ADVANCED REACTOR SAFEGUARDS & SECURITY

ARCADE

Advanced Reactor Cyber Analysis and Development Environment

PRESENTED BY

Andrew Hahn

May 2024

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

SAND2024-06115PE

Research Questions

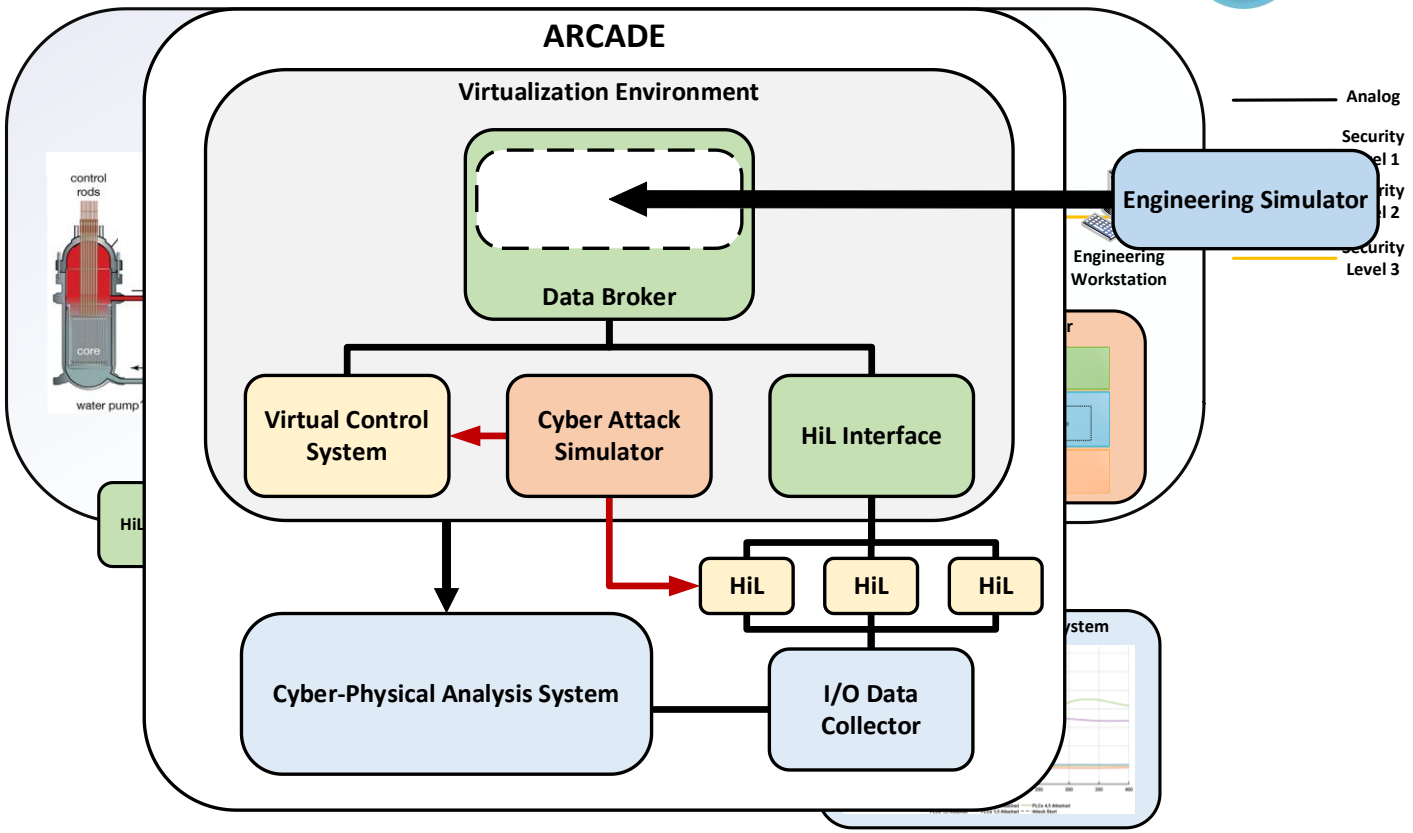
- Can Advanced Reactor inherent safety be accredited to cyber security?
  - Identify robustness factors that provide cyber resilience or where safety requires active control.
- Is a bounded set of cyber enabled accident scenarios sufficient to provide reasonable assurance of inherent cyber security?
  - For example, what operational states is the reactor most unstable?
- Do simple design requirements eliminate cyber enabled accident scenarios?
  - How can we measure the cyber security benefits of inherent safety cyber security risk?

