SANDIA REPORT
SAND2023-09408
Printed September 2023

Advanced Reactor Cyber Analysis and Development Environment (ARCADE) for System-Level Design Analysis

Andrew S. Hahn, Lee T. Maccarone, and Michael T. Rowland

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

ABSTRACT

Cybersecurity is a persistent concern to the safety and security of Nuclear Power Plants (NPPs), but has lacked data-driven, evidence-based research. Rigorous cybersecurity analysis is critical for the licensing of advanced reactors using a performance-based approach. One tool that enables cybersecurity analysis is modeling and simulation. The nuclear industry makes extensive use of modeling and simulation throughout the decision process but lacks a method to incorporate cybersecurity analysis with existing models. To meet this need, the Advanced Reactor Cyber Analysis and Development Environment (ARCADE) was developed. ARCADE is a suite of publicly available tools that can be used to develop emulations of industrial control system devices and networks and integrate those emulations with physics simulators. This integration of cyber emulations and physics models enables rigorous cyber-physical analysis of cyber-attacks on NPP systems. This report provides an overview of key considerations for using ARCADE with existing physics models and demonstrates ARCADE's capabilities for cybersecurity analysis. Using a model of the Small Modular Advanced High Temperature Reactor (SmAHTR), ARCADE was able to determine the sensitivity of the primary heat exchangers (PHX) to coordinated cyber-attacks. The analysis determined that while the PHX's failures cause disruption to the reactor, they did not cause any safety limits to be exceeded because of the plant design, including passive safety features. Further development of ARCADE will enable rigorous, repeatable, and automated cyber-physical analysis of advanced reactor control systems. These efforts will also help reduce regulatory uncertainty by presenting similar types of cybersecurity analyses in a common format, driving standard approaches and reporting.

ACKNOWLEDGEMENTS

This report was written for the U.S. Department of Energy Office of Nuclear Energy and satisfies milestone M3CT-23SN1103039. The authors would like to acknowledge the program leadership provided by Savannah Fitzwater (DOE-NE), Ben Cipiti (Sandia National Laboratories), and Katya Le Blanc (Idaho National Laboratory). The authors would like to acknowledge the insights provided by various industry stakeholders, including X-energy, NuScale Power, and Radiant Nuclear. Daniel Cole, Abhimanyu Kapuria, and Yifan Zhang of the University of Pittsburgh developed the Small Modular Advanced High-Temperature (SmAHTR) model and provided insights regarding its integration with ARCADE. Romuald Valme of Sandia National Laboratories assisted in modeling and simulation efforts presented in this report.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

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) to conduct cybersecurity research and development. 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).

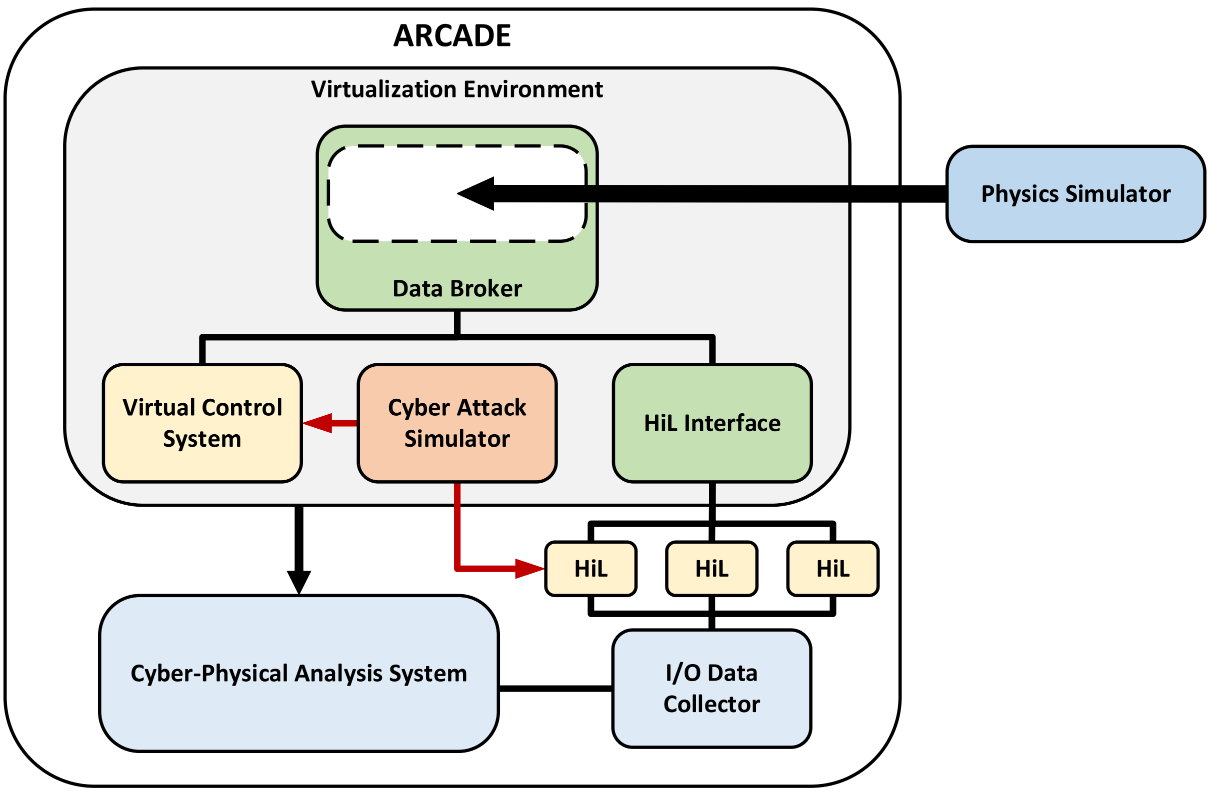

Figure 1. Advanced Reactor Cyber Analysis and Development Environment (ARCADE)

The key components of ARCADE are:

- Data Broker: software responsible for data exchange between the physics simulator, virtual control system, and hardware-in-the-loop (HiL) devices
- Virtual Control System: emulated industrial control system (ICS) devices and networks
- Cyber Attack Simulator: simulates the malicious manipulation of emulated ICS devices and HiL devices
- Hardware-in-the-loop (HiL) Interface: interface for connecting physical ICS devices to the virtual control system and Data Broker
- Input/Output (I/O) Data Collector: gathers data from HiL for cyber-physical analysis
- Cyber-Physical Analysis System: processing of cyber and physical data generated by experiments

The primary requirements for a physics model to be integrated with ARCADE are:

- Model must be real-time or faster than real-time
- Control surfaces must be modeled (e.g. when emulating a pump controller, a pump model must be included in the physics model). The fidelity of the modeling of the control surfaces can be scaled appropriately to the corresponding phase of design maturity

Additional design considerations include:

- Numeric stability and destabilization with the introduction of external control system loops
- Management of software licenses for virtual environments
- Timestep size should be smaller than the cycle time of the connected controllers

ARCADE's capabilities are demonstrated in this report using a model of the Small Modular Advanced High-Temperature Reactor (SmAHTR). SmAHTR is a fluoride-salt-cooled reactor that uses tri-structural isotropic (TRISO)-coated particle fuel and graphite as a moderator. Four SmAHTR reactors operate together to transfer energy to a salt vault through three integral primary heat exchangers (PHXs) per reactor. The energy stored in the salt vault is used to make steam to generate mechanical power in the turbines.

Two cyber-attack scenarios were simulated involving the manipulation of the power demand signal to the 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. ARCADE was used to demonstrate that the average temperature of the primary fluid increased but settled at a steady-state value for Scenario 1, but the average temperature increased steadily for Scenario 2. In both scenarios, it was assumed that the adversary has the capability to manipulate the power demand signal used to operate the pumps of the first reactor's PHXs.

