decreased mass flow rate. In Scenario 2, the difference between the two temperatures increases as the power demand is manipulated for more PHX pumps.

As the Reactor 1 PHX primary fluid outlet temperature increases, the primary fluid inlet temperature also increases (Figure 3e and Figure 4e). In Scenario 1, both temperatures settle and the inlet temperature returns to its original value, while in Scenario 2, both temperatures continue to rise until they nearly converge because proper heat transfer is not occurring in the PHX.

Although only Reactor 1's PHX pumps were manipulated, Reactors 2, 3, and 4 were also affected because the reactors are thermodynamically coupled through the salt vault. As the power demand was decreased for the Reactor 1 PHXs, the secondary coolant mass flow rate through the Reactors 2, 3, and 4 PHXs were reduced (Figure 3b and Figure 4b), the temperatures of the secondary coolant for the Reactors 2, 3, and 4 PHXs were reduced (Figure 3d and Figure 4d), and the temperatures of the primary fluid were the least affected by changes to the Reactor 1 PHX power demand (Figure 3f and Figure 4f).

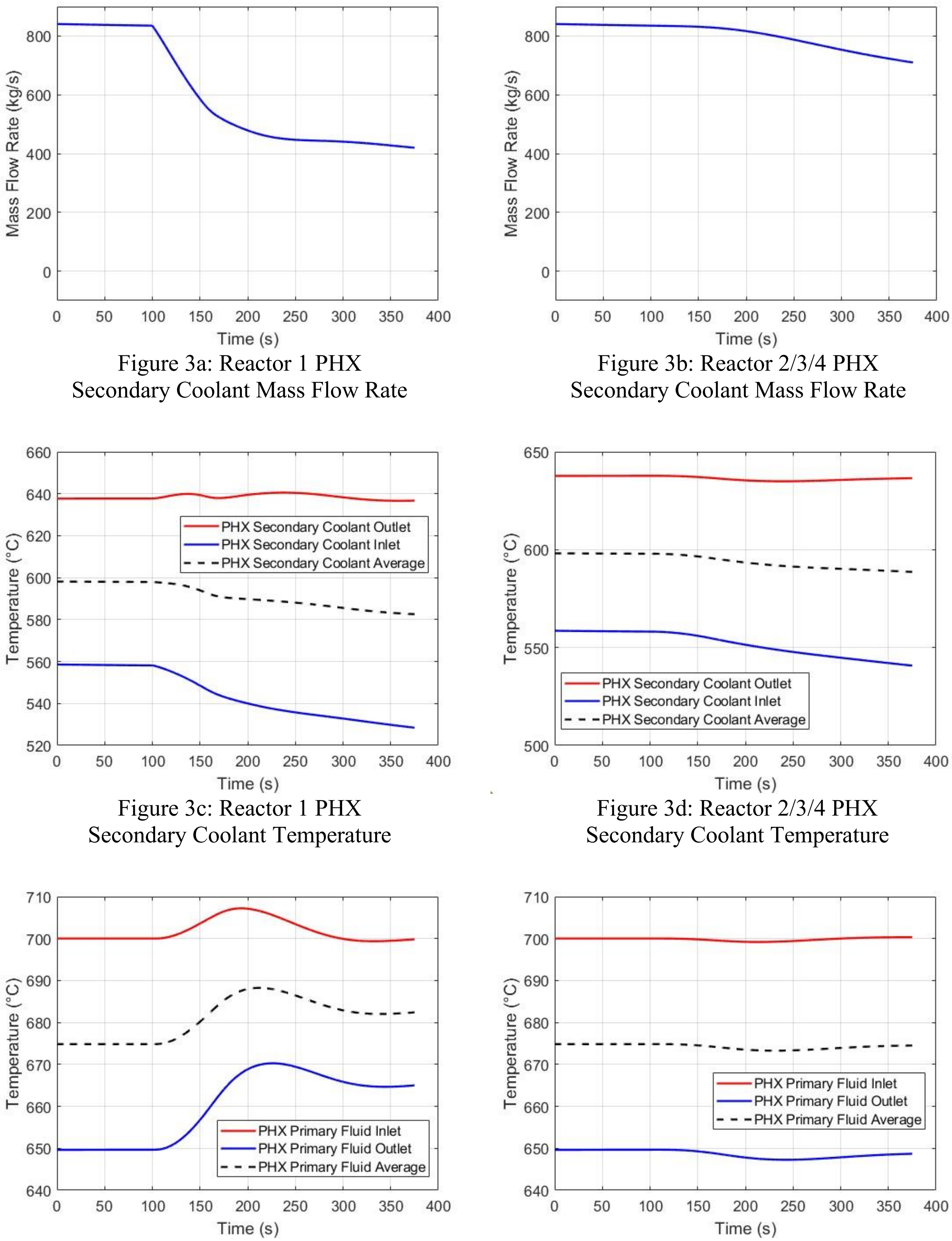

Figure 3a: Reactor 1 PHX
Secondary Coolant Mass Flow Rate

Figure 3b: Reactor 2/3/4 PHX
Secondary Coolant Mass Flow Rate

Figure 3c: Reactor 1 PHX
Secondary Coolant Temperature

Figure 3d: Reactor 2/3/4 PHX
Secondary Coolant Temperature

Figure 3e: Reactor 1 PHX
Primary Fluid Temperature

Figure 3f: Reactor 2/3/4 PHX
Primary Fluid Temperature

Figure 3: Simulation Results for Manipulation of One PHX

