System-Level Design Analysis for Advanced Reactor Cybersecurity

Lee Maccarone

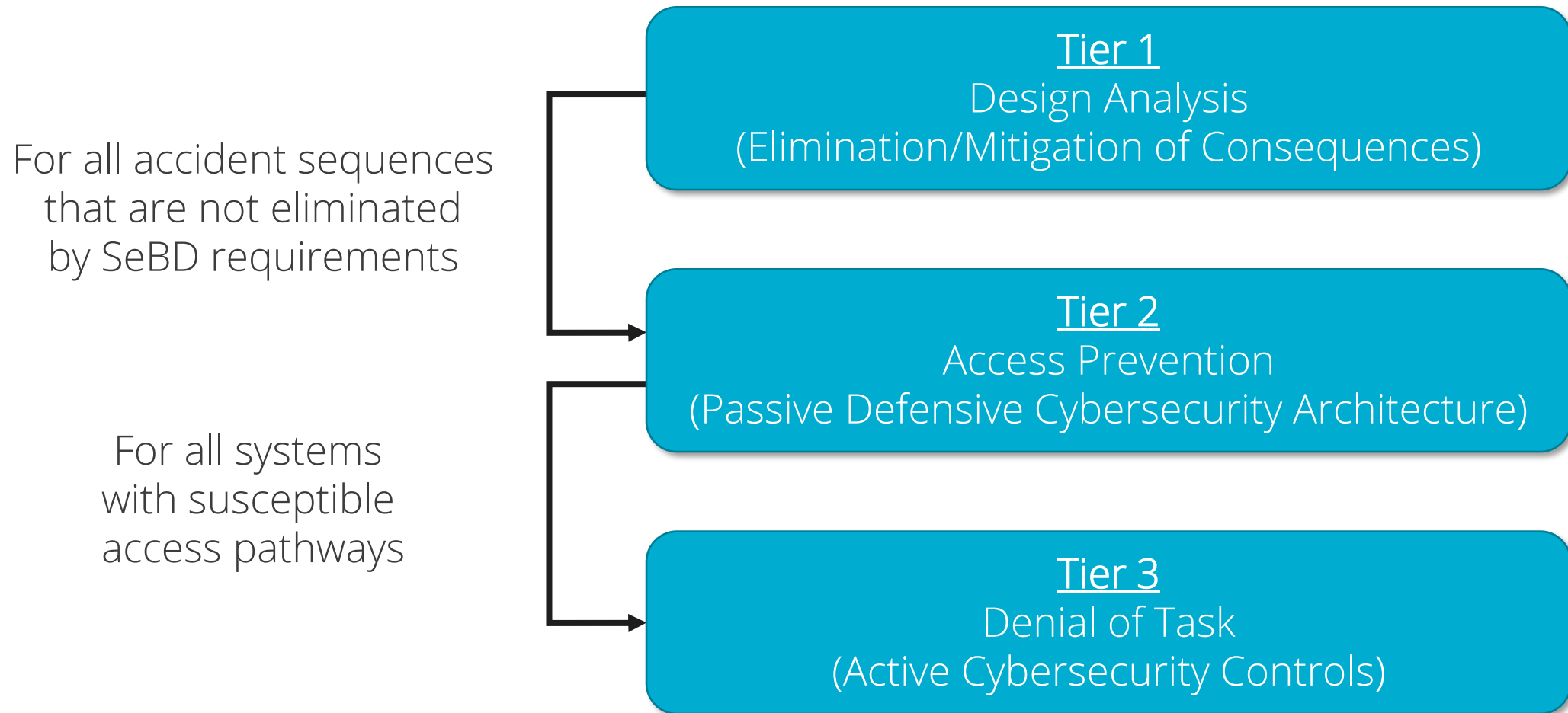## 2023 ARSS Fall Program Review

System-Level Design Analysis (SLDA) Motivation

- Active cybersecurity controls are costly to implement

- Many advanced reactors have inherent safety features that may mitigate the effects of a cyber-attack