These cybersecurity simulations serve to demonstrate the utility of ARCADE for SLDA. Understanding the physical consequences of a range of cyber-attacks should guide the design of systems and their network architectures. For example, Scenario 2 demonstrated that the primary fluid temperature continued to increase when three PHXs were manipulated. This result is of concern to plant safety. One cybersecurity strategy to prevent the adversary from gaining the access required to conduct this attack is to place the PHXs in separate networks (assuming the power demand signals are from independent locations). If the PHXs cannot be placed on separate networks or the power demand signals are not from independent locations, additional active cybersecurity measures are required.

These types of cybersecurity analyses need to consider the costs and efficacy of protection. ARCADE seeks to allow comparisons of design provisions, architecture, and functional design impacts to cybersecurity. This comparative analysis will enable a greater focus on the most effective cyber security solutions while minimizing cost and complexity. For SmAHTR, the PHX's may not require additional cybersecurity measures if design provisions, such as passive cooling systems, can be proven to already mitigate any consequence of cyber-attacks on the PHXs. These design provisions will then need to be evaluated for reliability, resilience, and possible need for redundancy.

Further development of ARCADE will enable rigorous, repeatable, and automated cyber-physical analysis of advanced reactor control systems. These efforts will also help reduce regulatory uncertainty by presenting similar types of cybersecurity analyses in a common format, driving standard approaches and reporting.

ACRONYMS AND TERMS

Acronym/Term	Definition
API	Application Programming Interface
AR	Advanced Reactor
ARCADE	Advanced Reactor Cyber Analysis and Development Environment
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
DCS	Distributed Control System
DCSA	Defensive Cybersecurity Architecture
DOE-NE	Department of Energy Office of Nuclear Energy
DRACS	Direct Reactor Auxiliary Cooling System
E2	Energy Exploration
FPGA	Field-Programmable Gate Array
HALEU	High Assay Low Enriched Uranium
HiL	Hardware-in-the-Loop
HTGR	High-Temperature Gas-Cooled Reactor
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
I/O	Input/Output
IPC	Inter-Process Communication
iPWR	Integral Pressurized Water Reactor
LWR	Light Water Reactor
NPP	Nuclear Power Plant
NQA	Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
PHX	Primary Heat Exchanger
PI	Proportional-Integral
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
POSIX	Portable Operating System Interface
RAM	Random-Access Memory
R&D	Research and Development
RX	Reactor
SeBD	Security-by-Design
SHX	Secondary Heat Exchanger
SLDA	System-Level Design Analysis

Acronym/Term	Definition
SmAHTR	Small Modular Advanced High-Temperature Reactor
SMR	Small Modular Reactor
SSCs	Systems, Structures, and Components
TCA	Tiered Cybersecurity Analysis
TRISO	Tri-structural Isotropic
UDP	User Datagram Protocol
VM	Virtual Machine
WNA	World Nuclear Association
ZMQ	ZeroMQ

1. INTRODUCTION

Advanced Reactor (AR) designers need analytical methods and tools to evaluate cybersecurity risks and develop mitigation strategies for their digital control systems. Rigorous, repeatable, and evidence-based cybersecurity analysis and evaluations require complex modeling and simulation platforms. To address this need, Sandia National Laboratories have 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 US Department of Energy Office of Nuclear Energy (DOE-NE) 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).

ARCADE allows physics simulators developed by AR designers to be integrated with a virtual distributed control system (DCS) that emulates the control systems and networks of a real AR. This merging of cyber and physical models and emulations enables AR designers to conduct comprehensive cyber-physical analysis of their integrated plant systems. ARCADE can also be used to conduct advanced cybersecurity R&D. ARCADE is leveraged extensively by the DOE-NE System-Level Design Analysis (SLDA) project that aims to align the application of the cybersecurity analyses with the system-level phase of plant design. For SLDA, ARCADE provides key insights regarding the physical impacts of design decisions, including the design of defensive cybersecurity architectures (DCSAs).

Analysis of systems with ARCADE can be aligned with the Tiered Cybersecurity Analysis (TCA) developed in the regulatory guide for the draft Title 10 of Code of Federal Regulations (10 CFR) 73.110 [1, 2]. ARCADE can be used to perform analyses in each tier of the TCA, providing insights regarding the mitigation/elimination of cyber-attack consequences by plant security-by-design (SeBD) features, the design of passive cybersecurity features (e.g., DCSA), and the implementation of active cybersecurity controls.

This report documents the key components of ARCADE and requirements for successful integration of AR physics models with the ARCADE environment throughout the phases of plant design maturity. ARCADE's capabilities are demonstrated with example cybersecurity simulations performed using a model of the Small Modular Advanced High-Temperature Reactor (SmAHTR).

This page left blank

2. BACKGROUND

Under the United States Nuclear Regulatory Commission (US NRC) Regulatory Guide 5.71 [3], licensees of light water reactors (LWRs) have been required to broadly apply a large set of technical and operational cybersecurity controls to all identified critical digital assets (CDAs). For advanced reactors (ARs), this prescriptive approach places a large time and resource burden on the licensee and does not allow the licensee the flexibility to prioritize the systems with the greatest potential for physical harm. The regulation that sets cybersecurity policy for ARs, Title 10 of Code of Federal Regulations (10 CFR) 73.110 specifies, "Technology neutral requirements for protection of digital computer and communication systems and networks," and is currently in draft review stages [1]. The draft rule proposes a graded approach to cyber security controls based on potential consequences of credible postulated attacks at each risk level [4].

The US NRC presented its regulatory efforts to address the requirements outlined in 10 CFR 73.110at the International Atomic Energy Agency (IAEA) Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors [2]. The presentation included a three-tier cybersecurity analysis approach proposed in the draft regulatory guide. The methodology is pre-decisional, but the concepts are referred to in this report as the Tiered Cybersecurity Analysis (TCA). The TCA is a cybersecurity assessment methodology that aligns domestic standards, international standards, and technical guidance to select Security-by-Design (SeBD) requirements to develop defensive network architectures and apply effective cybersecurity controls [4].

The TCA consists of three tiers and is shown in Figure 2. Tier 1 is Design and Impact Analysis and focuses on evaluating the capability of security-by-design (SeBD) features to eliminate or mitigate accident sequences caused by a cyber-adversary who is limited only by the physics of the plant design. Tier 2 is Denial of Access Analysis and focuses on developing passive Defensive Cyber Security Architecture (DCSA) features to deny the adversary access to the functions needed to conduct attacks that were not eliminated by SeBD features. Finally, Tier 3 is Denial of Task Analysis and focuses on preventing the adversary from conducting the specific tasks needed to conduct attacks that are not eliminated by SeBD or prevented by denial of access. For greater detail, readers are encouraged to refer to [2] and [5]. ARCADE must be able to support the analyses required in each tier of the TCA. The alignment of ARCADE's capabilities with the TCA will be discussed throughout this report.

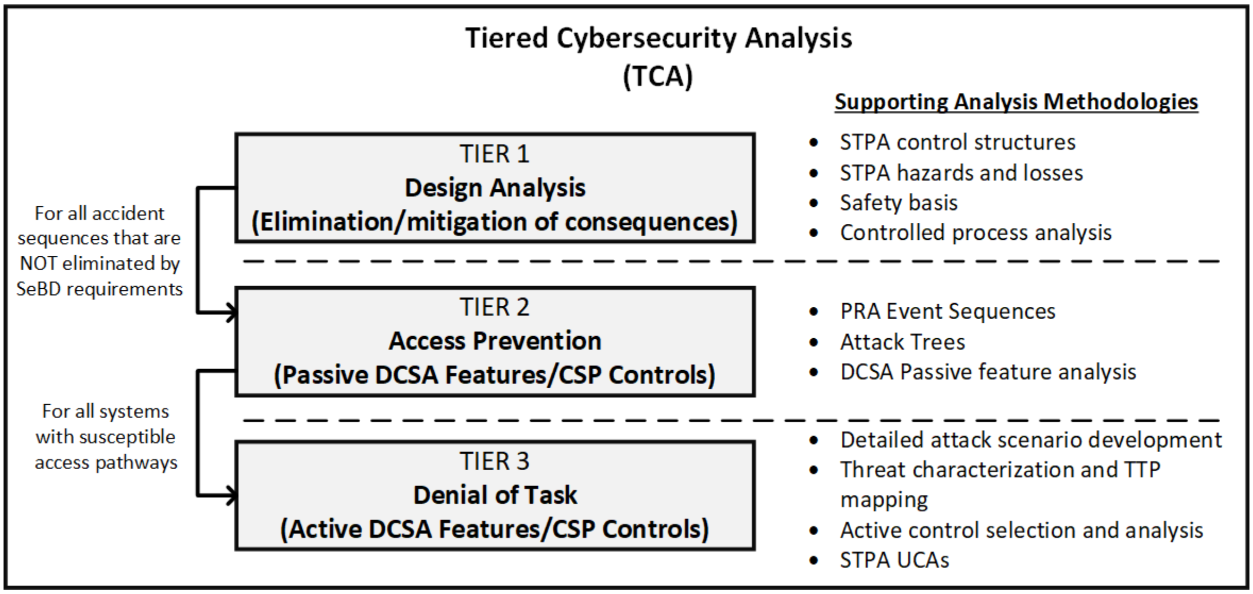

Figure 2: Tiered Cybersecurity Analysis (TCA) [5]