In/Out of Scope

- In Scope:
  - Passive safety system cyber resilience
  - STPA analysis
  - Unsafe Control Action (UCA) analysis and UCA grading
  - Function/System sensitivity analysis
- Out of Scope:
  - Supply Chain – risk transfer activity not modeled in ARCADE currently.
  - Physical Attacks – Acts of physical sabotage would require extensive changes to AR vendor models (e.g., fire modeling).
  - Network Analysis – network is replicated in ARCADE, but network pathway analysis is a Tier 2 activity.

ARCADE: Engineering Security

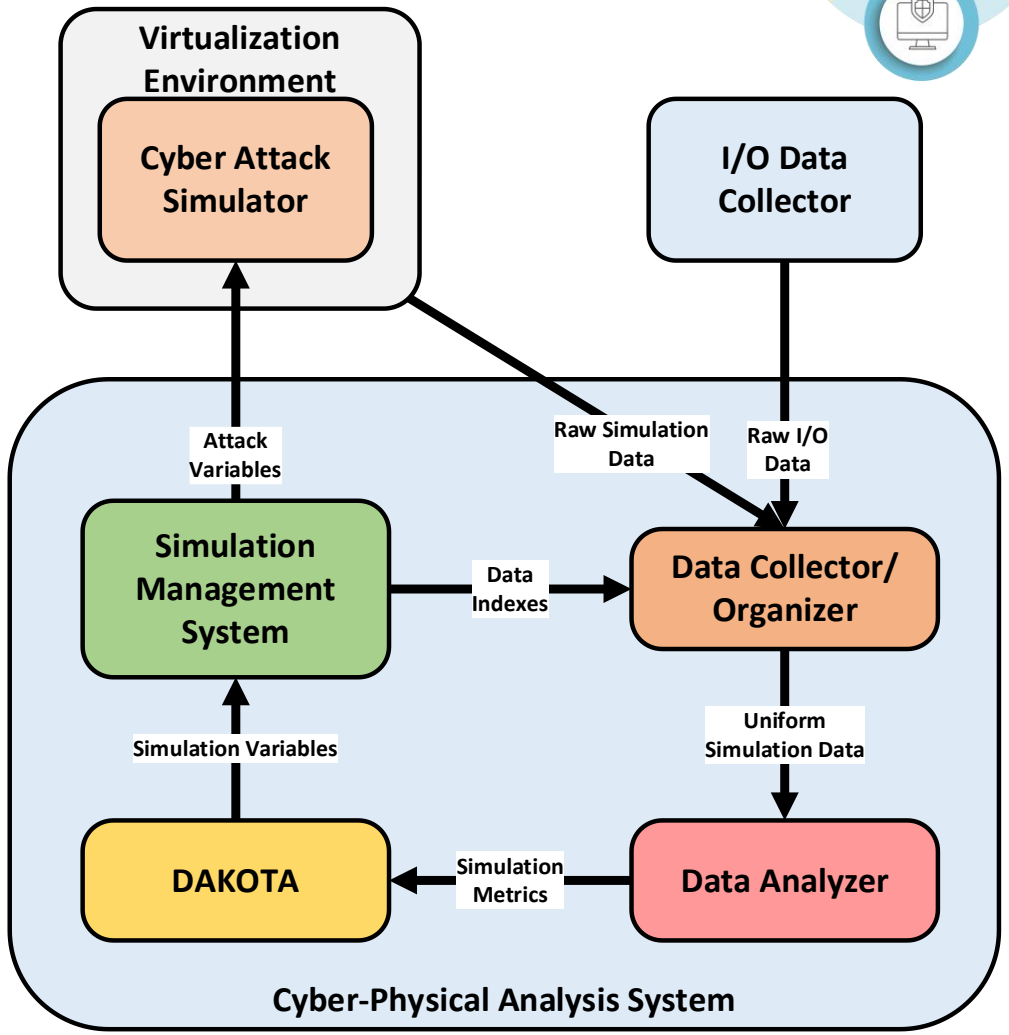
- Analyze control system sensitivity
- Simulate cyber attack scenarios and analyze consequences
- Investigate adversary pathways
- Develop architectural defenses
- Optimize detection methods and infrastructure
- Perform cyber attack exercises