- Evidence-based cybersecurity analysis methods are needed throughout the advanced reactor design process

- The goal of this research is to reduce cybersecurity costs by:
  - Leveraging security-by design (SeBD) features in cybersecurity analysis during the system-level design phase
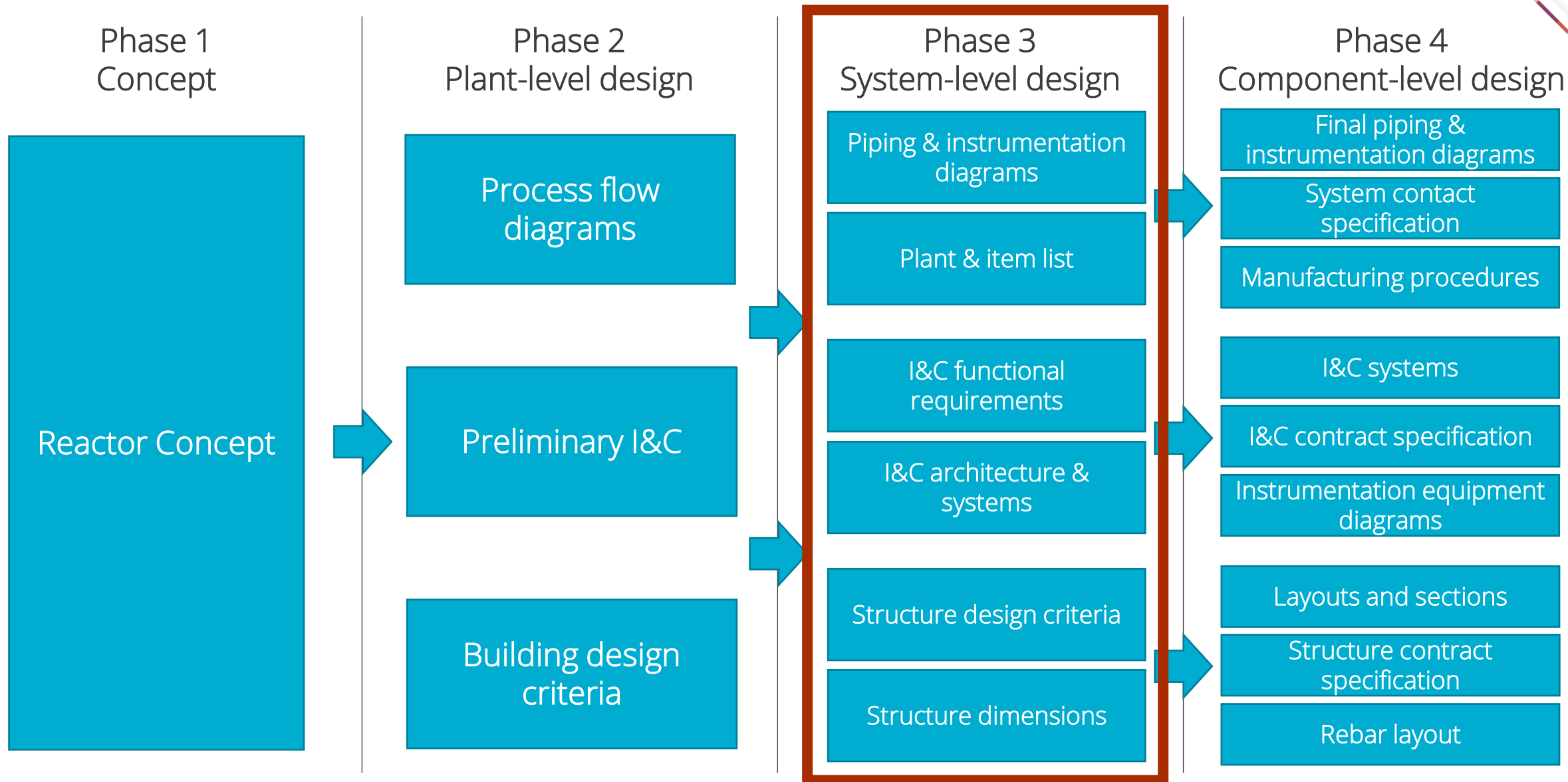 - Integrating cybersecurity analysis with the design process