3. SURVEY OF ADVANCED REACTOR MODELS

Industry engagement is an ongoing and critical element of ARCADE development. An understanding of industry modeling and simulation tools is essential to ensure compatibility with the ARCADE platform. This section provides an overview of several models developed by advanced reactor vendors. All information presented in this section is publicly available.

3.1. X-energy Xe-100 Reactor

The Xe-100 is a pebble bed High-Temperature Gas-Cooled Reactor (HTGR) designed by X-energy. High-Assay Low-Enriched Uranium (HALEU) will fuel the reactor in tri-structural isotropic (TRISO) particles suspended in the graphite pebbles [6]. The reactor is graphite moderated, uses helium as a primary coolant, and generates steam for Rankine cycle power conversion or process heat. Continuous refueling is enabled by the pebble bed design. Pebbles are removed from the bottom of the core and replenished at the top.

X-energy has performed extensive modeling of the Xe-100 and utilizes Flownex as the simulation platform to perform full system analysis for the development of control philosophy [7]. Flownex allows high fidelity transient analysis and offers Nuclear Quality Assurance (NQA) 1 compliant code and is ideal for developing control systems. The Flownex platform allows C# code integration natively which offers a significant foothold for integrating ARCADE.

3.2. NuScale US600 SMR

The NuScale reactor is an integral pressurized water reactor (iPWR) that is expected to operate in a fleet of multiple reactors that are housed in the same building. The reactor primary coolant circuit is entirely self-contained in the reactor vessel and relies entirely on natural circulation, eliminating the need for primary coolant pumps [8]. The steam generator is also contained in the reactor vessel which is submerged in a pool that acts as an emergency safety heat rejection path. The design is focused on passive safety and attempts to eliminate the possibility of any severe accident pathway.

NuScale has developed five Energy Exploration (E2) Centers that simulate the NuScale VOYGR SMR control room [9, 10]. The purpose of the E2 Centers is to allow users to interface with a realistic NuScale control room and observe the plant's response to operator input and simulated scenarios. The E2 documentation does not specify the fidelity of the physics model, but the E2 Centers are a potential opportunity for integration with ARCADE for educational purposes aligned with the E2 Center mission.

NuScale has also demonstrated commitment towards implementing digital twins in their plants. NuScale is implementing the Aras Product Lifecycle Management (PLM) platform to deliver a digital twin with traceability to product data [11]. Digital twins require high-fidelity modeling and would provide an opportunity for integration of a sophisticated physics model with ARCADE.

3.3. Radiant Kaleidos Reactor

The Kaleidos reactor is a small form factor high-temperature gas-cooled reactor (HTGR) that allows an entire nuclear power plant to be fit in a shippable container. The reactor will be fueled by HALEU, moderated by metal hydride, and cooled by helium [12, 13]. The power conversion on the secondary side will be accomplished with a supercritical CO_2 cycle. The control system, like the rest of the power plant, should be self-contained. This setup should allow for high efficiency, portability, and significant safety margins.

One of the novel aspects of Radiant is their simulation and modeling capabilities. The Kaleidos reactor is entirely modeled and simulated with high fidelity using in-house multi-physics simulation engines [14]. The SimEngine platform enables real-time simulation of the Kaleidos reactor under startup, shutdown, and off-normal scenarios [14]. The high fidelity and integrability of the simulation engines make the Kaleidos reactor a highly valuable research subject for ARCADE.

4. ADVANCED REACTOR 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 3. The remainder of this section describes ARCADE and is adapted from [15, 16].

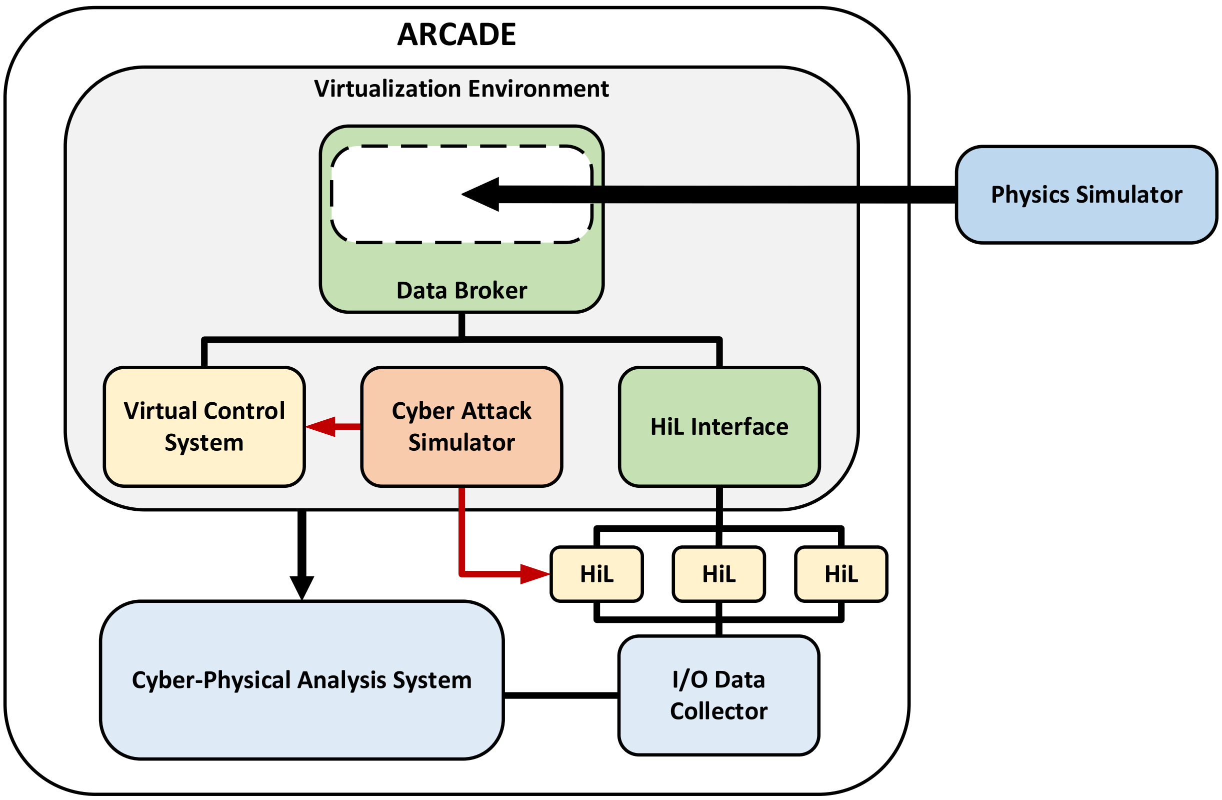

Figure 3: Advanced Reactor Cyber Analysis and Development Environment (ARCADE) Functional Block Diagram [15]

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 [17]. 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 [18]. 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 [19]. ARCADE incorporates ManiPIO into its cyber-attack simulation suite that is hosted on a Kali Linux virtual machine (VM).

