SANDIA REPORT
SAND2023-11782
Printed October 2023

System-Level Design Analysis for Advanced Reactor Cybersecurity

Lee T. Maccarone, Andrew S. Hahn, 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.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

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

The purpose of this report is to enable effective cybersecurity analysis in the system-level design phase by identifying and demonstrating cybersecurity analysis methodologies applicable to system-level design. The primary analysis framework considered in this report is the Tiered Cybersecurity Analysis (TCA). The TCA is a cybersecurity assessment methodology developed in the regulatory guide for the draft 10 CFR 73.110 and aligns domestic standards, international standards, and technical guidance. The resulting System-Level Design Analysis (SLDA) for cybersecurity is focused on the design of control architectures that are informed by cybersecurity analyses. One tool that enables cybersecurity analysis is modeling and simulation. Sandia National Laboratories developed a modeling and simulation environment called the Advanced Reactor Cyber Analysis and Development Environment (ARCADE) to enable rigorous cyber-physical analysis of cyber-attacks on nuclear power plant systems. 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. ARCADE was used to demonstrate SLDA with a model of the Small Modular Advanced High Temperature Reactor (SmAHTR). ARCADE was used to analyze the cyber-physical consequences of cyber-attacks on a set of candidate control architecture designs and a design was selected based on postulated design criteria.

ACKNOWLEDGEMENTS

This report was written for the U.S. Department of Energy Office of Nuclear Energy and satisfies milestone M2CT-24SN11020311. 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). 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 Sandia National Laboratories' Advanced Reactor Cyber Analysis and Development Environment (ARCADE).

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The purpose of this report is to enable effective cybersecurity analysis in the system-level design phase by identifying and demonstrating cybersecurity analysis methodologies applicable to system-level design. The primary analysis framework considered in this report is the Tiered Cybersecurity Analysis (TCA). The TCA is a cybersecurity assessment methodology developed in the regulatory guide for the draft Title 10 of Code of Federal Regulations (10 CFR) 73.110. The TCA 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.

The system-level design phase is characterized by refining the requirements and design parameters of key systems, structures, and components (SSCs) and defining plant systems not defined in earlier phases of plant design. Key outputs of the system-level design phase include piping and instrumentation diagrams and a refined instrumentation and control (I&C) architecture. The resulting System-Level Design Analysis (SLDA) for cybersecurity is focused on the design of control architectures that are informed by cybersecurity analyses.

One tool that enables SLDA 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 (ICS) 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 nuclear power plant systems.

SLDA was demonstrated in this report using a model of the Small Modular Advanced High-Temperature Reactor (SmAHTR) in ARCADE. 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.

Four candidate designs were considered for the control architecture of the pumps associated with the PHXs for a SmAHTR unit. The candidate designs included a minimum of one and a maximum of six programmable logic controllers (PLCs) to control the pumps. The candidate designs are:

1. One PLC: One PLC controls all six pumps associated with the PHXs
2. Primary and Secondary Side Control: One PLC controls all three pumps on the primary side of the PHXs and one PLC controls all three pumps on the secondary side of the PHXs
3. Individual PHX Control: For each PHX, one PLC controls both the pump on the primary side of the PHX and on the secondary side of the PHX
4. Individual Pump Control: Each pump is controlled by an individual PLC

For each design, ARCADE was used to simulate cyber-attacks to stop the pumps controlled by the corresponding PLC. The cyber-physical consequences of these simulations are summarized in Figure 1. The cyber consequence was the number of PLCs compromised, and the physical consequence was the peak average fuel temperature caused by the attack.

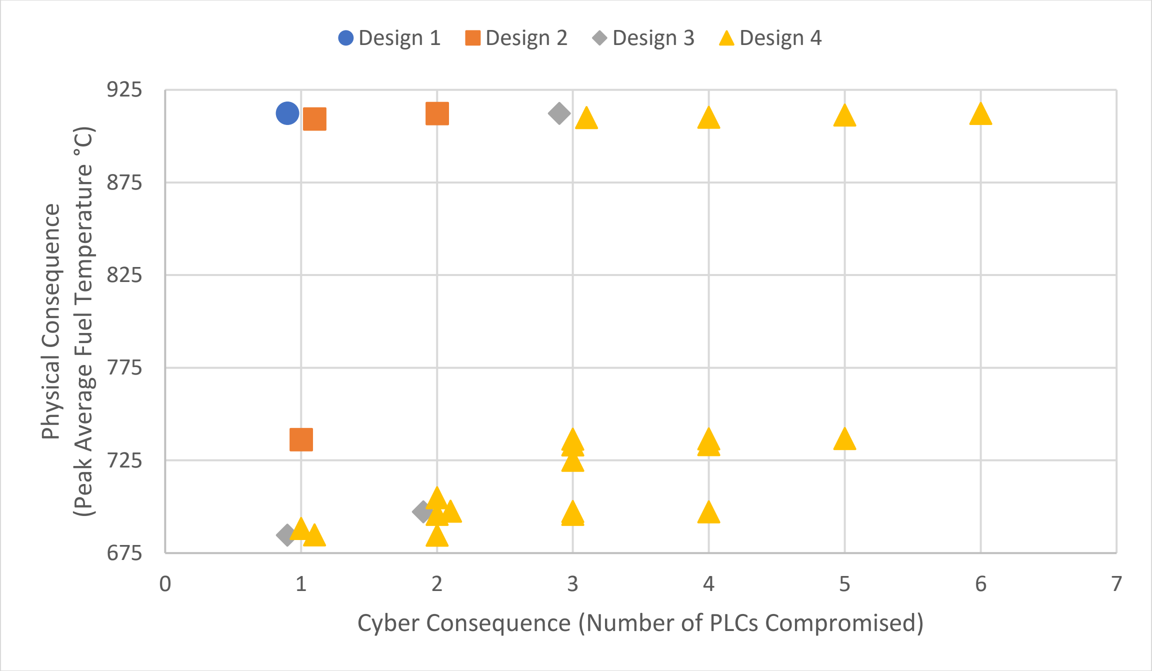

Figure 1. Cyber-Physical Consequence Analysis of Cyber-Attacks on Design Candidates

To use the data in Figure 1, the designer must specify two performance criteria. The first specification is a constraint on the peak average fuel temperature. This constraint is specified by safety analyses. The second specification is the maximum credible number of PLCs compromised by the adversary. This constraint is informed by the DCSA that denies adversary access to systems and their corresponding functions. For the sake of demonstration, we assume that the maximum peak average fuel temperature is 775 °C and the maximum credible number of PLCs compromised is two. Based on these criteria, Design 1 and Design 2 are unacceptable. Following the CIE principle of Design Simplification, Design 3 is preferred over Design 4 because it requires fewer PLCs.

If different design constraints were imposed and all four design candidates exceeded the safety specifications for credible cyber-attack scenarios, the AR designer would have two options. The first option is a SeBD approach to improve the fuel design to raise the maximum allowable peak average fuel temperature. The second option is an active defense approach to implement active cybersecurity plan features to prevent the adversary from conducting the attacks.

ACRONYMS AND TERMS

Acronym/Term	Definition
AR	Advanced Reactor
ARCADE	Advanced Reactor Cyber Analysis and Development Environment
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
CSP	Cybersecurity Plan
DCS	Distributed Control System
DCSA	Defensive Cybersecurity Architecture
DiD	Defense in Depth
DOE-NE	Department of Energy Office of Nuclear Energy
DRACS	Direct Reactor Auxiliary Cooling System
FPGA	Field-Programmable Gate Array
HiL	Hardware-in-the-Loop
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
ICS	Industrial Control System
I/O	Input/Output
LWR	Light Water Reactor
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSS	Nuclear Security Series
PHX	Primary Heat Exchanger
PI	Proportional-Integral
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Analysis
R&D	Research and Development
SeBD	Security-by-Design
SHX	Secondary Heat Exchanger
SLDA	System-Level Design Analysis
SmAHTR	Small Modular Advanced High-Temperature Reactor
SMR	Small Modular Reactor
SSCs	Systems, Structures, and Components
STPA	Systems-Theoretic Process Analysis
TCA	Tiered Cybersecurity Analysis
TRISO	Tri-structural Isotropic

Acronym/Term	Definition
VM	Virtual Machine
WNA	World Nuclear Association

1. INTRODUCTION

Advanced Reactor (AR) designers need analytical methods and tools to evaluate cybersecurity risks and develop mitigation strategies for their digital control systems. The purpose of this report is to enable effective cybersecurity analysis in the system-level design phase by identifying and demonstrating cybersecurity analysis methodologies applicable to system-level design. The system-level design phase is characterized by refining the requirements and design parameters of key systems, structures, and components (SSCs) and defining plant systems not defined in earlier phases of plant design. Key outputs of the system-level design phase include piping and instrumentation diagrams and a refined instrumentation and control (I&C) architecture and systems. The resulting System-Level Design Analysis (SLDA) for cybersecurity is focused on the design of control architectures that are informed by cybersecurity analyses.

In this report, the Tiered Cybersecurity Analysis (TCA) was examined for its applicability for SLDA. The TCA was developed in the regulatory guide for the draft Title 10 of Code of Federal Regulations (10 CFR) 73.110 [1, 2]. The TCA 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. For example, the TCA is one framework that can be used to implement Cyber-Informed Engineering (CIE) principles.

One tool that enables SLDA 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 [3, 4, 5]. ARCADE is a suite of publicly available tools that can be used to develop emulations of industrial control system (ICS) 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 nuclear power plant (NPP) systems.

This report documents the alignment of the TCA with the AR design process to enable effective cybersecurity analysis. Key connections between SLDA and CIE principles are highlighted. Finally, SLDA is demonstrated using a case study of a Small Modular Advanced High-Temperature Reactor (SmAHTR). ARCADE was used to analyze the cyber-physical consequences of cyber-attacks on the design candidates, and a design was selected based on postulated design criteria.