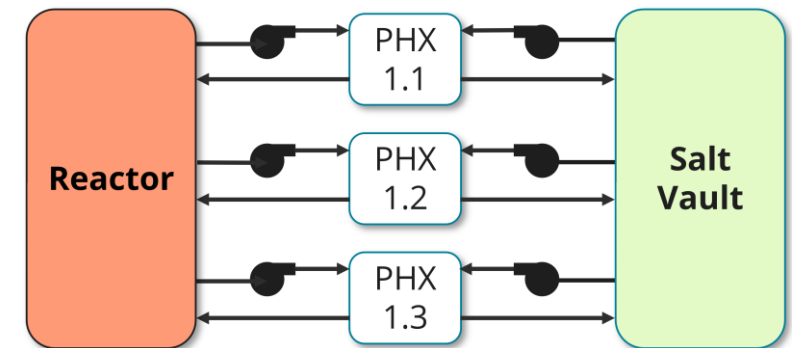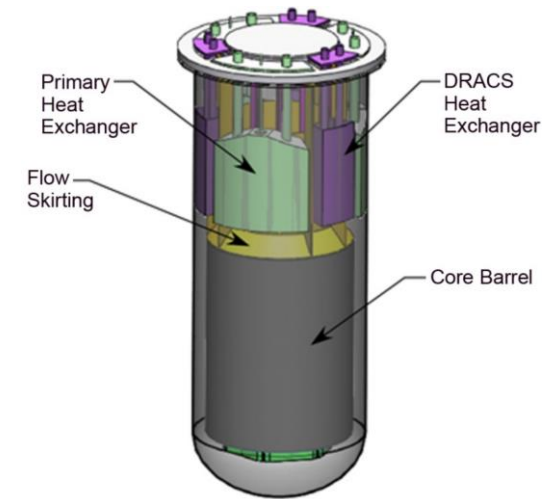# The Tiered Cybersecurity Analysis (TCA) for advanced reactors leverages security-by-design (SeBD) features

For all accident sequences that are not eliminated by SeBD requirements

Tier 1
Design Analysis
(Elimination/Mitigation of Consequences)

Tier 2
Access Prevention
(Passive Defensive Cybersecurity Architecture)

For all systems with susceptible access pathways

Tier 3
Denial of Task
(Active Cybersecurity Controls)

WNA Phases Of Design Maturity

Phase 1
Concept

Phase 2
Plant-level design

Phase 3
System-level design

Phase 4
Component-level design

Phase 1	Phase 2	Phase 3	Phase 4
Reactor Concept	Process flow diagrams	Piping & instrumentation diagrams	Final piping & instrumentation diagrams
		Plant & item list	System contact specification
			Manufacturing procedures
	Preliminary I&C	I&C functional requirements	I&C systems
		I&C architecture & systems	I&C contract specification
			Instrumentation equipment diagrams
	Building design criteria	Structure design criteria	Layouts and sections
			Structure contract specification
		Structure dimensions	Rebar layout