ARCADE does not include a physics simulator. This is to enable researchers to conduct cybersecurity R&D on their specific systems. While ARCADE does not include a physics simulator, it is important to understand how some key tools were developed around the Asherah NPP Simulator [20]. The Data Broker, ManiPIO, and many elements of the virtual control system were first developed using Asherah as the physics simulator [18, 19]. 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.

5. MODEL INTEGRATION EFFORTS

The efforts to integrate models and simulations into ARCADE are centered around the Data Broker system. This system is the core component that bridges the physics simulations and models of advanced reactor designers and the emulated control system of ARCADE. The Data Broker was originally designed with two central questions in mind: can data and actuation information be transferred fast enough to accurately represent a controller connecting to a real physical process, and can this scale to the number of controllers in a real NPP? These concerns drove the initial development to utilize the fastest available communication methods and compiled intermediary language code base. The system was designed with careful consideration for computational load balancing through distributed computing. The result was an exceptionally fast and highly scalable system that allows significant modularity.

The initial target simulator (the Asherah NPP Simulator [9]) was developed in Simulink which has a method to allow C code integration in the model. The Simulink C MEX S-Function allows any Simulink program to utilize arbitrary C code and, if correctly designed, compile that code with the program into an executable. Utilizing the C MEX S-Function, a connector program was designed to establish a shared memory link to the Data Broker to exchange live physics and actuation data. This data updates the internal Data Broker database which interacts with the threads responsible for exchanging data with the end points.

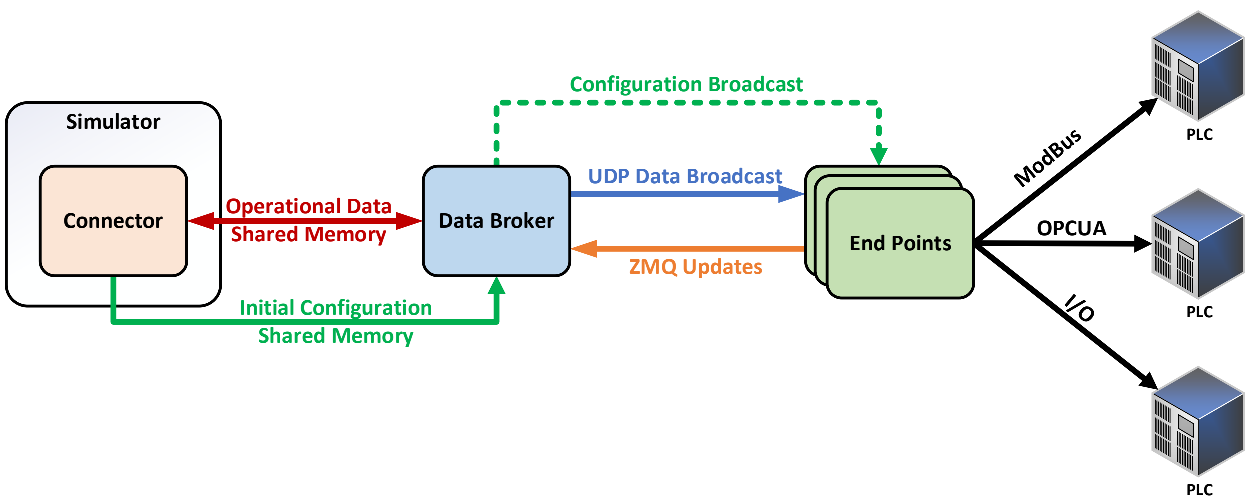

Figure 4: Functional Block Diagram of the Data Broker System

Endpoints handle the communication with PLCs directly, either via a network protocol or directly on the I/O. Each endpoint can handle communication with multiple PLCs and is Python-based to allow a high degree of interface flexibility. On startup, the Data Broker broadcasts configuration data to the endpoints, assigning them their functions and data (Figure 4). Two threads in the Data Broker then continue the communication with the endpoints, the UDP broadcaster, and ZMQ server. The data exported from the simulator is broadcast via UDP to all the endpoints at every timestep, providing them a constant stream of updated physics data. The UDP broadcast allows a stream of live data with a constant overhead for the network regardless of the number of endpoints. When an endpoint responds to the Data Broker it uses a ZMQ socket to pass a value and its variable name to the ZMQ server at the Data Broker. These messages are short, uniform, and rapidly parsed. This communication system allows resource conservation and an asynchronous distributed computational solution to managing large DCS simulations.

The number of endpoints the system can handle has not been reached in testing. The developed communication and computational system have enabled a two-core 4 GB RAM VM to manage 12 end points simultaneously while handing the Asherah NPP simulation as well. The intent was to off load the more difficult, slow, and computationally expensive parsing to the end points. It is much easier to spawn hundreds of low powered nodes than it is to allocate a single powerful node. The limiting factor would be the ZMQ server, but this server was made in a modular thread that can replicated with different listening ports. Should the limit ever be met, the capacity can be doubled with two lines of code.

5.1. Model Integration Plans

The initial release of the Data Broker was limited to Simulink and C code model integrations and only on Unix/Linux machines. It relies on POSIX Inter Process Communication (IPC) standards that are only available in Unix/Linux architectures. Many AR designers use Windows-based simulators and models that have no Linux equivalent, creating a major gap for integration. To alleviate this shortcoming a new branch of the Data Broker was made specifically for Windows. The source code was revamped and using the Windows API for IPC. Then the connector was entirely redeveloped in C# to operate in native Windows applications.

Currently the C# connector is at a stage of a generic API; it defines all the functionality needed to perform the functions necessary to communicate with the Windows Data Broker. The next step for this connector is to be integrated with a simulator or modeling program in a way that conforms to how the physics solution is computed. Flownex was identified as the first candidate to integrate with the C# and Windows Data Broker. Flownex is used by many AR designers to make real-time physics models of their NPP for the development of I&C systems [21].

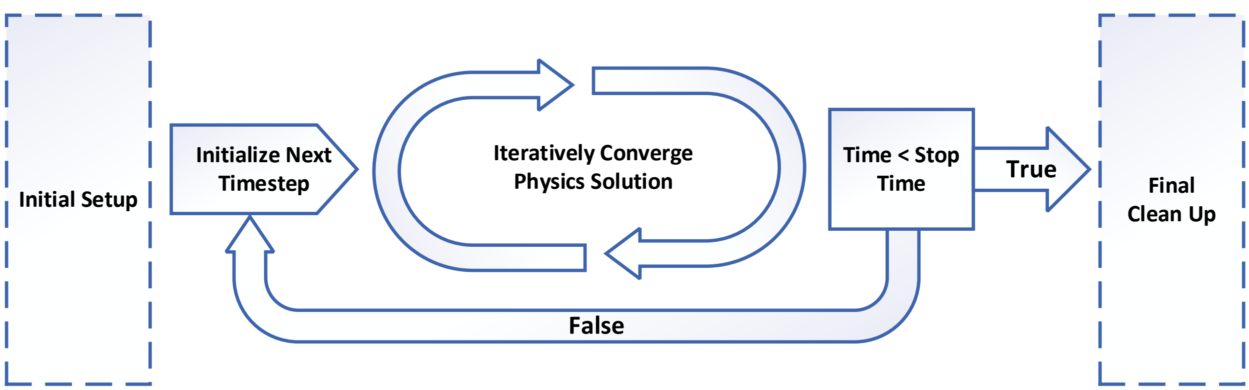

Figure 5: Time-Based Physics Solution Flow Chart

An integration strategy was developed through investigation of Flownex's capabilities. Flownex uses C# programs and scripts as a central tool for developers to design novel physics solvers. This allows a large degree of freedom for designers, but it also allows the Data Broker connector to integrate seamlessly. Coincidentally Flownex and Simulink have relatively similar timestep solution stages which are generalized in Figure 5. An initialization step allows variables and initial conditions to be established before the transient computation begins. Each timestep starts with advancing the simulation time and executing the solvers which iterate to converge on a solution for the conditions of the simulation at that timestep. When the convergence criteria are met, the timestep ends and sets up conditions for the next timestep. When the length of time requested for the simulation is exceeded, the simulation stops and cleans up the environment safely.