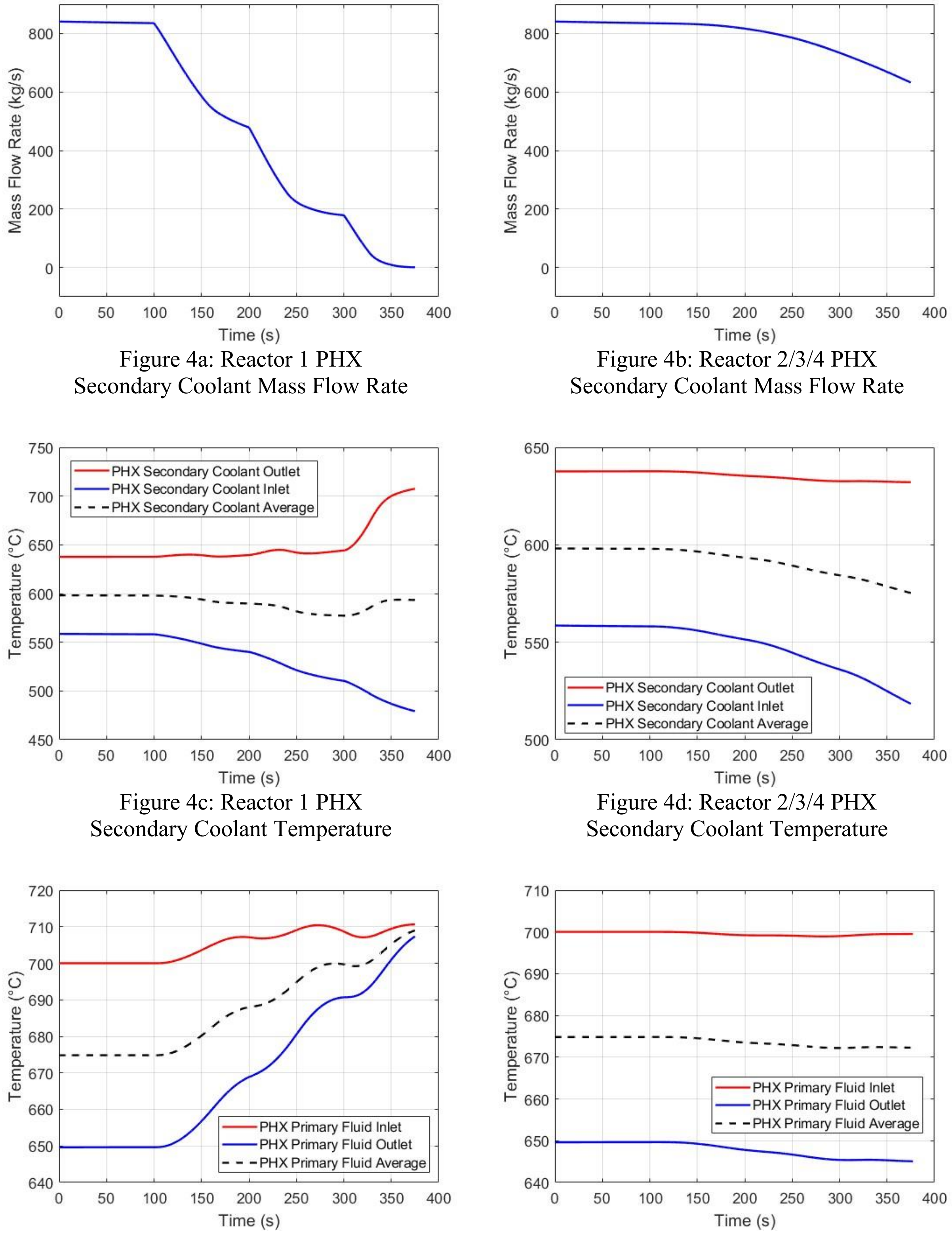

Figure 4a: Reactor 1 PHX
Secondary Coolant Mass Flow Rate

Figure 4b: Reactor 2/3/4 PHX
Secondary Coolant Mass Flow Rate

Figure 4c: Reactor 1 PHX
Secondary Coolant Temperature

Figure 4d: Reactor 2/3/4 PHX
Secondary Coolant Temperature

Figure 4e: Reactor 1 PHX
Primary Fluid Temperature

Figure 4f: Reactor 2/3/4 PHX
Primary Fluid Temperature

Figure 4: Simulation Results for Manipulation of Three PHXs

6. Conclusion

This paper presented the collaborative research being conducted by SNL and the University of Pittsburgh to investigate the cybersecurity analysis of advanced reactors. The University of Pittsburgh SmAHTR plant physics simulator was integrated with SNL's ARCADE network emulation environment for holistic cyber-physical analysis of the system. This combination enables the studying of investigation of specific cyber-attack scenarios for the SmAHTR plant as presented in this paper, and also enables the development of novel cyber-physical analysis tools such as the IHT. This collaboration also has significant benefits for the development of the future cybersecurity workforce.

Historically, the management of networks and data has been the purview of information technology (IT) professionals, and the management of devices and machines has been the purview of operational technology (OT) professionals. The different needs, standards, and requirements of the two fields have meant that these two fields have evolved with distinct language, culture, and educational priorities, resulting in an IT/OT gap. Now, as the OT environment has become more cyber-physical and connected, there has been debate about who should manage security, IT or OT? No longer should it be one or the other — instead, security professionals must be able to cross the IT/OT gap and be knowledgeable about both. More and more, employers are looking for new hires with interdisciplinary backgrounds and need technologists who can work across the interface between disciplines and who understand technology in context.

In order to educate IT and OT professionals more broadly, we will need to create new educational opportunities that require them to work across the interface between disciplines. Tools and testbeds like ARCADE enable this by making it possible to study cyber-physical systems from the physics of the system, to the characteristics of control, to the firmware of individual components. Using ARCADE, we will be better able to train future security professionals for cross-cutting roles that blend traditional engineering disciplines such as mechanical and electrical engineering with information and computing competencies.

Acknowledgements

This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan. SAND2023-04332C

The research conducted at the University of Pittsburgh was supported by Sandia National Laboratories Contract 2448640: Development of a System-Level Design Analysis Method for Advanced Reactors.

References

[1] B. E. Silva, R.A, R. Shirvan, J. Piqueira and R. Marques, "Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment," in *IAEA International Conference on Nuclear Security*, Vienna, Austria, 2020.