Citation: World Nuclear Association, "Design Maturity and Regulatory Expectations for Small Modular Reactors", 2021
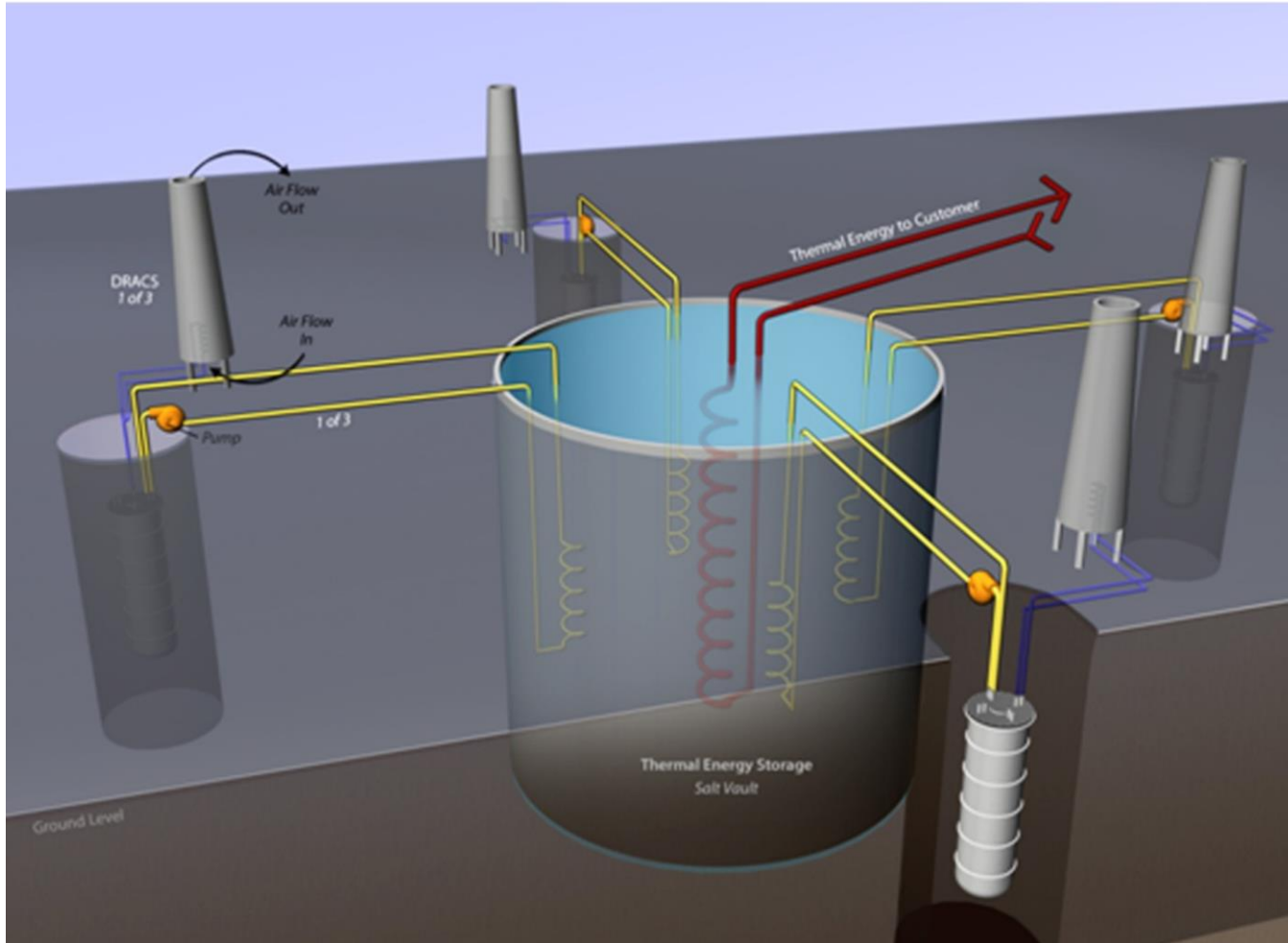