This solution method is generally similar across the time-based physics models that have been investigated in this research because it is intuitively based on linear calculation methods. This similarity provides a great benefit to the Data Broker because once one modeling software is integrated in a particular code base, it should make integration with any modeling software in that code base significantly easier. Changing the API references for each phase of the time solution to those for the specific simulator should be all that is needed to integrate another software. This greatly reduces overall development cost and time. When Flownex integration is complete, it should allow rapid integration with any C# simulators in Windows.

Greater integration across simulators will also allow a critically needed capabilities for AR designers beyond ARCADE. Co-simulation is rapidly becoming an important tool for designers to drastically improve simulation and modeling resources. ARCADE is itself a co-simulator for the I&C, network architecture, and DCSA, but through its development a high-speed data connection was created that could benefit new simulation efforts. A cross-platform, highly integrated, high-speed simulation data highway would allow new modes of simulation such as multi-unit simulation and parallel coupled high-fidelity physics simulators. With more integrations, the Data Broker can provide the cross-platform support of its high-speed physics data highway to support expanded types of co-simulations.

5.2. Model Integration and Design Maturity

The World Nuclear Association (WNA) has defined a series of four design maturity phases to describe the development of small modular reactors (SMRs) [22]. The design maturity phases are shown in Figure 6. The first phase of design maturity is the conceptual phase where the reactor concept is developed. In Phase 1 critical questions are asked and major risks are identified. The second phase of design maturity is plant-level design. In Phase 2 the requirements and design parameters of key systems, structures, and components (SSCs) are defined. The third phase of design maturity is system-level design. In Phase 3 the requirements and design parameters of key SSCs are further refined and other plant systems are defined. Finally, the fourth phase of design maturity is component-level design. In Phase 4 the engineering details are finalized for SSCs to allow for manufacturing to begin [22].

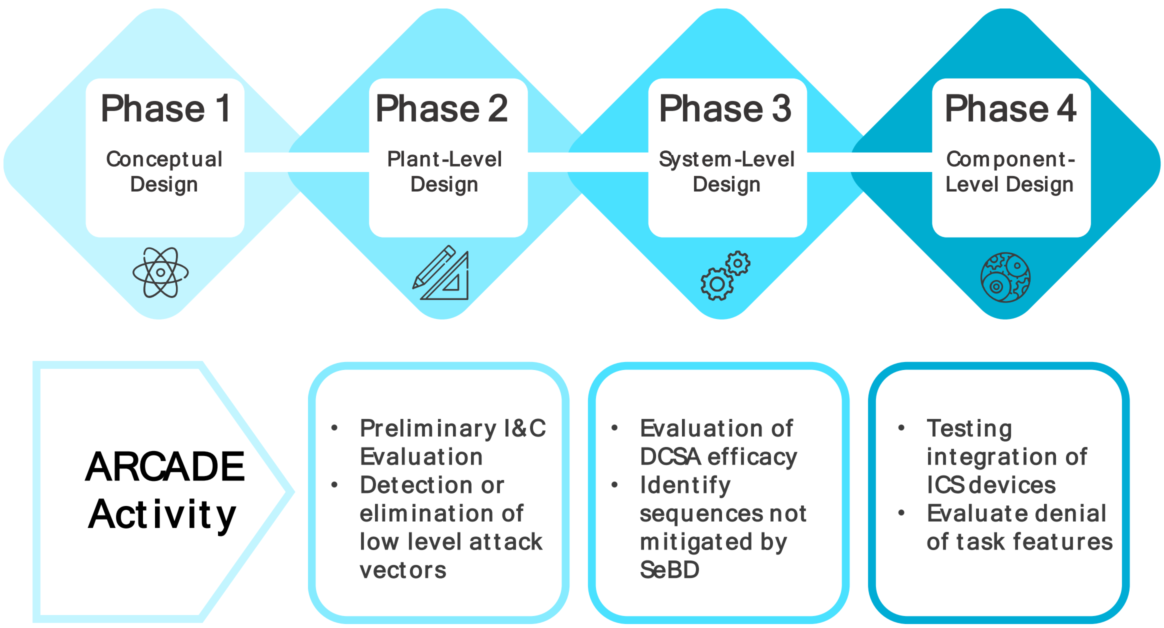

Figure 6: Plant Design Phases of Maturity [22]

ARCADE must be able to support cybersecurity analysis for the plant-level, system-level, and component-level design phases. The conceptual design phase is not applicable to ARCADE because this phase is focused purely on reactor physics without consideration of interfacing SSCs. The design of interfacing SSCs begins in the plant-level design phase and therefore ARCADE must be able to support design analysis beginning in this phase. The activities enabled by ARCADE at each design phase and TCA tier are summarized in Table I.

Table I: ARCADE Benefits by Design Phase [15]

Design Phase	TCA Tier	ARCADE Benefits
Concept	Begin Tier 1	N/A: focused exclusively on reactor design
Plant-Level	Complete Tier 1	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	Tier 2	Evaluation of DCSA interaction with high-fidelity physics models to evaluate attack sequences not mitigated or eliminated by security-by-design features
Component-Level	Tier 3	Testing of integration of specific ICS devices through emulation or HiL and denial of adversary's ability to conduct specific tasks

Integration of physics models with ARCADE becomes slightly more challenging as the complexity of the model increases. This increased difficultly is not due to integrating the modeling software and Data Broker, it is due to the emulation of the network and control system. As the complexity of the design increases the number of devices and networks also increase. This may only be an initial increase in effort however, since once a piece of hardware has been sufficiently emulated that effort never has to be replicated again. Since most hardware has yet to be emulated in the environment it incurs a high development cost. As the available emulated hardware library increases it will only take a configuration file or logic file from the AR designer to implement a piece of hardware or component in ARCADE.

There are a few ways to reduce the cost and time to implement designs in ARCADE. Using HiL can significantly reduce integration time of components, but it is costly and increases the physical footprint of an ARCADE instance. It is preferable to emulate hardware, which would require source code or firmware images from the hardware vendors to expedite emulation and ARCADE component implementation. Control logic is another source of significant effort for ARCADE integration. Often models do not include the control logic in a format that is easily implemented in controllers. This is more of an issue in early design phases, but clear control logic documentation or even ladder logic files would speed integration.

There are some limits to the abilities of ARCADE due to the nature of physics models that becomes increasingly important for Tier 3 analysis. Typically, NPP physics models do not include the building structure and layout that do not have a direct influence on the processes being modeled. The layout and structure of the buildings and equipment locations can influence adversary pathways considered in Tier 3. Additionally, ARCADE is limited by the fidelity and comprehensive modeling of the system under analysis. It cannot adequately evaluate AR systems without sufficiently detailed modeling and specification commensurate with the phase of development.

5.3. Model Requirements

As more codebases and simulation platform connectors are developed for model integration with ARCADE, the number of requirements for model integration will be reduced. There are two major requirements that will not be eliminated with further development:

- Real-time operation is a minimum requirement for successful model integration. Control system components use real-time operating systems and are thus locked into real-time operation. For the simulator to interact with a control system in a manner contiguous with their normal operation, it must match their inherent real-time operation.
- Control surfaces must be modeled. For those controllers to interact with the physics, the control surfaces they would control in a real system must be modeled in the simulation. For a pump controller to integrate with a simulator, that simulation must have a pump model with inputs and sensors that are at least similar to a real system.

During development and operation of several Simulink models, some modeling recommendations were identified. These are not strictly requirements, but ease integration to ARCADE.