[2] A. Hahn, D. R. Sandoval, R. E. Fasano and C. C. Lamb, "Automated Cyber Security Testing Platform for Industrial Control Systems," in *Proceedings of the 12th International Nuclear Plant Instrumentation, Control Human-Machine Interface Technologies (NPIC&HMIT 2021)*, Virtual Online Meeting, 2021.

[3] L. T. Maccarone, A. S. Hahn and M. T. Rowland, "Using the Information Harm Triangle to Model Sequences of Unsafe Control Actions In Instrumentation and Control Systems," in *Proceedings of the 2023 30th International Conference on Nuclear Engineering (ICONE30)*, Kyoto, Japan, 2023.

[4] M. T. Rowland, "Investigation of Data Harm and its Relevance to Unsafe Control Actions of Control Systems through Application of the Information Harm Triangle," University of London, London, UK, 2022.

[5] M. T. Rowland, A. S. Hahn, R. P. Marques, N. White and C. Spirito, "NPP Simulator Platform for Cyber Security Research and Training," in *Proceedings of the INMM 63rd Annual Meeting*, 2022.

[6] A. S. Hahn, M. T. Rowland, S. Eggers, C. C. Lamb and R. Valme, "Assessment and Experience Using Open-Source NPP Environments for Cyber-Security Training," in *Proceedings of the 13th International Nuclear Plant Instrumentation, Control Human-Machine Interface Technologies (NPIC&HMIT 2023)*, Knoxville, TN, 2023.

[7] A. S. Hahn, M. Higgins, L. T. Maccarone, M. T. Rowland and R. Valme, "Lessons Learned from Advanced Reactor Cyber Analysis and Development Environment (ARCADE)," in *Proceedings of the 13th International Nuclear Plant Instrumentation, Control Human-Machine Interface Technologies (NPIC&HMIT 2023)*, Knoxville, TN, 2023.

[8] J. Crussell, J. Erickson, D. Fritz and J. Floren, "minimega v. 3.0," Sandia National Laboratories, Albuquerque, NM, 2015.

[9] A. S. Hahn and R. E. Fasano, "OT Emulation Data Broker," Sandia National Laboratories, Albuquerque, NM, 2021.

[10] A. S. Hahn, "ManiPIO - Manipulate Process I/O," Sandia National Laboratories, Albuquerque, NM, 2021.

[11] World Nuclear Association, "Design Maturity and Regulatory Expectations for Small Modular Reactors," London, UK, 2021.

[12] S. Greene, J. Gehin, D. Holcomb, J. Carbajo, D. Ilas, A. Cisneros, V. Varma, W. Corwin, D. Wilson, G. Yoder Jr., A. Qualls, F. Peretz, G. Flanagan, D. Clayton, E. Bradley, G. Bell, J. Hunn, P. Pappano and M. Cetiner, "Pre-Conceptual Design of a Flouride-Salt-Cooled Small Modular Advanced High-Temperature Reactor (SmAHTR)," Oak Ridge National Laboratory, Oak Ridge, TN, 2010.

[13] C. J. D'Angelo and D. G. Cole, "Hot Standby State Observers for Sensor Fault-Tolerance in Small Modular Reactors," in *American Nuclear Society Winter Meeting*, Washington, D.C., 2015.

[14] J. A. Farber and D. G. Cole, "Real-Time Supervisory Control Implementation of SmAHTR Power Plant," in *Proceedings of the 10th International Nuclear Plant Instrumentation, Control Human-Machine Interface Technologies (NPIC&HMIT 2017)*, San Francisco, CA, 2017.

[15] 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,* 2022.

[16] L. T. Maccarone and M. T. Rowland, "Advances in Qunatifying Data Harm and Physical Harm for Defense-in-Depth Cybersecurity Measures," in *Proceedings of the 13th International Nuclear Plant Instrumentation, Control Human-Machine Interface Technologies (NPIC&HMIT 2023)*, Knoxville, TN, 2023.