ARCADE: Current Development Focus

Cyber-Physical Analysis System is primary development focus

- Drives automated cyber attack simulations
- Manages parallel ARCADE simulations to complete problem sets faster
- Collects and pre-processes simulation data into DAKOTA and human readable formats
- DAKOTA manages parametric analysis to efficiently search problem space.



Progress

- Data Broker
  - Flownex integration – complete
  - Control system emulation - complete
  - Data export system – complete
  - OPCUA system – complete
- Cyber analysis system (Expected Completion: June 2024)
  - Attack simulator – 25%
  - Simulation Management System – 90%
  - Data Analysis System – 50%
  - DAKOTA integration – 25%

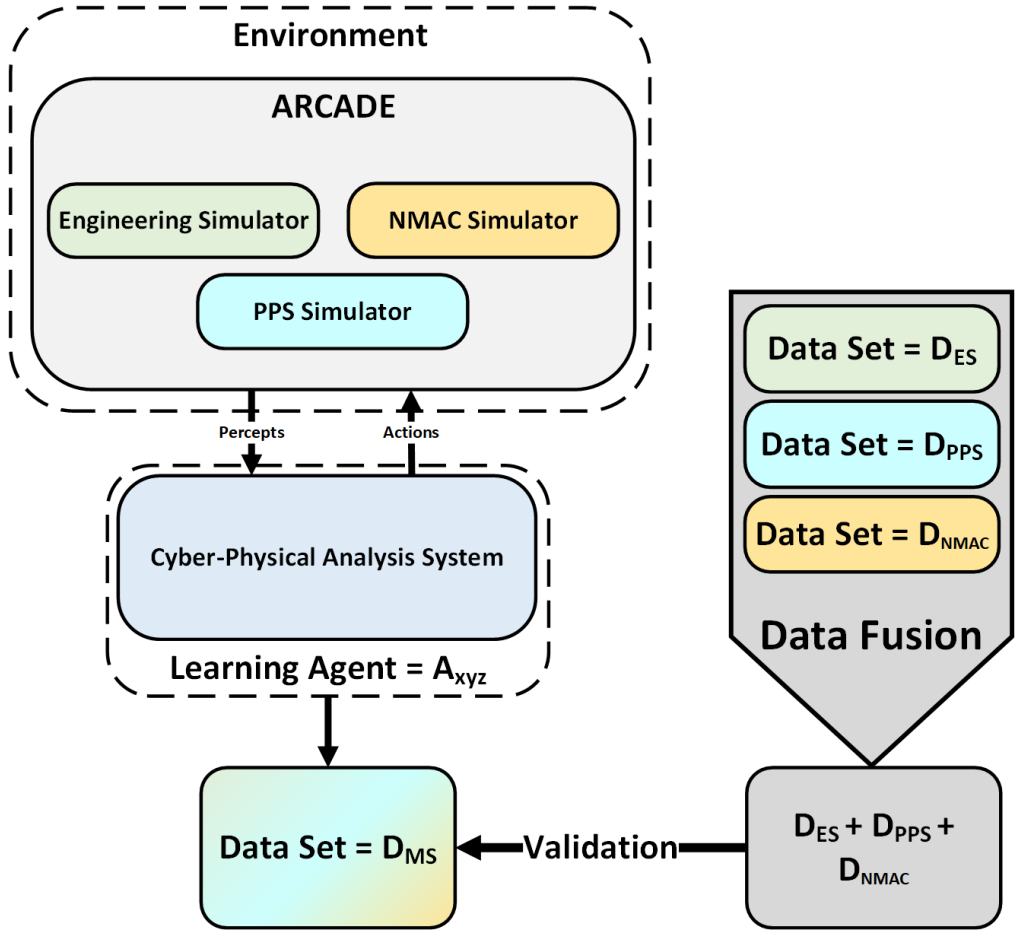
Expected FY24 Deliverables

- Opensource Release of ARCADE tools (September 2024)
  - Full installer will be available with tool suite.