- Numeric stability can become the most frustrating issue in integration. When a model is highly sensitive to single timestep delays in signals, it can be destabilized by the introduction of any external control system loop.
- Software licenses are difficult to manage in a virtual environment that is isolated from the internet. Many licenses for software are locked to hardware IDs which are randomized or sometimes null for VMs. Managing these licenses requires special consideration for the virtual environment.
- Timestep size should be smaller than the cycle time of the PLCs connected. This increases the likelihood that each command or signal from the PLCs are input into the simulator. The system is asynchronous; if the timestep is greater or equal to the cycle time of the PLC, the simulator cannot pick up the commands and signals from each PLC cycle.

These requirements are core to allowing ARCADE to integrate with the model, but they do not inform the analysis possible with the information. The model alone can sometimes provide the necessary information for an analysis of general sensitivity of the control surfaces. More information about the design of the control system and its network is required to perform more advanced analysis. Developing conceptual architectures and mock network designs can only drive theoretical advances to the security of a given model and risks invalidating findings. Increasingly advanced analysis requires increasing amounts of design information input which is described in Table II.

Table II. ARCADE Inputs Necessary for TCA

Design Phase	TCA Tier	ARCADE Inputs
Concept	Begin Tier 1	N/A: focused exclusively on reactor design
Plant-Level	Complete Tier 1	• Physics model with control surfaces • Equations/logic to drive control surfaces • Basic I&C network architecture (Division of controller security levels)
System-Level	Tier 2	• Physics model with control surfaces • PLC control logic • Detailed I&C architecture • Detailed network architecture
Component-Level	Tier 3	• Physics model with control surfaces • PLC software with logic • Detailed I&C architecture • Detailed network architecture • Emulations/HiL of exact PLCs to be used • Emulations of exact network components to be used • Building designs with equipment locations and access requirements.

6. DEMONSTRATION OF ARCADE CAPABILITIES

A model of a small modular advanced high-temperature reactor (SmAHTR) model was used to demonstrate ARCADE's cybersecurity analysis capabilities. Two cybersecurity scenarios were investigated. In Scenario 1, the adversary decreases the power demand of the first primary heat exchanger (PHX). In Scenario 2, the adversary sequentially decreases the power demand of all three PHXs. The following results are quoted from a conference paper written during this research [16].

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

SmAHTR is a fluoride-salt-cooled reactor that was designed be easily transported to and assembled at remote sites [23]. SmAHTR uses TRISO particle fuel and graphite as a moderator. The following SmAHTR description and model development is based upon a pre-conceptual design report [23], and is quoted from a conference paper written during this research [16].

SmAHTR employs three in-vessel 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.

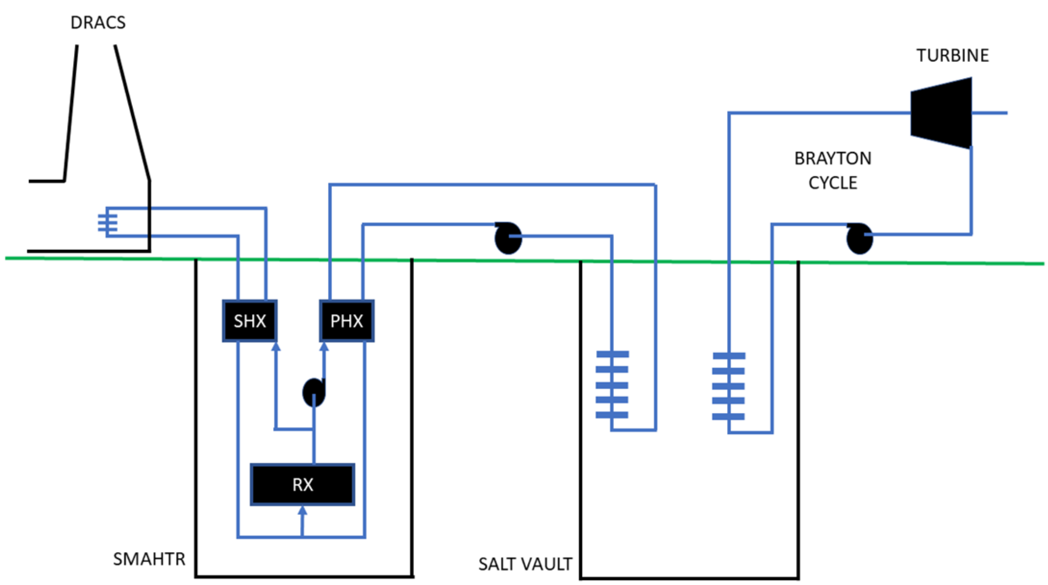

Figure 7: SmAHTR Simulink model includes the reactors, salt vault, and Brayton cycle.

A SmAHTR model has been developed and used in research at the University of Pittsburgh [24, 25]. Although the University of Pittsburgh's SmAHTR model was originally developed for other applications, the model has been repurposed for cybersecurity R&D. 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 7. 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 proportional-integral (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.

6.2. SmAHTR 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 8. The results shown were selected because of their relevance for heat transfer from the reactor to the salt vault. The results shown in Figure 8 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 8a and Figure 8b, the temperatures of the secondary side of the PHX are shown in Figure 8c and Figure 8d, and the temperatures of the primary side of the PHX are shown in Figure 8e and Figure 8f.