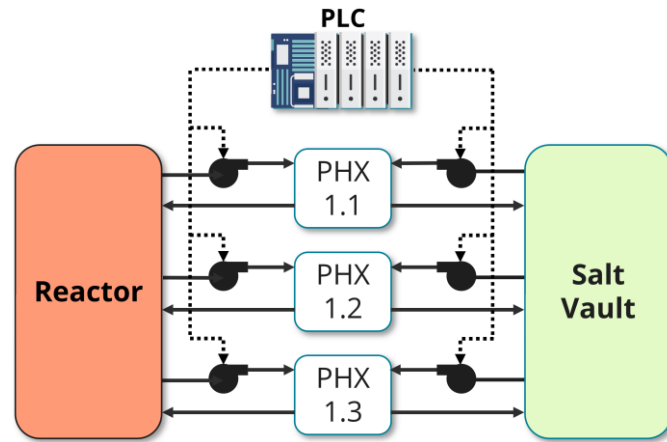
SLDA Case Study:
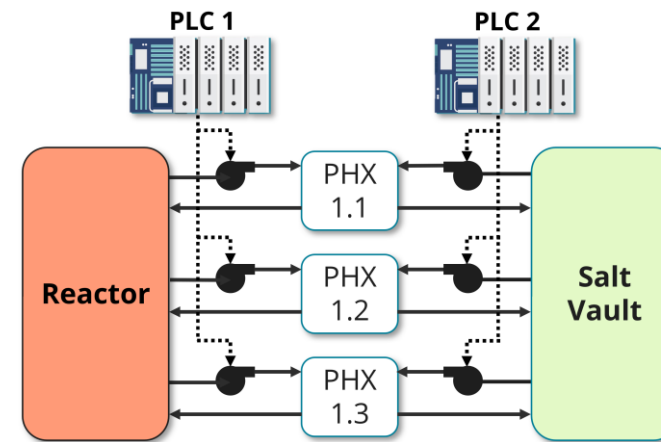# Small Modular Advanced High-Temperature Reactor (SmAHTR)