  - Deployment and testing at AR vendor environment expected soon after release.
- Evaluation of quality of evidence to support SeBD and CIE (July 2024)
  - CUI data sets will be evaluated and short UUR report delivered.
- Publish conference report on ARCADE cyber analysis (August 2024)
  - Initial reports are already delivered to conferences.
  - Additional reports will be developed after final evaluation of evidence quality.

ARCADE: Future Complex Modeling (Cont.)

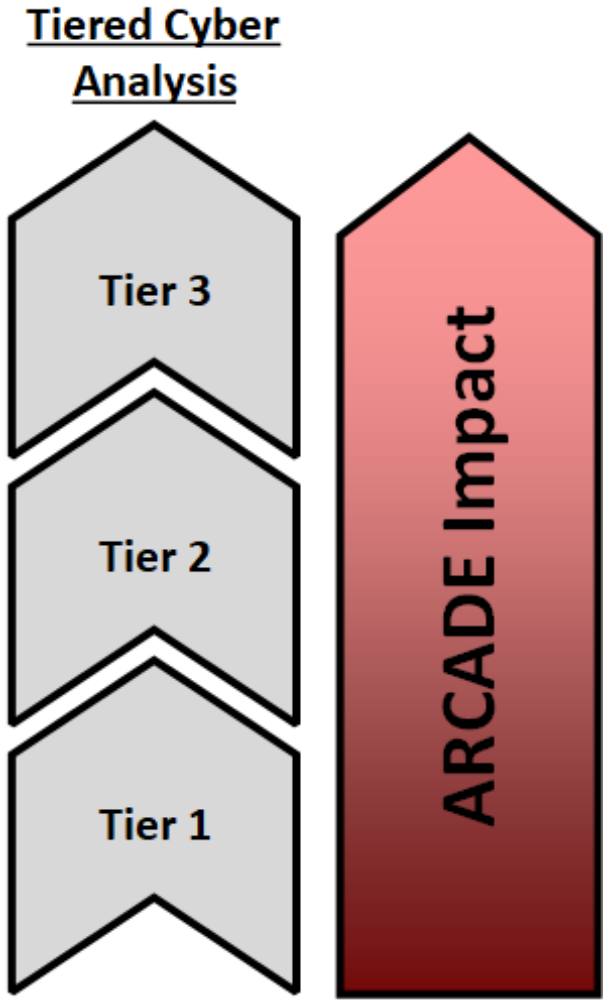
Multi-domain Simulation

- Integrated ICS, PPS, and MC&A simulators
- Individual data sets can be fused to provide validation of integrated simulation
- Learning Agent has all the necessary capabilities to perform analysis on combine simulation
  - Can rapidly evolve new cross-domain capabilities to investigate complex interactions