This page left blank

2. THE TIERED CYBERSECURITY ANALYSIS AND THE ADVANCED REACTOR DESIGN PROCESS

This section provides an overview of the performance-based draft cybersecurity analysis method for ARs and its alignment with the AR design process. Integration of cybersecurity analysis with the design process is critical to minimize cybersecurity costs and maximize cybersecurity posture. This is particularly true for ARs due to the prevalence of passive safety features that may mitigate or eliminate the effects of a cyber-attack. By integrating cybersecurity analysis with the design process, AR designers can "design-out" many cybersecurity concerns with Security-by-Design (SeBD) features.

2.1. The Tiered Cybersecurity Analysis (TCA)

Under the United States Nuclear Regulatory Commission (US NRC) Regulatory Guide 5.71 [6], 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 [7].

The US NRC presented its regulatory efforts to address the requirements outlined in 10 CFR 73.110 at 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 SeBD requirements to develop defensive network architectures and apply effective cybersecurity controls [7].

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 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 Access Prevention Analysis and focuses on developing passive Defensive Cyber Security Architecture (DCSA) features and passive cybersecurity plan (CSP) controls 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. The outcome of Tier 3 analysis is the selection of active CSP controls. Further descriptions of each tier are provided below.

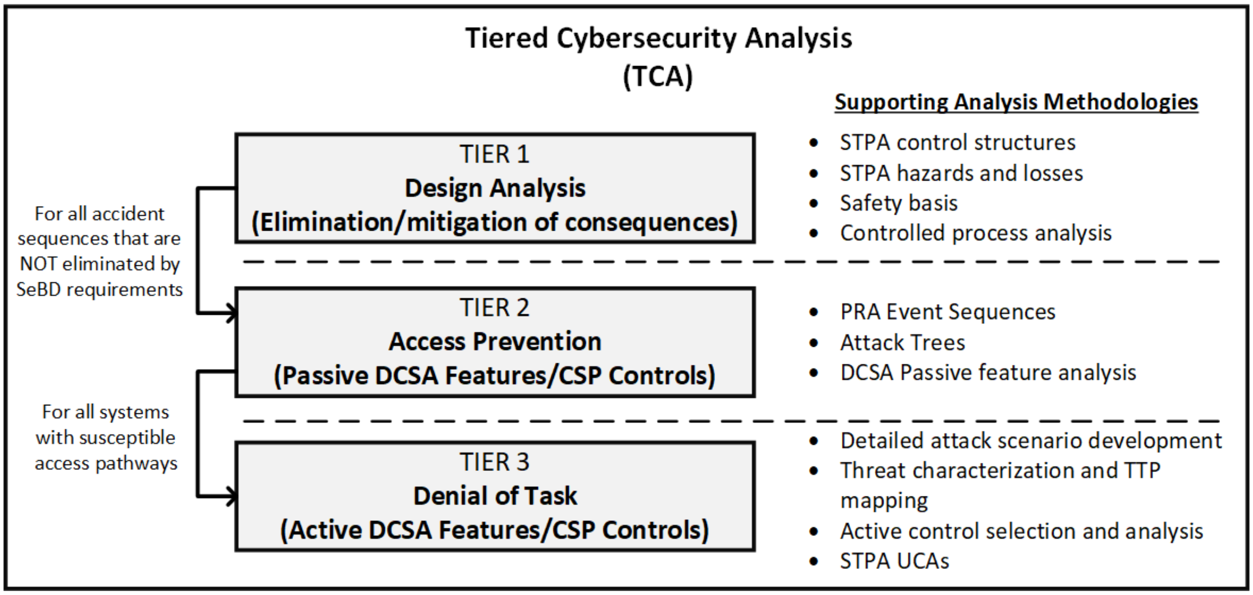
Tiered Cybersecurity Analysis
(TCA)
Supporting Analysis Methodologies
For all accident sequences that are NOT eliminated by SeBD requirements
TIER 1
Design Analysis
(Elimination/mitigation of consequences)
STPA control structures
STPA hazards and losses
Safety basis
Controlled process analysis
TIER 2
Access Prevention
(Passive DCSA Features/CSP Controls)
PRA Event Sequences
Attack Trees
DCSA Passive feature analysis
For all systems with susceptible access pathways
TIER 3
Denial of Task
(Active DCSA Features/CSP Controls)
Detailed attack scenario development
Threat characterization and TTP mapping
Active control selection and analysis
STPA UCAs

Figure 2: Tiered Cybersecurity Analysis (TCA) [8]

2.1.1. Tier 1 Analysis

The goal of Design and Impact Analysis is to evaluate the plant's safety design features and determine if they can be credited as SeBD features. Crediting the design features means that they would prevent an attack from leading to an unacceptable consequence, and therefore a more detailed analysis of the scenario is not required. To make this claim, the impact of an attack would need to be eliminated. Protective measures that would delay an attack are valuable to the security of the plant, but still require Tier 2 analysis of the function because the impact is not eliminated. Abstraction at the three tiers is best thought of as adversary capabilities. At Tier 1, the scenarios are developed considering an adversary that is limited only by the physical limitations of the plant design. This adversary is assumed to have access to any digital system, component, or network in the plant, and is assumed to be capable of implementing any control action within the capability of the system. Supporting methodologies include Systems-Theoretic Process Analysis (STPA), analysis of the plant safety basis, and controlled process analysis [9].

2.1.2. Tier 2 Analysis

The goal of Access Prevention Analysis is to evaluate adversary access vectors and implement passive measures to deny system and network access. At this tier of analysis, it is assumed that the adversary can achieve their objective if they gain access to the appropriate systems. Once again, safety analyses are taken as inputs and used to identify unsafe event sequences. One method to represent attack sequences and bound the scope of scenarios is to use traditional probabilistic risk assessment (PRA) event trees. Each plant function that must operate to mitigate an accident should be considered. This analysis should examine each system in the sequence of plant functions required for accident mitigation and identify available pathways for an adversary. The results of Tier 2 analysis are passive or deterministic DCSA or CSP elements.

The IAEA defines the features of DCSA in the Nuclear Security Series (NSS) publication 17-T [10]. Several key definitions are quoted below from NSS 17-T.

- Function: “a coordinated set of actions and processes that need to be performed at a nuclear facility”
- Security Level: “a designation that indicates the degree of security protection required for a facility function and consequently for the system that performs that function”
- Security Zone: “a logical and/or physical grouping of digital assets that are assigned to the same computer security level and that share common computer security requirements owing to inherent properties of the systems or their connections to other systems”

A zone is a region bounded by logical and physical protections which contains at least one system. Communication between assets within a zone is trusted, while communication between different zones is restricted and controlled [10]. DCSA levels provide a framework for implementing a graded approach where security measures correspond to the criticality of each level. Each plant function is assigned a level based on its criticality. The stringency of measures put in place for a given level is directly related to the significance of the function protected by the level. Levels allow flexibility in security requirements across the facility which allows designers to prioritize the areas of greatest risk. Each level includes one or more zones. Zones enable defense in depth (DiD) if systems performing redundant functions are placed in separate zones. By placing systems performing redundant functions in separate zone, the adversary is forced to compromise multiple zones in order to prevent the function from being performed. Figure 3 provides an example of how DCSA zones and levels would be implemented.

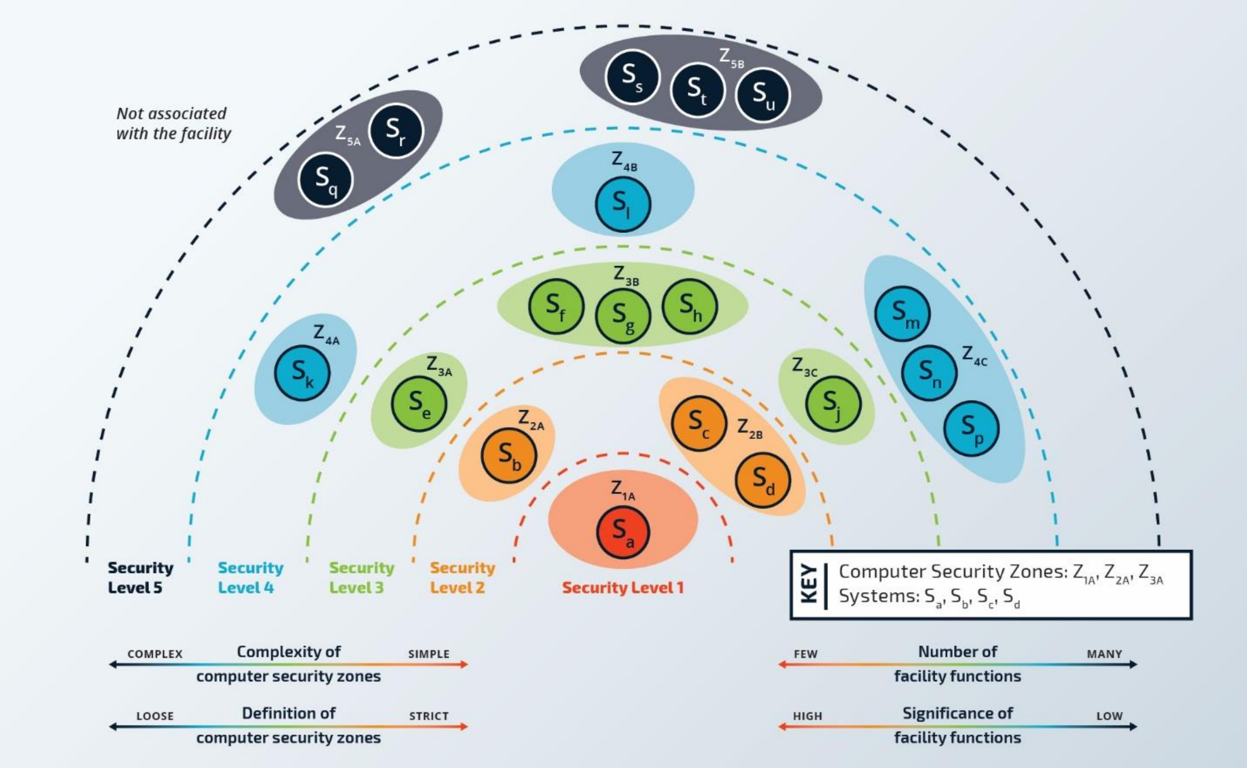

Figure 3. Conceptual DCSA Model [10]

2.1.3. Tier 3 Analysis

The goal of Denial of Task Analysis is to provide risk-informed control measures to unmitigated systems identified in Tier 2. In Tier 3, it is assumed that the adversary has obtained the access required to achieve their objective and control measures must be implemented to prevent the adversary from completing their objective. Generally, a body of controls may consist of baseline controls and risk-informed controls. Baseline controls apply broadly and provide information security assurance while risk-informed controls treat a specific identified risk. There are several methods that can be leveraged to identify applicable risk-informed controls (e.g., combining control action modeling using STPA and adversary sequence modeling using attack tree modeling).