6.3. SmAHTR 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 9. Figure 9 has the same structure as Figure 8.

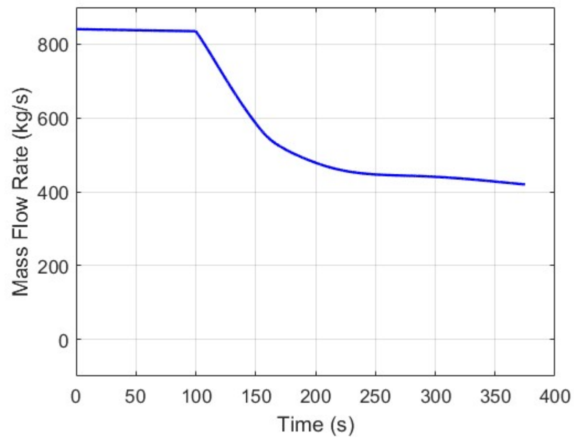

Figure 8a: Reactor 1 PHX Secondary Coolant Mass Flow Rate

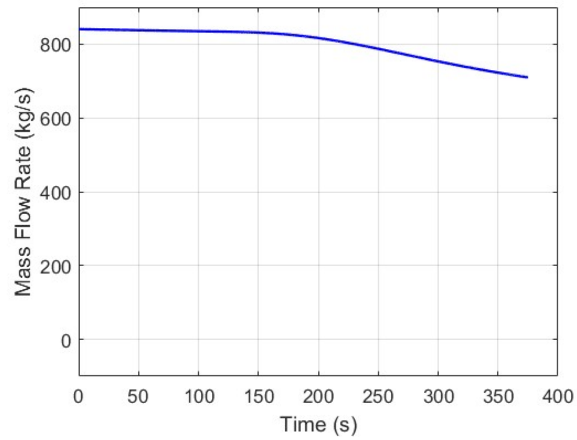

Figure 8b: Reactor 2/3/4 PHX Secondary Coolant Mass Flow Rate

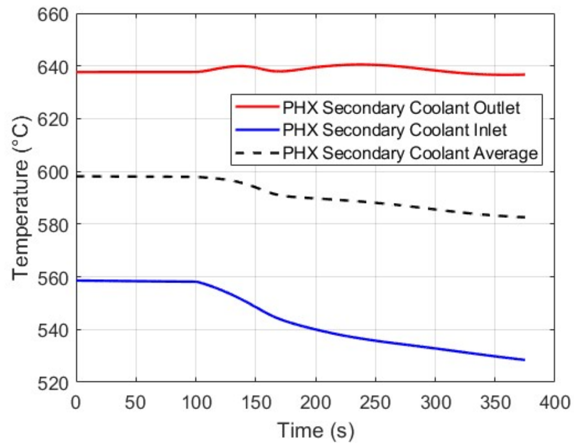

Figure 8c: Reactor 1 PHX Secondary Coolant Temperature

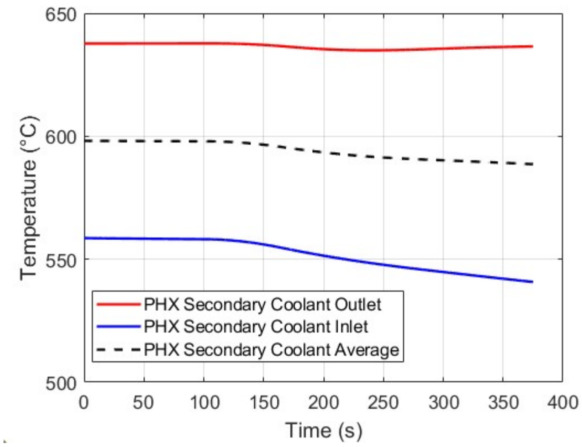

Figure 8d: Reactor 2/3/4 PHX Secondary Coolant Temperature

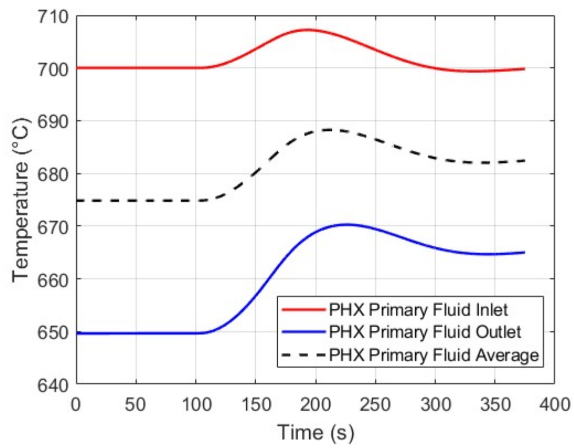

Figure 8e: Reactor 1 PHX Primary Fluid Temperature

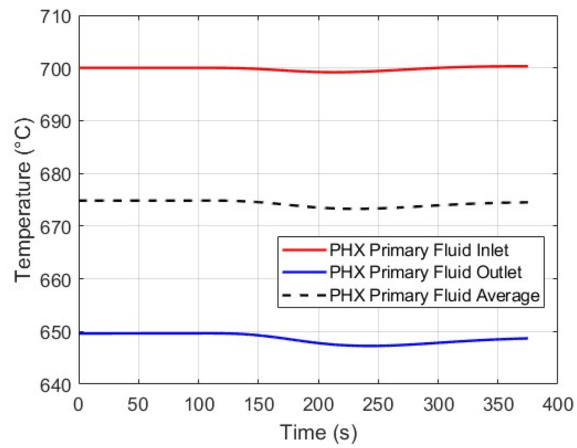

Figure 8f: Reactor 2/3/4 PHX Primary Fluid Temperature

Figure 8: Simulation Results for Manipulation of One PHX [16]

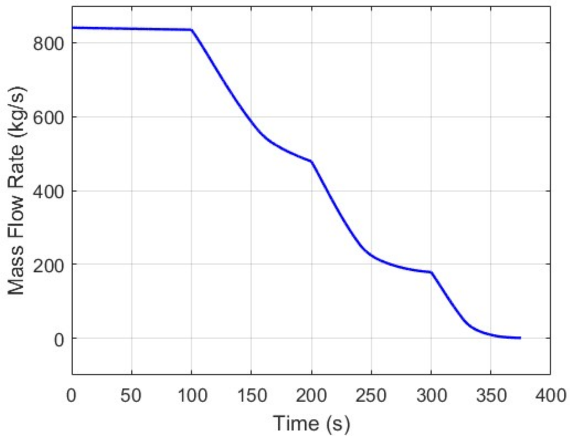

Figure 9a: Reactor 1 PHX Secondary Coolant Mass Flow Rate

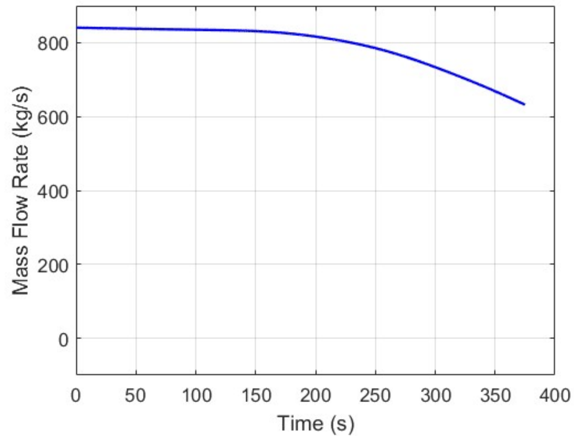

Figure 9b: Reactor 2/3/4 PHX Secondary Coolant Mass Flow Rate

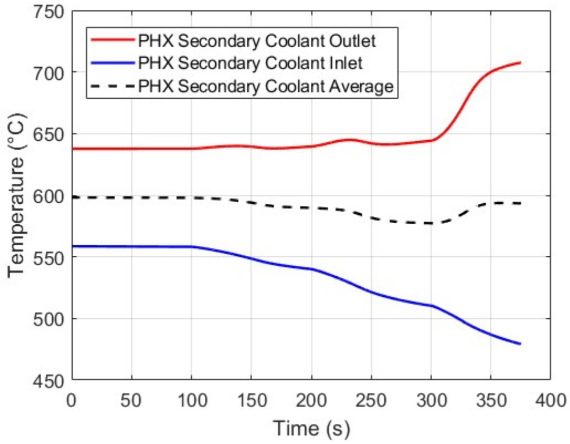

Figure 9c: Reactor 1 PHX Secondary Coolant Temperature

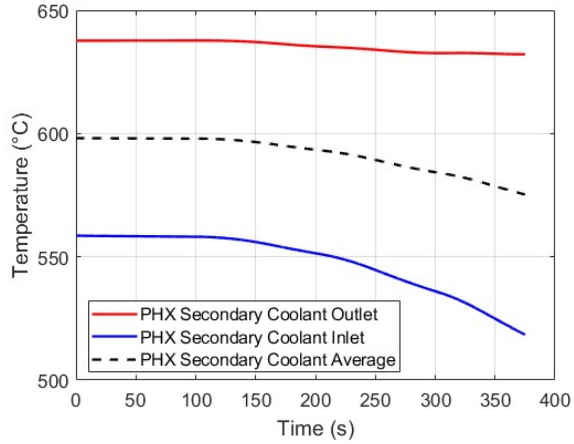

Figure 9d: Reactor 2/3/4 PHX Secondary Coolant Temperature

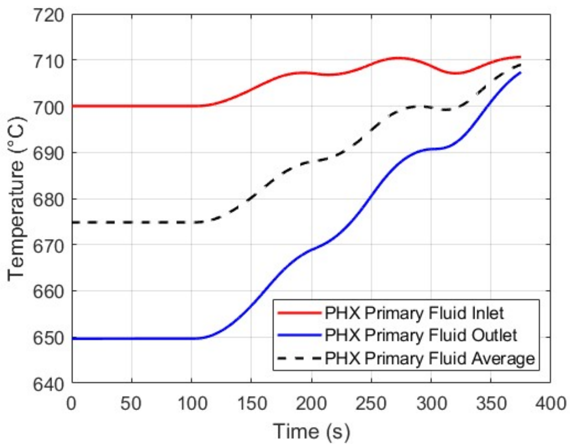

Figure 9e: Reactor 1 PHX Primary Fluid Temperature

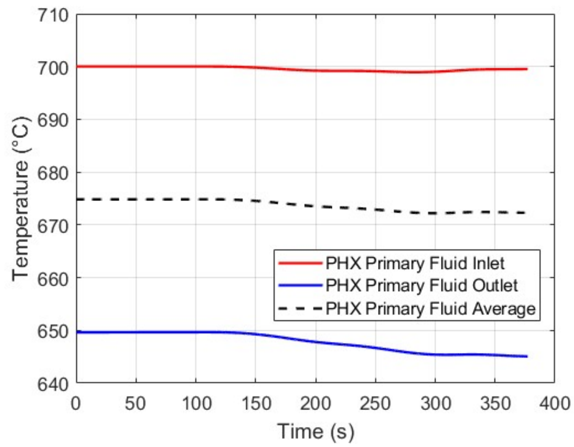

Figure 9f: Reactor 2/3/4 PHX Primary Fluid Temperature

Figure 9: Simulation Results for Manipulation of Three PHXs [16]

6.4. SmAHTR Analysis

In both scenarios, the secondary coolant mass flow rate through the Reactor 1 PHXs were reduced as the power demand was decreased (Figure 8a and Figure 9a). 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 8c and Figure 9c). 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 8e and Figure 9e). 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 8b and Figure 9b), the temperatures of the secondary coolant for the Reactors 2, 3, and 4 PHXs were reduced (Figure 8d and Figure 9d), and the temperatures of the primary fluid were the least affected by changes to the Reactor 1 PHX power demand (Figure 8f and Figure 9f).