Impact

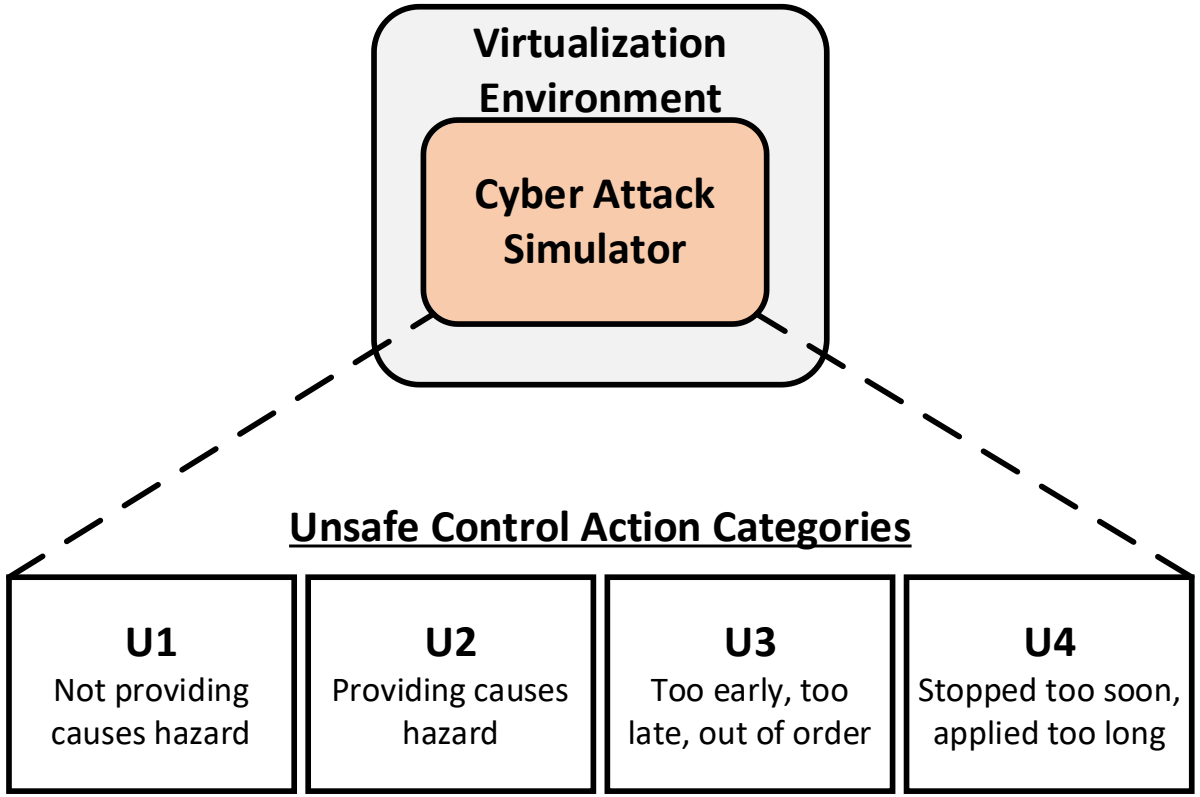
- Tier 1
  - Tier 1 of the TCA represents a novel process to incorporate cybersecurity as part of the design basis.
  - Provides evidence to support a technical basis for use of digital technology for OT systems.
  - Identifies underlying threat vectors which may be mitigated via physics.
  - Bounds and simplifies Tier 2 and 3 analysis
- Tier 2 & 3
  - The tools in ARCADE produce a highly accurate cyber-security digital twin of the AR.
  - Allows HITL integration for designer integration testing and validation.



Questions?

ARCADE: Problem Space Reduction

- The problem space for cyber attacks is too large to exhaustively search.
- Focus on STPA derived Unsafe Control Action (UCA) categories drastically reduces problem space.
- DAKOTA allows the application of many solution space search algorithms to experimentally determine most efficient method.



ARCADE: Future Complex Modeling

Multi Agent Analysis

- Agents assist in the analysis of complex environments
  - Simplify unique data set production from environments
- The cyber-physical analysis system in ARCADE is a multi-agent system
- Iteratively improved through simulation runs
  - Capability gaps are identified, closed, and provide more data to identify further gaps
- A finalized Agent after **x** iterations (A_x) produces the most complete data set possible from a given environment.