2.2. Phases of Advanced Reactor 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) [11]. The design maturity phases are shown in Figure 4. 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. Key outputs of Phase 2 include process flow diagrams and a preliminary instrumentation and control (I&C) architecture. 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. Key outputs of Phase 3 include piping and instrumentation diagrams, I&C systems design, and a refined I&C architecture. 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 [11].

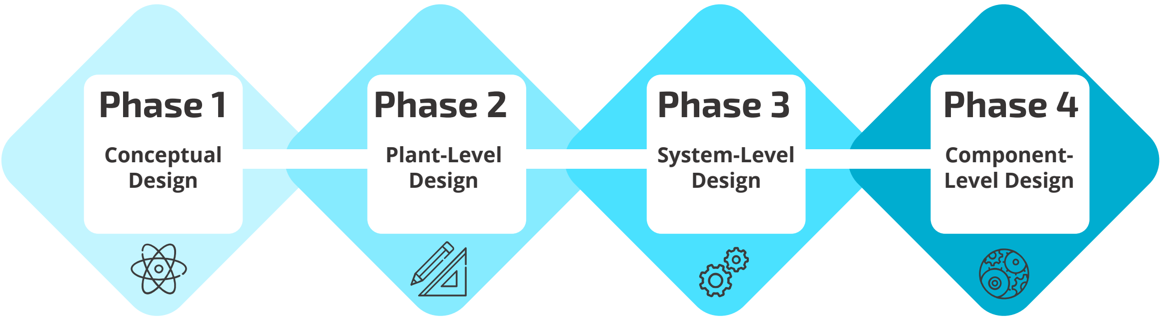

Figure 4: Plant Design Phases of Maturity [11]

2.3. Alignment of the TCA and WNA Design Phases

The TCA can be aligned with the WNA phases of design maturity to enhance the efficiency of cybersecurity analysis throughout the design process. The alignment of the TCA and WNA design phases is summarized in Table I.

Table I. WNA Design Phases and TCA Tiers [7]

WNA Design Phase	TCA Tier
Conceptual Design & Plant-Level Design	Tier 1 (Design Analysis)
System-Level Design	Tier 2 (Access Prevention)
Component-Level Design	Tier 3 (Denial of Task)

The concept and plant-level design phases align with Tier 1 of the TCA. Upon completion of these design phases, the impact of SeBD features can be analyzed. The system-level design phase aligns with Tier 2 of the TCA. This alignment occurs because the system-level design phase results in the design of I&C functional requirements and architectures and a DCSA is the primary output of Tier 2 analysis. The component-level design phase aligns with Tier 3 of the TCA. This alignment occurs because the component-level design phase provides the level of detail required to create the attack scenarios required for Tier 3 analysis. Improper alignment of the TCA with the WNA design phases may result in less efficient cybersecurity analysis and increased cybersecurity costs [7].

This page left blank

3. SYSTEM-LEVEL DESIGN ANALYSIS AND CYBER-INFORMED ENGINEERING

Cyber-Informed Engineering (CIE) is an engineering approach that integrates cybersecurity considerations into the lifecycle of a cyber-physical system [12]. The U.S. Department of Energy and the Securing Energy Infrastructure Executive Task Force developed a strategy for enabling the energy sector to utilize CIE for critical infrastructure that leverage digital monitoring or control [13] and this approach was recommended in the 2023 National Cybersecurity Strategy [14]. The most current iteration of CIE consists of 12 design principles that enhance the integration of cybersecurity analysis with the lifecycle of a cyber-physical system. The TCA is one method for applying the CIE principles for the cybersecurity of ARs as part of a performance-based approach. The remainder of this section discusses the relationship between SLDA and several of the most pertinent CIE principles.

- **Consequence-Focused Design:** This principle is most focused on how the manipulation of functions may cause unacceptable consequences. The consequence-focused design principle is most strongly connected to Tier 1 of the TCA, but is also related to SLDA because SLDA is informed by the attack consequences that were not eliminated or mitigated by SeBD features. Adequate mitigation must be defined in terms of a consequence of importance (e.g., expected dose at site boundary). As part of the TCA, DCSAs are designed to deny adversary access to the functions needed to cause an unmitigated accident sequence.
- **Secure Information Architecture:** This principle is focused on architecture design to limit the adversary's access to critical data and functions. A DCSA is one example of a secure information architecture. A DCSA separates systems into zones based on the functions that those systems perform.
- **Design Simplification:** This principle is focused on reducing complexity by eliminating unnecessary functions or components. Design simplification can reduce the attack surface available to the adversary and reduce the opportunity for adversarial manipulation of digital functions. This principle is pertinent to SLDA because it guides designers to eliminate unnecessary systems and devices within the preliminary I&C architecture.
- **Layered Defenses:** This principle is focused on implementing DiD to reduce the likelihood that a single failure impacts the performance of critical functions. This principle is pertinent to the design of a DCSA because DCSA zones provide DiD. If systems that perform redundant functions are placed in separate zones, the adversary must compromise multiple zones to prevent the performance of the function.
- **Digital Asset Awareness:** This principle is focused on understanding where digital assets are used and the functional capabilities of those assets. Implementing this principle is a requirement for the design of a DCSA. Systems are placed into zones based on the functions that they perform.
- **Planned Resilience:** This principle is focused on planning how to continue operations even if a cyber-attack degrades performance of a function. Planned resilience is pertinent to SLDA because many AR designs are purported to have passive safety features and/or redundant systems to mitigate or eliminate the effects of a cyber-attack and enable continued operation.

This page left blank

4. MODELING AND SIMULATION FOR SYSTEM-LEVEL DESIGN ANALYSIS

Cybersecurity is a persistent concern to the safety and security of NPPs but has lacked data-driven, evidence-based research. Rigorous cybersecurity analysis is critical for the licensing of ARs 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 design 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 [3, 4, 5].

ARCADE is a suite of publicly available tools that can be used to develop emulations of industrial control system (ICS) 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. 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 distributed control system (DCS) from the physics of control, down to the firmware of individual components. A functional block diagram of ARCADE is shown in Figure 5. The remainder of this section describes ARCADE and is quoted from another report written in the course of this research [5].

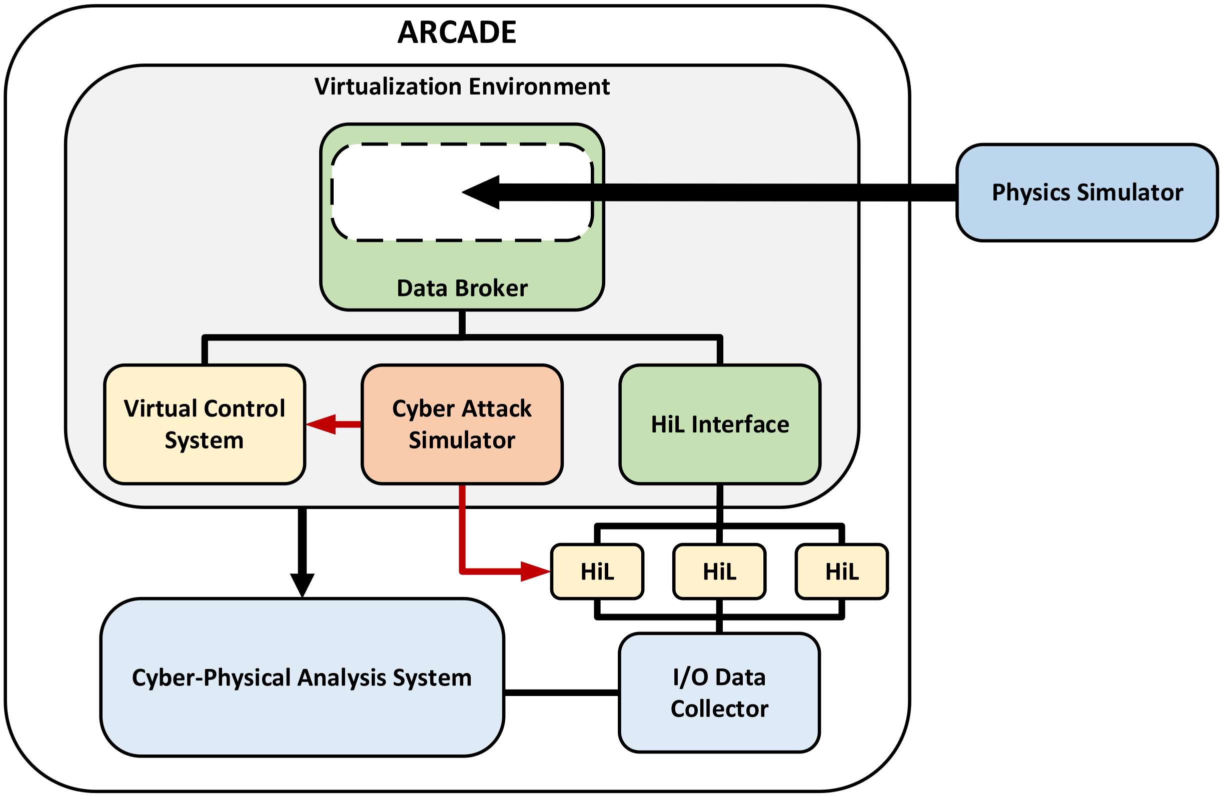

Figure 5: Advanced Reactor Cyber Analysis and Development Environment (ARCADE) Functional Block Diagram [4]

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 [15]. 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 [16]. 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 [17]. 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 [18]. The Data Broker, ManiPIO, and many elements of the virtual control system were first developed using Asherah as the physics simulator [16, 17]. 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. SYSTEM-LEVEL DESIGN ANALYSIS CASE STUDY

A model of a small modular advanced high-temperature reactor (SmAHTR) was used to demonstrate SLDA methods. This model is the same as that used to demonstrate ARCADE's capabilities in [5]. In this case study, the design of the control architecture for the primary heat exchangers (PHXs) of a SmAHTR unit was investigated. Four designs were developed, and cybersecurity experiments were conducted using ARCADE.