Citation: Oak Ridge National Laboratory, "Pre-Conceptual Design of a Fluoride-Salt-Cooled Small Modular Advanced High-Temperature Reactor (SmAHTR)", 2010
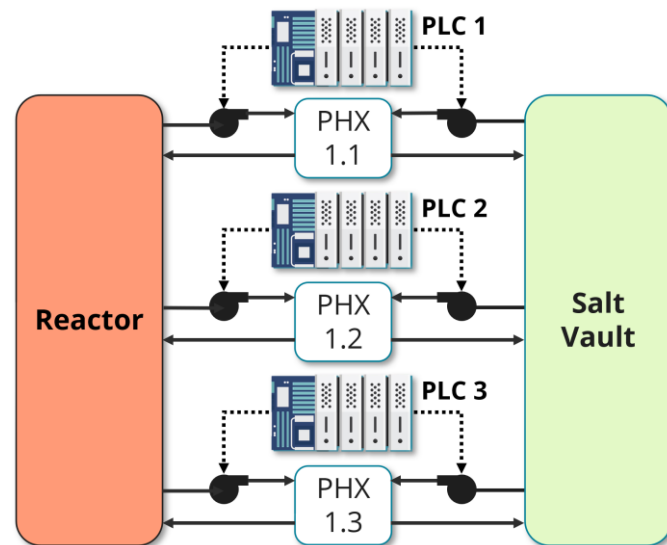