These cybersecurity simulations serve to demonstrate the utility of ARCADE for SLDA. Understanding the physical consequences of a range of cyber-attacks should guide the design of systems and their network architectures.

In Scenario 1 the primary fluid temperature increased and settled at a steady-state value when one PHX was manipulated. If this steady-state value is within design specifications, then this cyber-attack scenario is not a safety concern. If the steady-state value exceeds design specifications, then cybersecurity measures are required to deny the adversary the ability to conduct the attack.

In Scenario 2 the primary fluid temperature continued to increase when three PHXs were manipulated. This result could be of concern to plant safety. One cybersecurity strategy to prevent the adversary from gaining the access required to conduct this attack is to place the PHXs in separate networks (assuming the power demand signals are from independent locations). If the PHXs cannot be placed on separate networks (or the power demand signals are not from independent locations), additional active cybersecurity measures are required.

During these experiments with the SmAHTR model, design safety margins were not exceeded. This was surprising as even with a sudden and total loss of forced cooling, fuel temperatures maintained within safe limits. The negative reactivity temperature coefficient and the DRACS seemed to reduce the reactor power and provide enough cooling support to mitigate an extreme temperature peak. This could be simply a model limitation on the point kinetics or the 1-D thermohydraulics. This finding points to design provisions providing robust cyber defense but require further investigation with physics models with greater fidelity.

This page left blank

7. CONCLUSION

ARCADE is a suite of open-source network emulation tools developed and implemented to enable the rigorous, repeatable, and evidence-based cybersecurity analysis and evaluation of ARs require complex modeling and simulation platforms. Using ARCADE, AR designers can leverage existing physics simulators for their cybersecurity analyses. Understanding how AR SeBD features mitigate or eliminate the consequences of cyber-attacks is critical to conducting performance-based cybersecurity analysis such as the TCA. ARCADE was developed as a robust toolset to enable AR designers to conduct comprehensive cyber-physical analysis of their facilities throughout the plant design process.

The two primary requirements for a physics model to be successfully integrated with ARCADE are that the model must be real-time or faster than real-time and all control surfaces must be modeled. The fidelity of the modeling of the control surfaces can be scaled appropriately to the corresponding phase of design maturity. Additional design considerations include the numeric stability of the model, management of software licenses for virtual environments, and specifying a timestep size smaller than the cycle time of the connected controllers.

Further development of ARCADE will enable rigorous, repeatable, and automated cyber-physical analysis of advanced reactor control systems. The analysis of sets of cyber-attack scenarios should be automated and integrated with the design process to enable AR designers to understand the impact of design decisions on cybersecurity. Further development and automation of data visualization is also required to enable AR designers to understand the extensive data that ARCADE can provide. These efforts will also help reduce regulatory uncertainty by presenting similar types of cybersecurity analyses in a common format, driving standard approaches and reporting.

This page left blank

REFERENCES

[1] U.S. Nuclear Regulatory Commission, "DRAFT 10 CFR Part 73, Section 10: Technology Neutral Requirements for Protection of Digital Computer and Communication Systems and Networks," in *U.S. Code of Federal Regulations*, Rockville, MD, 2022.

[2] J. Jauntirans, I. Garcia and M. Rowland, "U.S.A. Regulatory Efforts for Cyber Security of Small Modular Reactors/Advanced Reactors," in *IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors*, Vienna, Austria, 2021.

[3] U.S. Nuclear Regulatory Commission, "Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities," Rockville, MD, 2010.

[4] L. T. Maccarone and M. T. Rowland, "The Sliding Scale of Cybersecurity Applied to the Cybersecurity Analysis of Advanced Reactors," in *American Nuclear Society 13th Nuclear Plant Instrumentation, Control, & Human-Machine Interface Technologies*, Knoxville, TN, 2023.

[5] J. James, J. Mohmand, L. Maccarone, D. R. Sandoval, A. Haddad, M. T. Rowland and A. J. Clark, "Consequence Modeling and Simulation of Hazardous Events for Advanced Reactors," Sandia National Laboratories, Albuquerque, NM, 2023.

[6] DOE-NE, "X-energy's TRISO-X Fuel Fabrication Facility to Produce Fuel for Advanced Nuclear Reactors," Department of Energy, 8 April 2022. [Online]. Available: https://www.energy.gov/ne/articles/x-energys-triso-x-fuel-fabrication-facility-produce-fuel-advanced-nuclear-reactors.

[7] X-Energy, "X-energy Xe-100 Reactor Initial NRC Meeting," NRC, 2018.

[8] T. Bergman, S. Mirsky, S. Pope and S. Unikewicz, "The NuScale Design," NRC, 2016.

[9] NuScale Power, LLC, "The NuScale Energy Exploration (E2) Center," 2022. [Online]. Available: https://www.nuscalepower.com/-/media/nuscale/pdf/fact-sheets/e2c-fact-sheet.pdf. [Accessed 12 August 2023].

[10] NuScale Power, LLC, "E2 Centers," 2023. [Online]. Available: https://www.nuscalepower.com/en/products/e2-centers. [Accessed 12 August 2023].

[11] J. Kasper, "The Digital Twin: Everything, Everywhere, All at Once – Part 3," Aras Community, 11 July 2023. [Online]. Available: https://www.aras.com/community/b/english/posts/the-digital-twin-everything-everywhere-all-at-once---part-3. [Accessed 12 August 2023].

[12] Radiant Nuclear, "Radiant Industries Partners with Centrus Energy to Secure Commercial HALEU Supply for Kaleidos Portable Microreactor," 26 January 2023. [Online]. Available: https://www.radiantnuclear.com/blog/radiant-centrus-partnership/. [Accessed 15 August 2023].

[13] Radiant Nuclear, "Radiant products and services," 9 August 2022. [Online]. Available: https://www.radiantnuclear.com/blog/radiant-products-and-services/.

[14] J. Tompkins, B. Betzler, B. Urberger and D. Bernauer, "Design and Demonstration of the Kaleidos Portable Nuclear Microreactor," in *TRTR-IGORR*, College Park, MD, 2023.

[15] 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.

[16] L. T. Maccarone, A. S. Hahn, R. Valme, M. T. Rowland, A. Kapuria, Y. Zhang and D. G. Cole, "Advanced Reactor Cyber Analysis and Development Environment (ARCADE) for University Research," in *TRTR-IGORR Joint Research Reactor Conference*, College Park, MD, 2023.

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

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

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

[20] 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.

[21] Flownex Simulation Environment, "Nuclear & SMR," [Online]. Available: https://flownex.com/industries/nuclear-smr/. [Accessed 12 August 2023].

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

[23] 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.

[24] 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.

[25] 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.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Ben Cipiti	8845	bbcipit@sandia.gov
Lon Dawson	8851	ladawso@sandia.gov
Andrew Hahn	8851	ashahn@sandia.gov
Lee Maccarone	8851	lmaccar@sandia.gov
Michael Rowland	8851	mtrowla@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya Le Blanc	katya.leblanc@inl.gov	INL
Savannah Fitzwater	savannah.fitzwater@nuclear.energy.gov	DOE-NE

This page left blank

This page left blank

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.