5.1. 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 [19]. SmAHTR uses tri-structural isotropic (TRISO) particle fuel and graphite as a moderator. The following SmAHTR description and model development is based upon a pre-conceptual design report [19], and is quoted from a conference paper written during this research [3].

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.

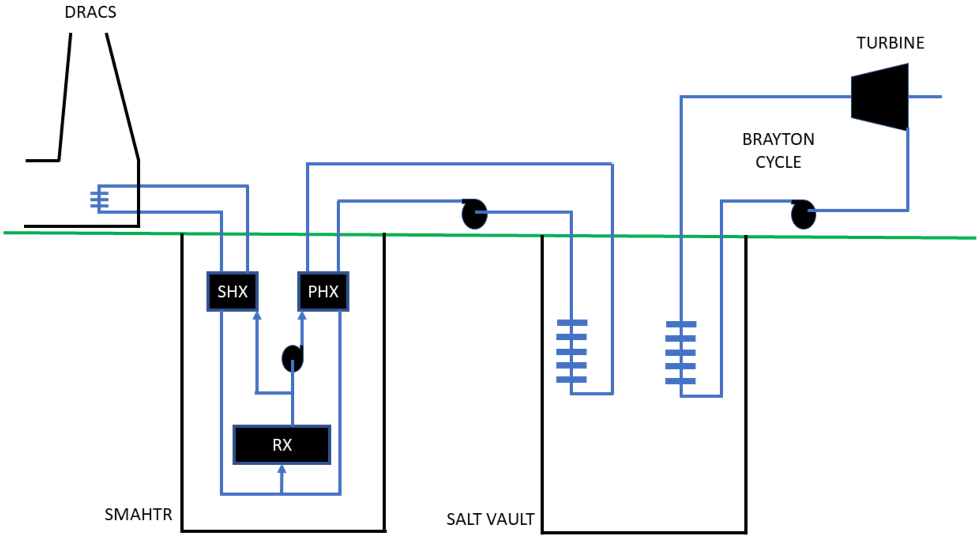

Figure 6: SmAHTR Simulink model includes the reactors, salt vault, and Brayton cycle.

A SmAHTR model has been developed and used in research at the University of Pittsburgh [20, 21]. 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 6. 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.

All of the PHXs and corresponding pumps for one SmAHTR unit are shown in Figure 7. As previously stated, each reactor has three PHXs. Each PHX has one pump on the primary side (reactor side) and one pump on the secondary side (salt vault side). The purpose of this case study is to determine the control architecture for the pumps associated with these PHXs. Four candidate designs using various configurations of programmable logic controllers (PLCs) will be considered:

1. One PLC: One PLC controls all six pumps associated with the PHXs
2. Primary and Secondary Side Control: One PLC controls all three pumps on the primary side of the PHXs and one PLC controls all three pumps on the secondary side of the PHXs
3. Individual PHX Control: For each PHX, one PLC controls both the pump on the primary side of the PHX and on the secondary side of the PHX
4. Individual Pump Control: Each pump is controlled by a separate PLC

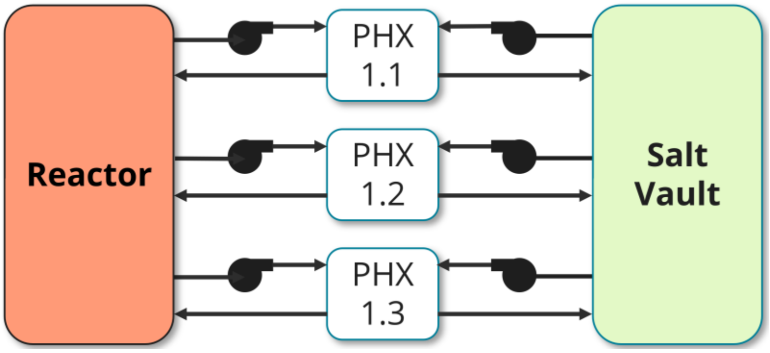

Figure 7. PHXs and Pumps for One SmAHTR Unit

5.2. Candidate Design 1: One PLC

In candidate design 1, one PLC is used to control all six pumps associated with the three PHXs. This design is shown in Figure 8.

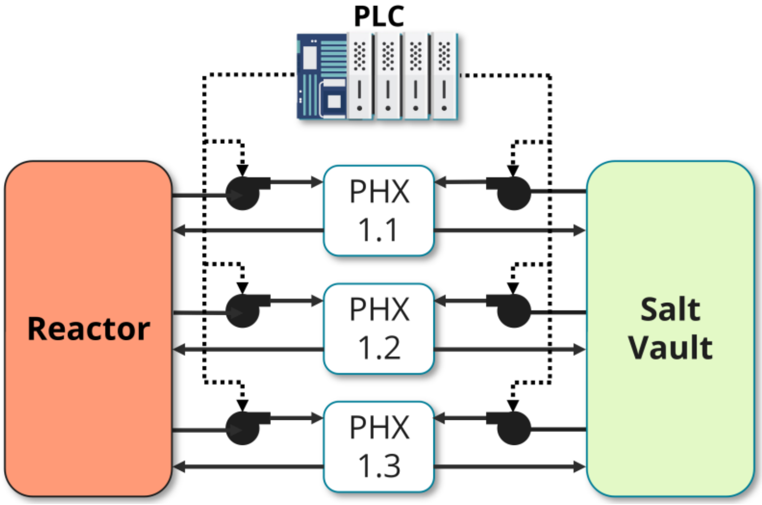

Figure 8. Candidate Design 1: One PLC

One cyber-attack scenario was simulated for this candidate design because there is only one PLC. In this scenario, the adversary compromises the PLC and stops all of the pumps. The average fuel temperature over the course of the attack is plotted in Figure 9. This scenario bounds the maximum average fuel temperature for all further analyses.

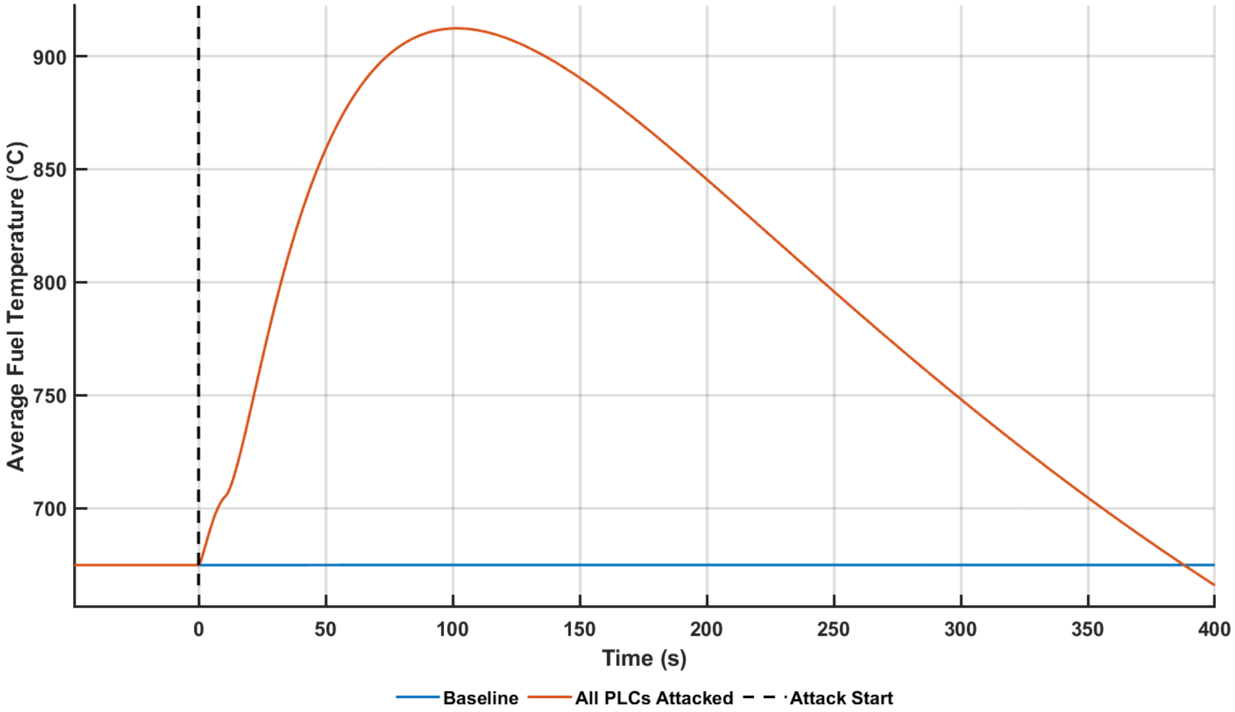

Figure 9. ARCADE Simulation of Cyber-Attack on Candidate Design 1

5.3. Candidate Design 2: Primary and Secondary Side Control

In candidate design 2, one PLC is used to control the three pumps on the primary side of the PHXs, and another PLC is used to control the three pumps on the secondary side of the PHXs. This design is shown in Figure 10.