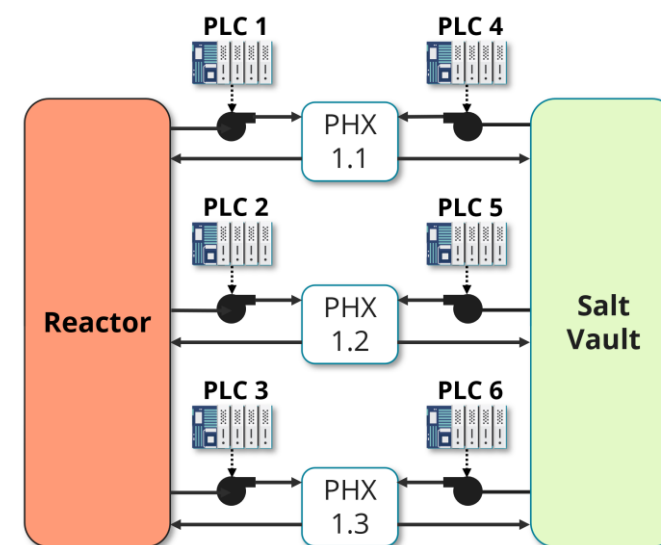
PHX Pump Control Design Candidates
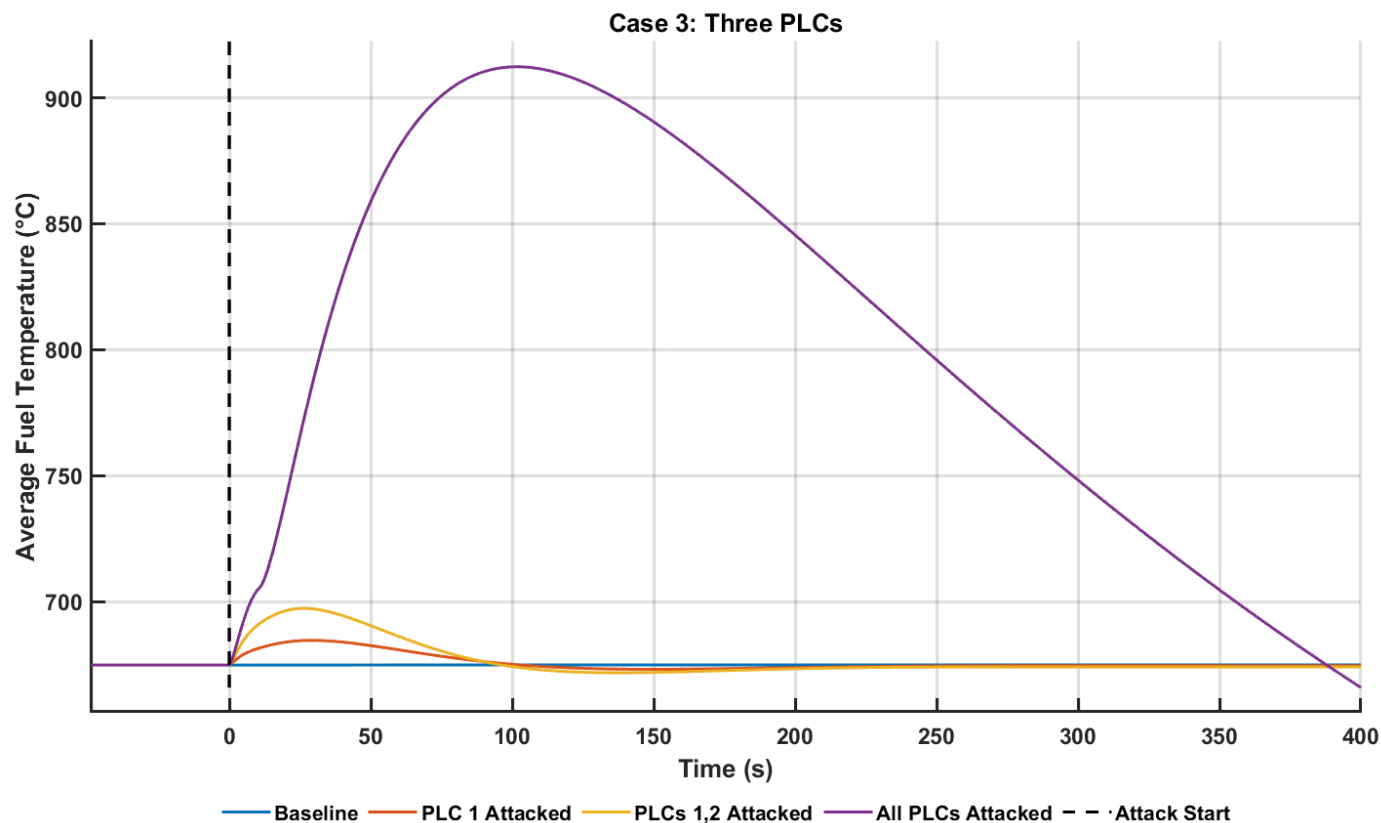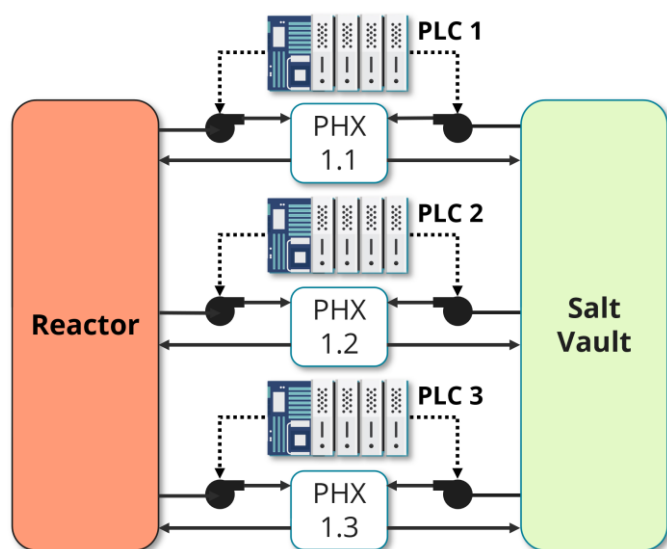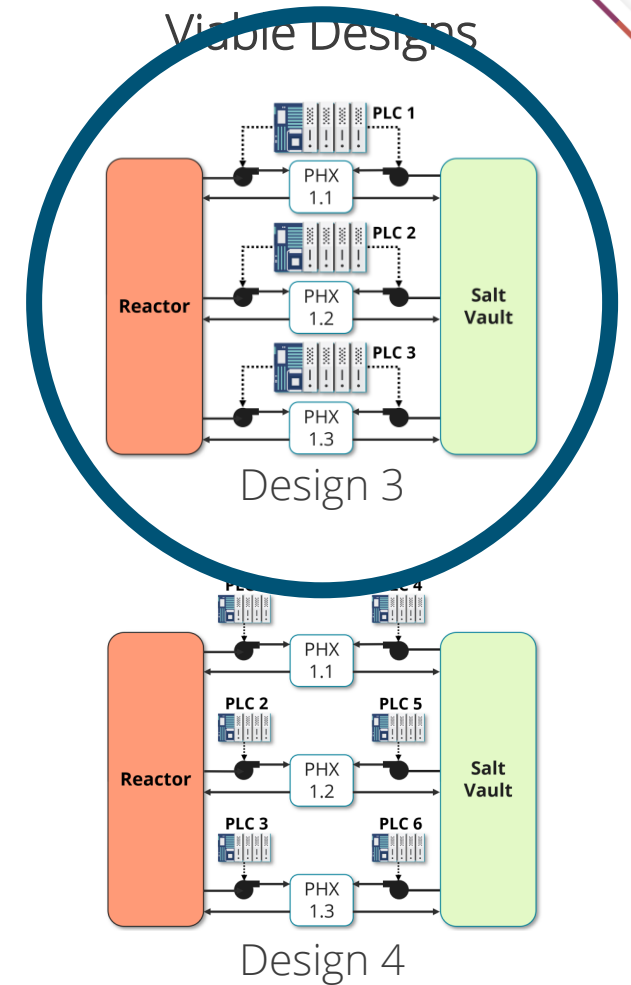