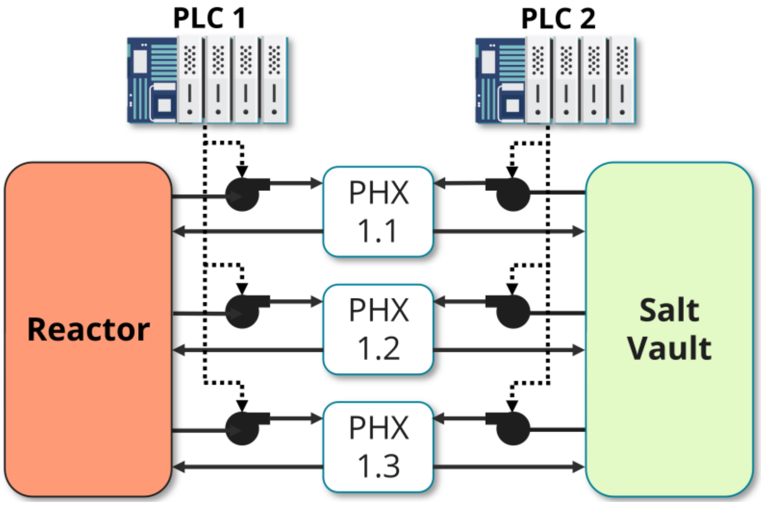

Figure 10. Candidate Design 2: Primary and Secondary Side Control

Three cyber-attack scenarios were simulated for this candidate design. In these scenarios, the adversary stops the individual PLCs and both PLCs. The average fuel temperatures over the course of the attacks are plotted in Figure 11. As shown in Figure 11, the attack targeting the pumps on the primary side had a much greater effect on the average fuel temperature than the attack targeting the pumps on the secondary side. The attack where both PLCs are compromised is identical to the attack conducted for the first design candidate. The attack targeting the pumps on the primary side is nearly equivalent to the attack targeting all of the pumps.

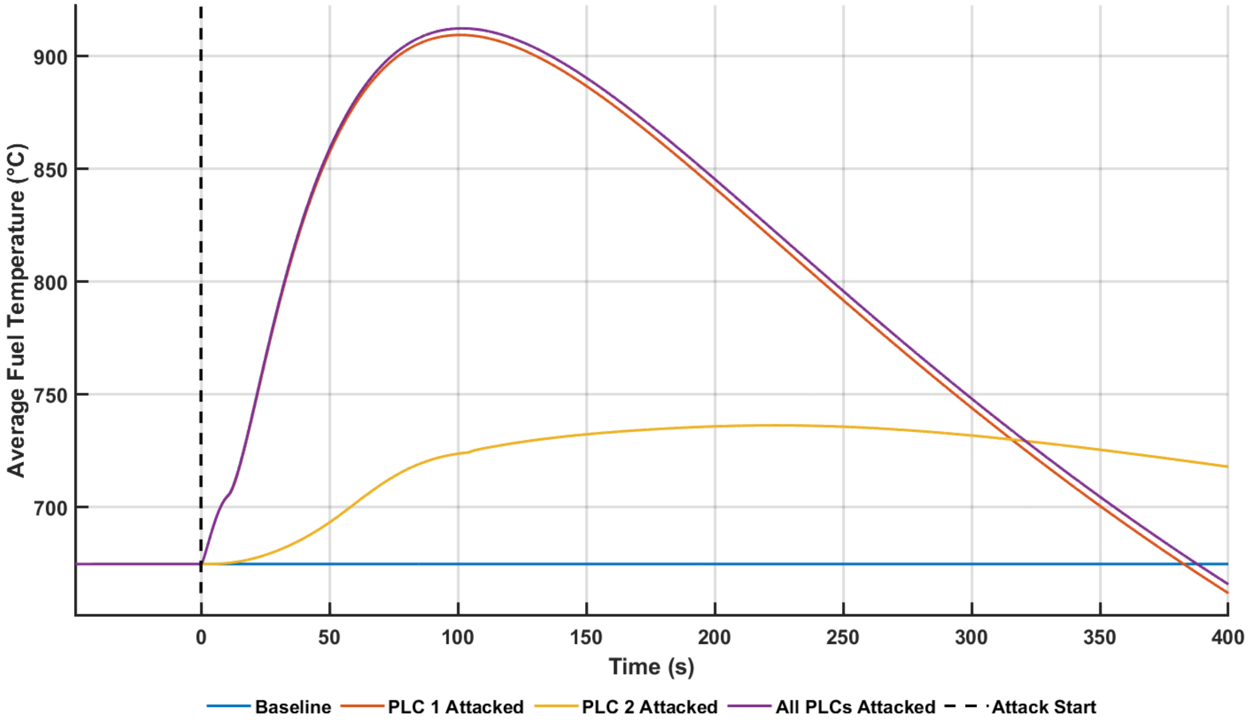

Figure 11. ARCADE Simulation of Cyber-Attacks on Candidate Design 2

5.4. Candidate Design 3: Individual PHX Control

In candidate design 3, for each PHX, one PLC is used to control both the pump on the primary side of the PHX and the pump on the secondary side of the PHX. This design is shown in Figure 12.

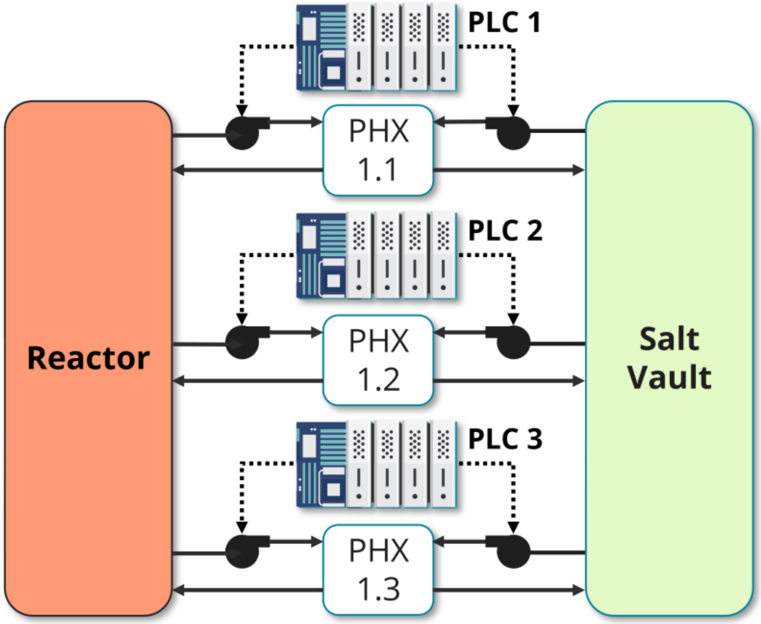

Figure 12. Candidate Design 3: Individual PHX Control

Three cyber-attack scenarios were simulated for this candidate design. In these scenarios, the adversary stops one PLC, two PLCs, and all of the PLCs. Note that the PHXs are identical, therefore only one simulation is required for the scenario where two PLCs are compromised. The average fuel temperatures over the course of the attacks are plotted in Figure 13. As shown in Figure 13, the attacks targeting a subset of the PHXs have a relatively small effect on the average fuel temperature compared to the attack targeting all of the PHXs. The attack where all of PLCs are compromised is identical to the attack conducted for the first design candidate.

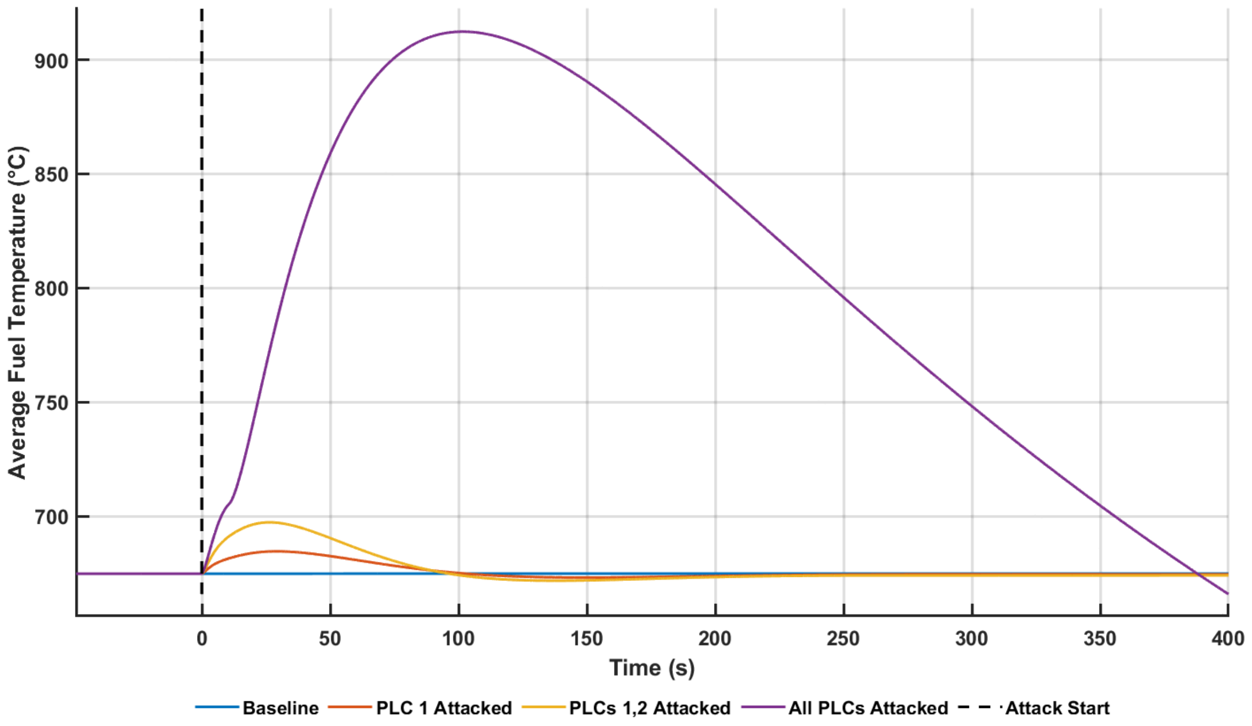

Figure 13. ARCADE Simulation of Cyber-Attacks on Candidate Design 3

5.5. Candidate Design 4: Individual Pump Control

In candidate design 4, each pump is controlled by a unique PLC. This design is shown in Figure 14.

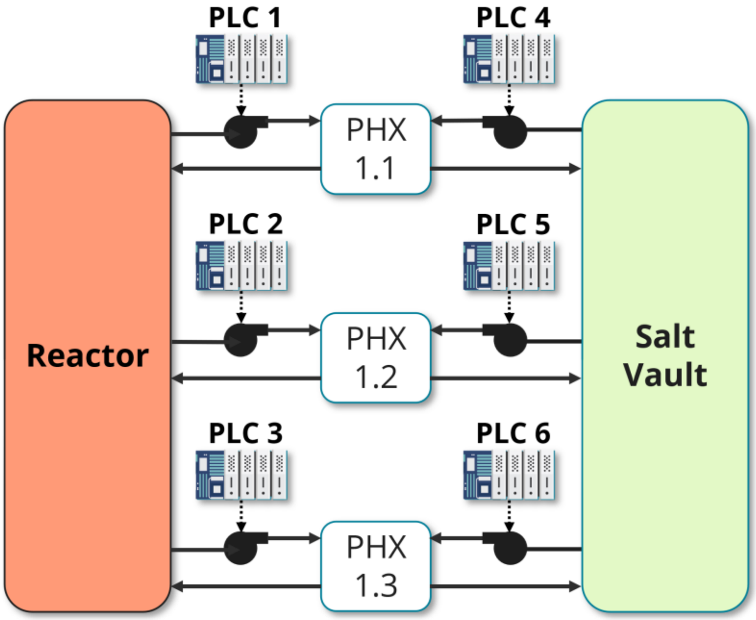

Figure 14. Candidate Design 4: Individual Pump Control

The simulation scenarios are most complex for this design because of the number of PLCs used, therefore the simulation results are divided over several graphs based on the number of PLCs that were compromised in the attack. These simulation results are provided in Appendix A.

5.6. Design Analysis

To summarize the cyber-attack simulations on the design candidates, each attack was decomposed into its cyber and physical consequences. Here, the cyber consequence is most readily interpreted as the number of PLCs compromised by the adversary in the cyber-attack scenario, and the physical consequence is the peak average fuel temperature. The cyber-physical consequences of the attacks are plotted in Figure 15. Note that the number of PLCs compromised is always an integer value, but some points are offset from the vertical gridlines for ease of viewing.

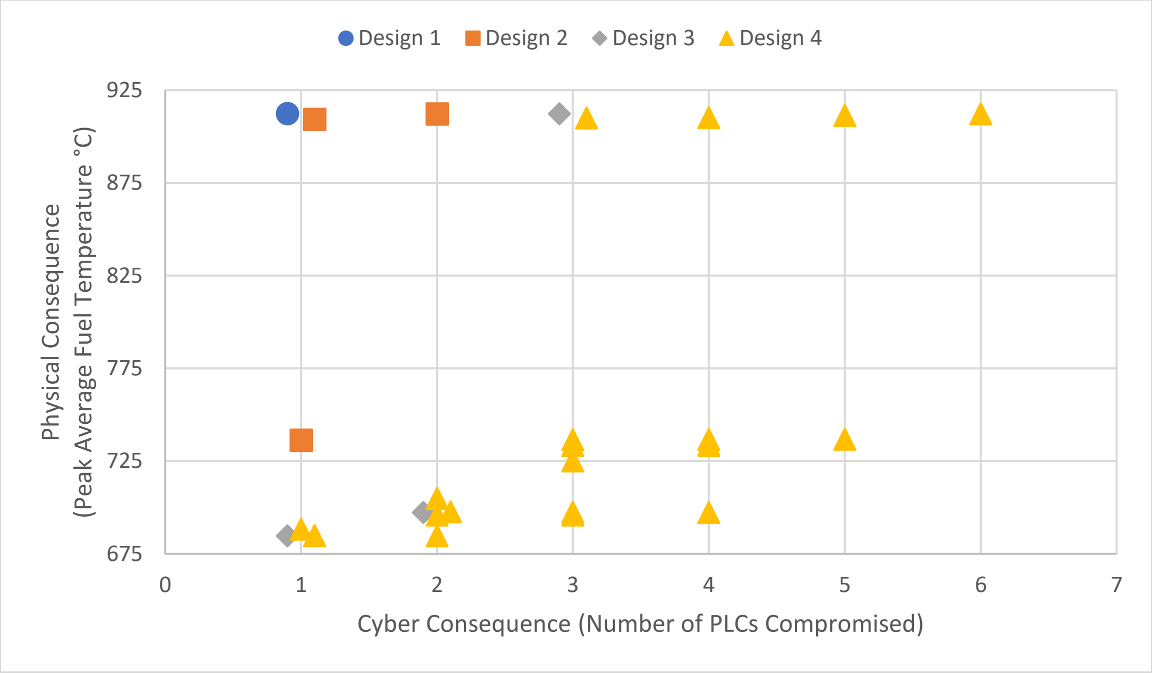

Figure 15. Cyber-Physical Consequence Analysis of Cyber-Attacks on Design Candidates

To use the data in Figure 15, the designer must specify two performance criteria. The first specification is a constraint on the physical consequence (i.e., peak average fuel temperature). This constraint is specified by safety analyses. The safe temperature limit of TRISO fuel is well above the peak temperatures observed in these simulations [22], but for the sake of demonstration, we will assume that this specification is 775 °C. The second specification is a constraint on the cyber consequence (i.e., maximum credible number of PLCs compromised by the adversary). This constraint is informed by the DCSA that denies adversary access to systems and their corresponding functions. For the sake of demonstration, we assume that this specification is two. Any design that results in a peak average fuel temperature of greater than 775 °C when two or fewer PLCs are compromised is not acceptable. Design 1 and Design 2 (one PLC, and primary and secondary side control, respectively) are therefore eliminated, leaving Design 3 and Design 4 (individual PHX control and individual pump control, respectively) as viable options. Following the CIE principle of Design Simplification, Design 3 is the preferred design because it requires fewer PLCs.

Suppose that the maximum credible number of PLCs compromised by the adversary is three instead of two, and the maximum allowable peak average fuel temperature remains 775 °C. In this case, all four design candidates exceed the safety specifications for credible cyber-attack scenarios. The AR designer has two options: (1) improve the fuel design to raise the maximum allowable peak average fuel temperature (i.e., return to Tier 1 Analysis) or (2) implement active CSP features as part of

Denial of Task Analysis (i.e., Tier 3 Analysis) to prevent the adversary from conducting the tasks needed to conduct the cyber-attacks.

6. CONCLUSION

Integration of cybersecurity analyses with the AR design process is critical to enable cost-effective cybersecurity designs. To enable this integration, SLDA techniques were identified using the TCA as a cybersecurity framework and the WNA phases of SMR design maturity as the design framework. SLDA for cybersecurity is focused on the design of control architectures that are informed by cybersecurity analyses.

One tool that enables SLDA is modeling and simulation. 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. In this report, ARCADE was implemented to analyze a set of candidate control system designs for the SmAHTR PHX pumps. The SmAHTR case study demonstrated how cyber-physical consequence analysis can be used to inform design decisions. In the case where SLDA does not identify a viable design based on the specified design criteria, the AR designer must achieve a secure posture through another tier of analysis. This can be done by designing SeBD features as part of Tier 1 analysis or by selecting active cybersecurity controls as part of Tier 3 analysis.

Although the unsafe control actions caused by the adversary in the SmAHTR case study were relatively simple, ARCADE can be used to analyze more complex unsafe control actions and combinations of unsafe control actions. Given that the control system can either be emulated in ARCADE or included as HiL, ARCADE's cyber-physical analysis capabilities are only constrained by the control surfaces that have been included in the physics model and the valid domain of the physics model.

Future efforts will examine the application of these tools and methods to develop comprehensive DCSAs for ARs. By developing a DCSA that is informed by the ARs SeBD features, AR designers can reduce the plant's dependency on active cybersecurity controls without compromising the plant's security posture.

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] 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.

[4] 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.

[5] A. S. Hahn, L. T. Maccarone and M. T. Rowland, "Advanced Reactor Cyber Analysis and Development Environment (ARCADE) for System-Level Design Analysis," Sandia National Laboratories, Albuquerque, NM, 2023.

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

[7] 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.

[8] 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.

[9] N. G. Leveson and J. P. Thomas, "STPA Handbook," 2018.

[10] International Atomic Energy Agency, "NSS 17-T: Computer Security Techniques for Nuclear Facilities," IAEA, Vienna, Austria, 2021.

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

[12] Idaho National Laboratory, "Cyber-Informed Engineering Implementation Guide," Idaho National Laboratory, Idaho Falls, ID, 2023.

[13] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, "National Cyber-Informed Engineering Strategy," DOE, Washington, DC, 2022.

[14] The White House, "National Cybersecurity Strategy," The White House, Washington, DC, 2023.

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

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

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] U.S. Department of Energy, Office of Nuclear Energy, "TRISO Particles: The Most Robust Nuclear Fuel on Earth," U.S. DOE, 9 July 2019. [Online]. Available: https://www.energy.gov/ne/articles/triso-particles-most-robust-nuclear-fuel-earth#:~:text=Simply%20put%2C%20TRISO%20particles%20cannot,threshold%20of%20current%20nuclear%20fuels.. [Accessed 16 September 2023].