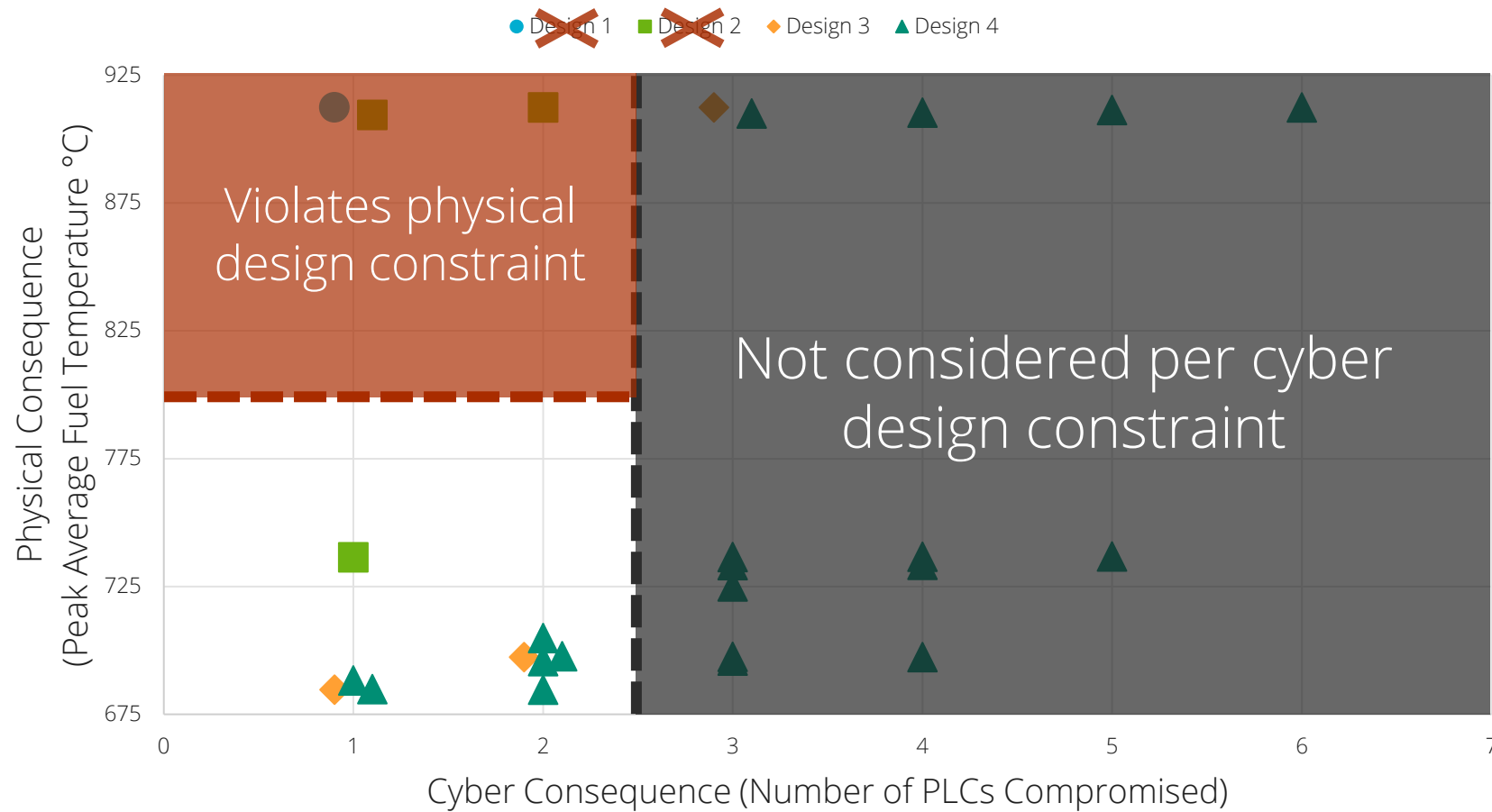Design 1

Design 2

Design 3

Design 4

Cyber-attacks were simulated using the Advanced Reactor Cyber Analysis and Development Environment (ARCADE)

Cyber-Physical Design Analysis

- Cyber Design Constraint: Passive cybersecurity controls shall be implemented to ensure that a maximum of two PLCs may be compromised by an adversary
- Physical Design Constraint: Peak average fuel temperature shall not exceed 800 °C

Impact and Future Work

- Enables advanced reactor designers to integrate cybersecurity analysis earlier in the design process
  - Can reduce costs and improve cybersecurity posture

- Provides an evidence-based approach to cybersecurity analysis

- Enables advanced reactor designers to credit SeBD features for cybersecurity design

- FY24: Defensive Cybersecurity Architecture (DCSA) for one class of advanced reactor

Thank you for your time and attention

Contact Information:
Lee T. Maccarone
lmaccar@sandia.gov