APPENDIX A. ARCADE SIMULATIONS FOR CANDIDATE DESIGN 4

This appendix contains the results of the ARCADE simulations for the fourth candidate design that were too numerous to be included in the body of the report.

Two cyber-attack scenarios were simulated for the case where the adversary compromises one PLC. The average fuel temperatures over the course of the attacks are plotted in Figure 16. Note that because the PHXs are identical, simulating a cyber-attack on PLC 1 is equivalent to simulating an attack on PLC 2 or PLC 3. Similarly, simulating a cyber-attack on PLC 4 is equivalent to simulating an attack on PLC 5 or PLC 6. The attack on the secondary-side pump resulted in a greater peak average fuel temperature than the attack on the primary-side pump.

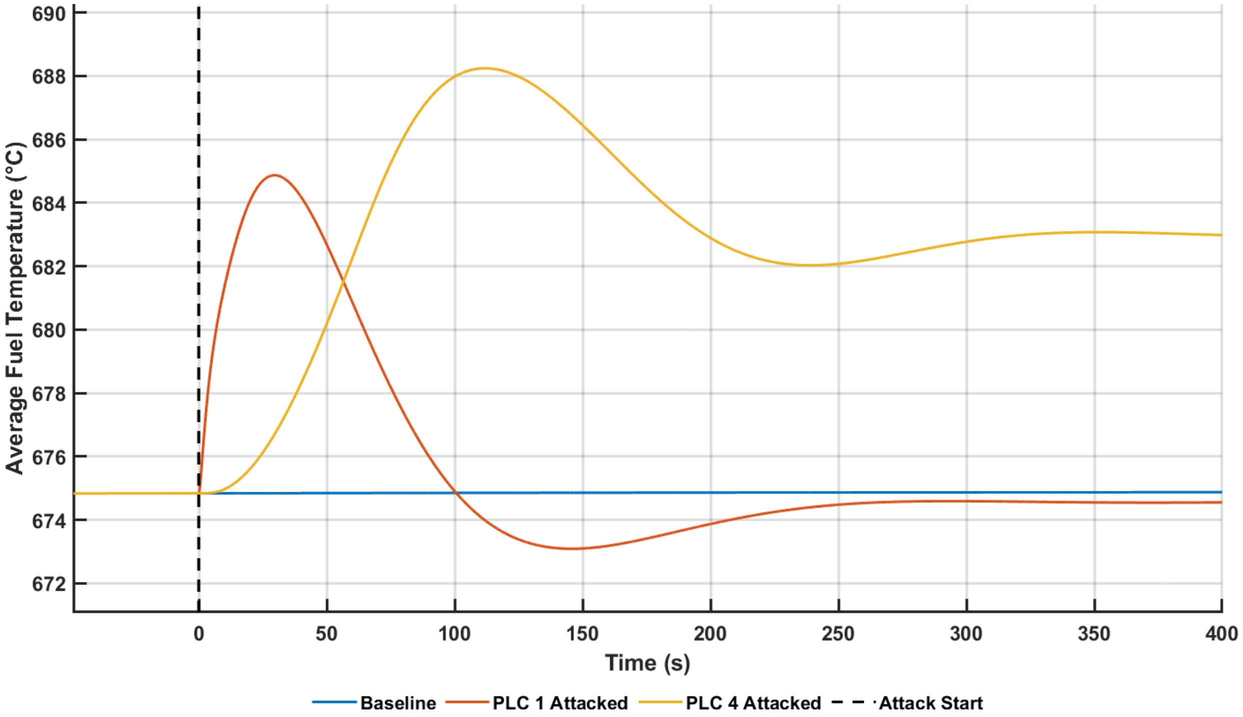

Figure 16. ARCADE Simulation of Cyber-Attacks Compromising One PLC in Candidate Design 4

Four cyber-attack scenarios were simulated for the case where the adversary compromises two PLCs. The average fuel temperatures over the course of the attacks are plotted in Figure 17 and a summary of the plots and the corresponding scenarios is provided in Table II. The greatest peak average fuel temperature occurred for the scenario where two pumps were stopped on the secondary side of the PHXs, and the smallest peak average fuel temperature occurred for the scenario where both pumps were stopped for one PHX. Note that the smallest peak average fuel temperature scenario is equivalent to the scenario where one PLC was compromised for the third design candidate.

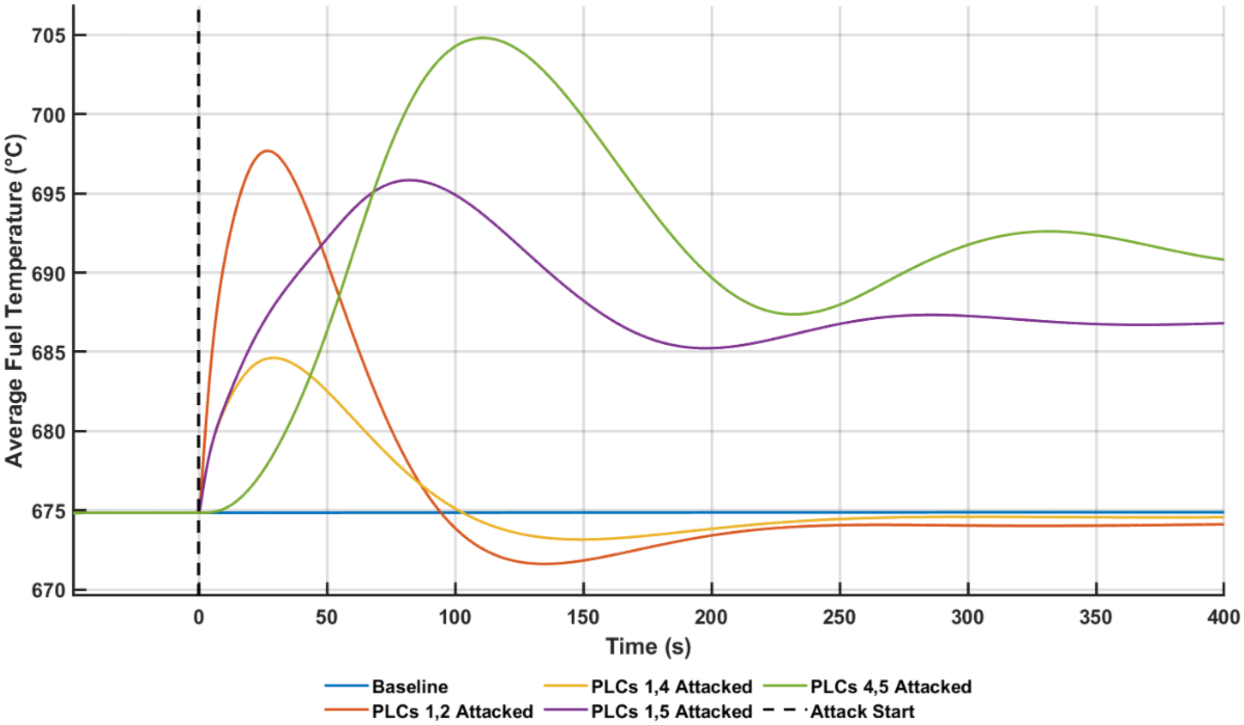

Figure 17. ARCADE Simulation of Cyber-Attacks Compromising Two PLCs in Candidate Design 4

Table II. Descriptions of Cyber-Attacks Compromising Two PLCs in Candidate Design 4

Compromised PLCs	Scenario Description
PLCs 1 & 2	Two pumps stopped on the primary side of the PHXs
PLCs 1 & 4	Both pumps stopped for one PHX
PLCs 1 & 5	One primary-side pump stopped for one PHX and one secondary-side pump stopped for another PHX
PLCs 4 & 5	Two pumps stopped on the secondary side of the PHXs

Six cyber-attack scenarios were simulated for the case where the adversary compromises three PLCs. The average fuel temperatures over the course of the attacks are plotted in Figure 18 and a summary of the plots and the corresponding scenarios is provided in Table III. The greatest peak average fuel temperature occurred for the scenario where all of the primary-side pumps were stopped, and the smallest peak average fuel temperature occurred for the scenario where both pumps were stopped for one PHX, and a secondary-side pump was stopped for another PHX.

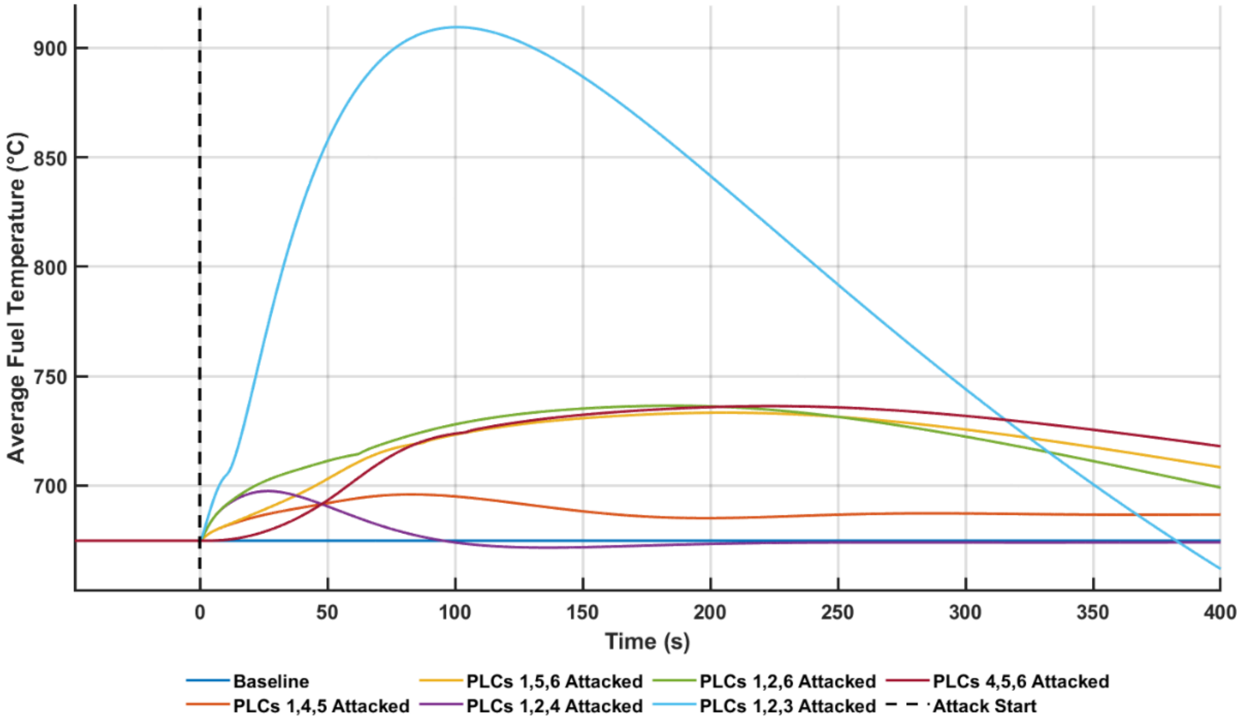

Figure 18. ARCADE Simulation of Cyber-Attacks Compromising Three PLCs in Candidate Design 4

Table III. Descriptions of Cyber-Attacks Compromising Three PLCs in Candidate Design 4

Compromised PLCs	Scenario Description
PLCs 1, 4, & 5	Both pumps stopped for one PHX, and a secondary-side pump stopped for another PHX
PLCs 1, 5, & 6	Primary-side pump stopped for one PHX, and secondary-side pumps stopped for the other PHXs
PLCs 1, 2, & 4	Both pumps stopped for one PHX, and a primary-side pump stopped for another PHX
PLCs 1, 2, & 6	Primary-side pumps stopped for two PHXs, and secondary-side stopped for the third PHX
PLCs 1, 2, & 3	All pumps on the primary side stopped
PLCs 4, 5, & 6	All pumps on the secondary side stopped

Four cyber-attack scenarios were simulated for the case where the adversary compromises four PLCs. The average fuel temperatures over the course of the attacks are plotted in Figure 19 and a summary of the plots and the corresponding scenarios is provided in Table IV. The greatest peak average fuel temperature occurred for the scenario where all of the primary-side pumps were stopped and one secondary-side pump was stopped. The smallest peak average fuel temperature occurred for the scenario where both pumps were stopped for two PHXs. This scenario corresponds to the scenario where two PLCs were compromised for the third candidate design.

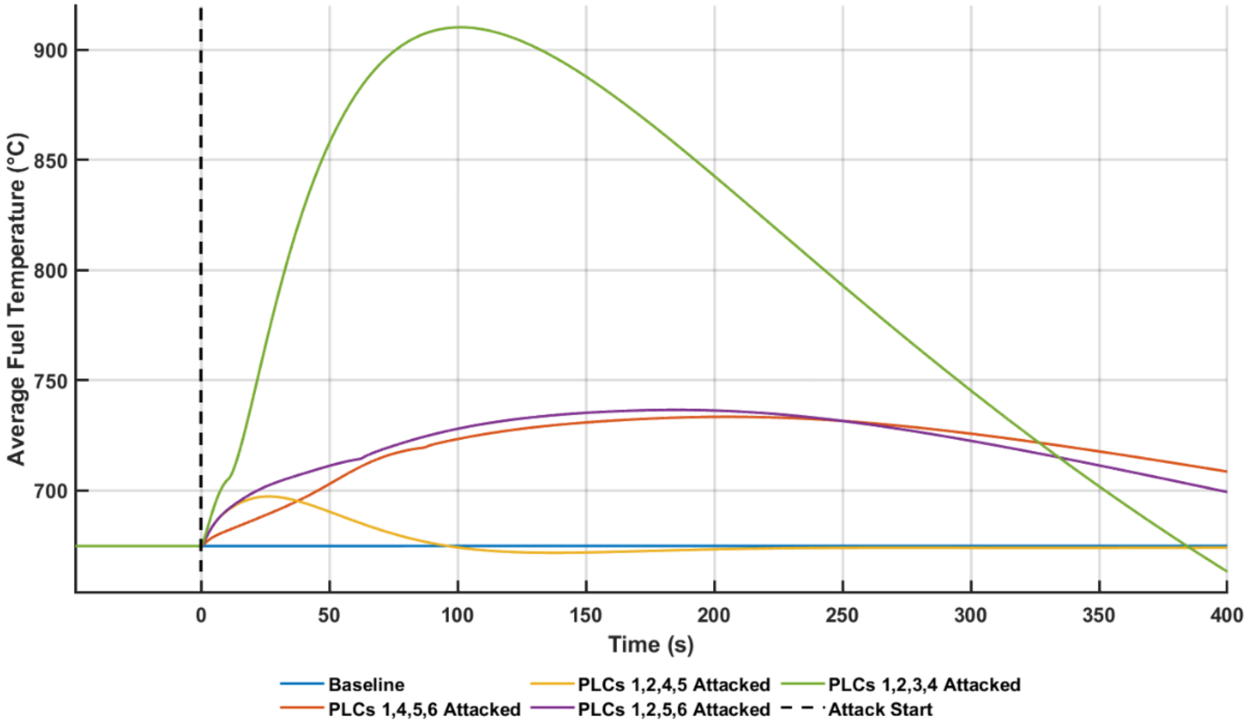

Figure 19. ARCADE Simulation of Cyber-Attacks Compromising Four PLCs in Candidate Design 4

Table IV. Descriptions of Cyber-Attacks Compromising Four PLCs in Candidate Design 4

Compromised PLCs	Scenario Description
PLCs 1, 4, 5, & 6	One primary-side pump stopped and all secondary-side pumps stopped
PLCs 1, 2, 4, & 5	Both pumps stopped for two PHXs
PLCs 1, 2, 5, & 6	Both pumps stopped for one PHX, primary-side pump stopped for one PHX, and secondary-side pump stopped for one PHX
PLCs 1, 2, 3, & 4	All primary-side pumps stopped and one secondary-side pump stopped

Two cyber-attack scenarios were simulated for the case where the adversary compromises five PLCs. The average fuel temperatures over the course of the attacks are plotted in Figure 20 and a summary of the plots and the corresponding scenarios is provided in Table V. The greatest peak average fuel temperature occurred for the scenario where all of the primary-side pumps were stopped and two of the secondary-side pumps were stopped. This scenario is nearly equivalent to the scenario where all of the pumps were stopped.

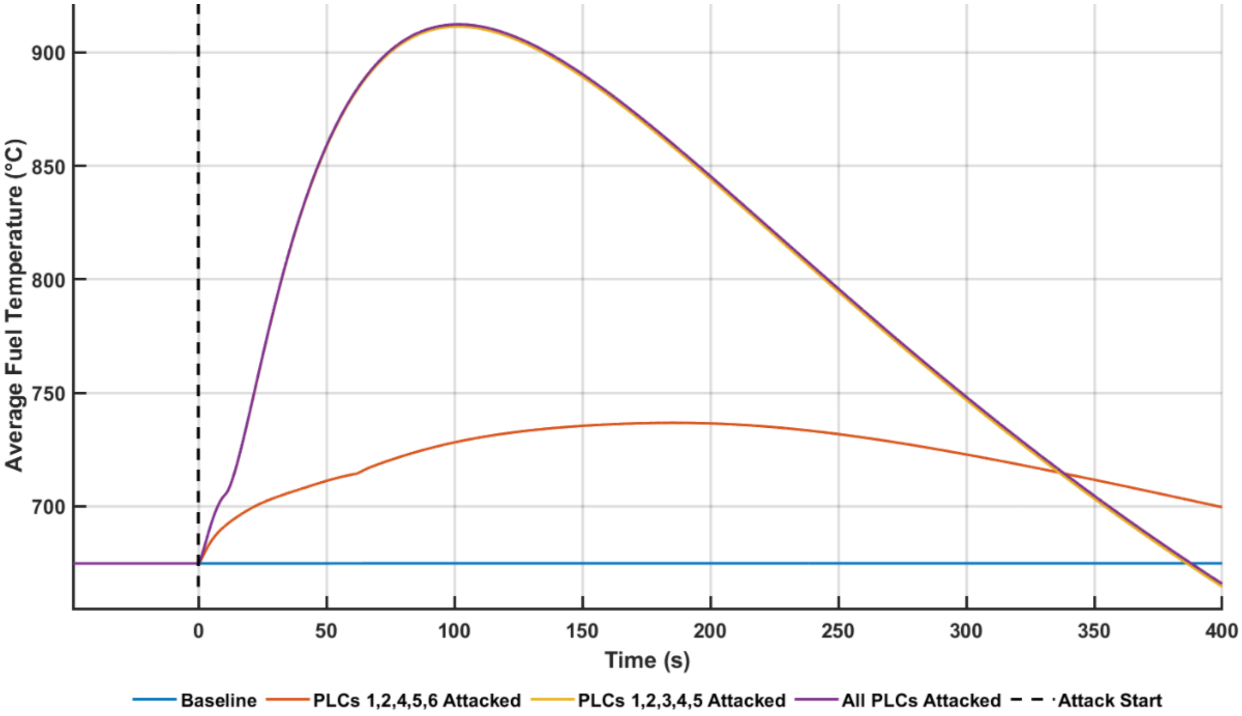

Figure 20. ARCADE Simulation of Cyber-Attacks Compromising Five to Six PLCs in Candidate Design 4

Table V. Descriptions of Cyber-Attacks Compromising Five PLCs in Candidate Design 4

Compromised PLCs	Scenario Description
PLCs 1, 2, 4, 5, & 6	Two primary-side pumps stopped and all secondary-side pumps stopped
PLCs 1, 2, 3, 4, & 5	All primary-side pumps stopped and two secondary-side pumps stopped

This page left blank

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