ADVANCED REACTOR SAFEGUARDS & SECURITY

ARCADE & Tier 1 Analysis

PRESENTED BY

Andrew S. Hahn

SAND2026-20440PE

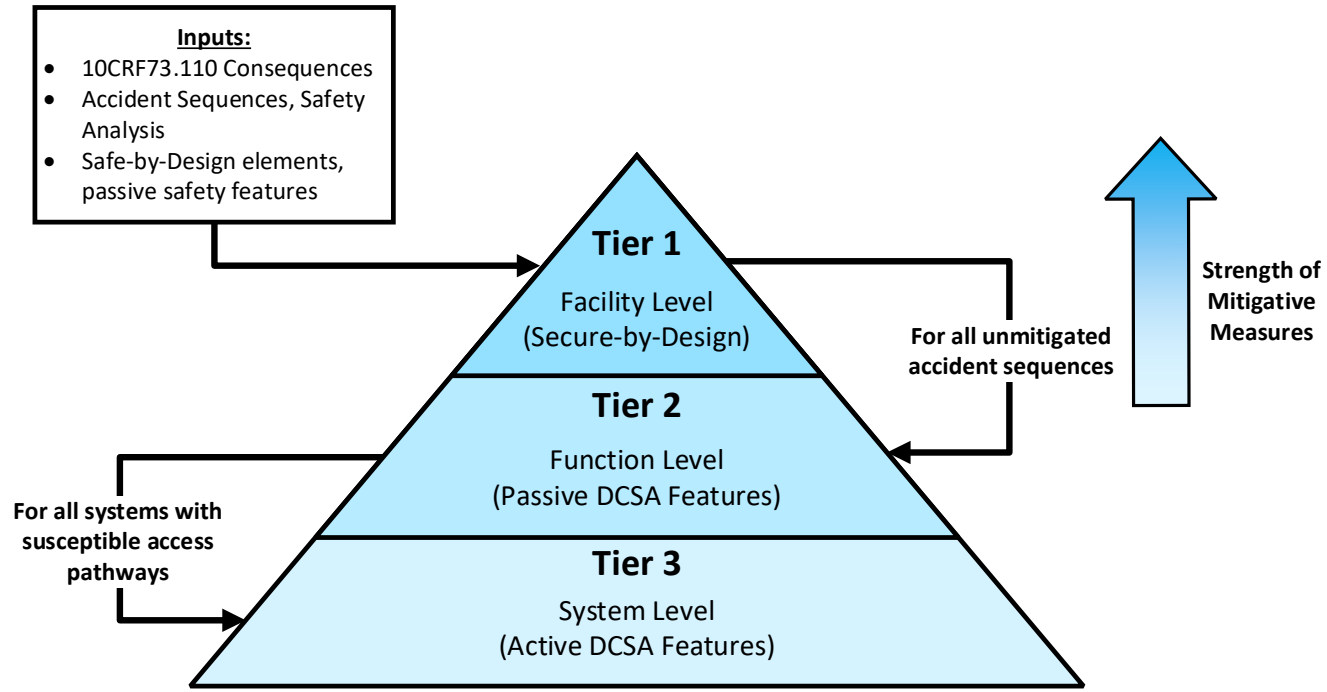
Cybersecurity By Design

NRC RG 5.96 (DG 5075) outlines the Tiered Cybersecurity Analysis (TCA) which requires identifying and evaluating all potential cyberattack sequences which lead to consequence.

- The highly coupled nature of NPP's requires high fidelity simulation of attacks to determine consequence.
- Using conventional methods is impossible as the number of simulations required has a factorial relationship to sequence length.

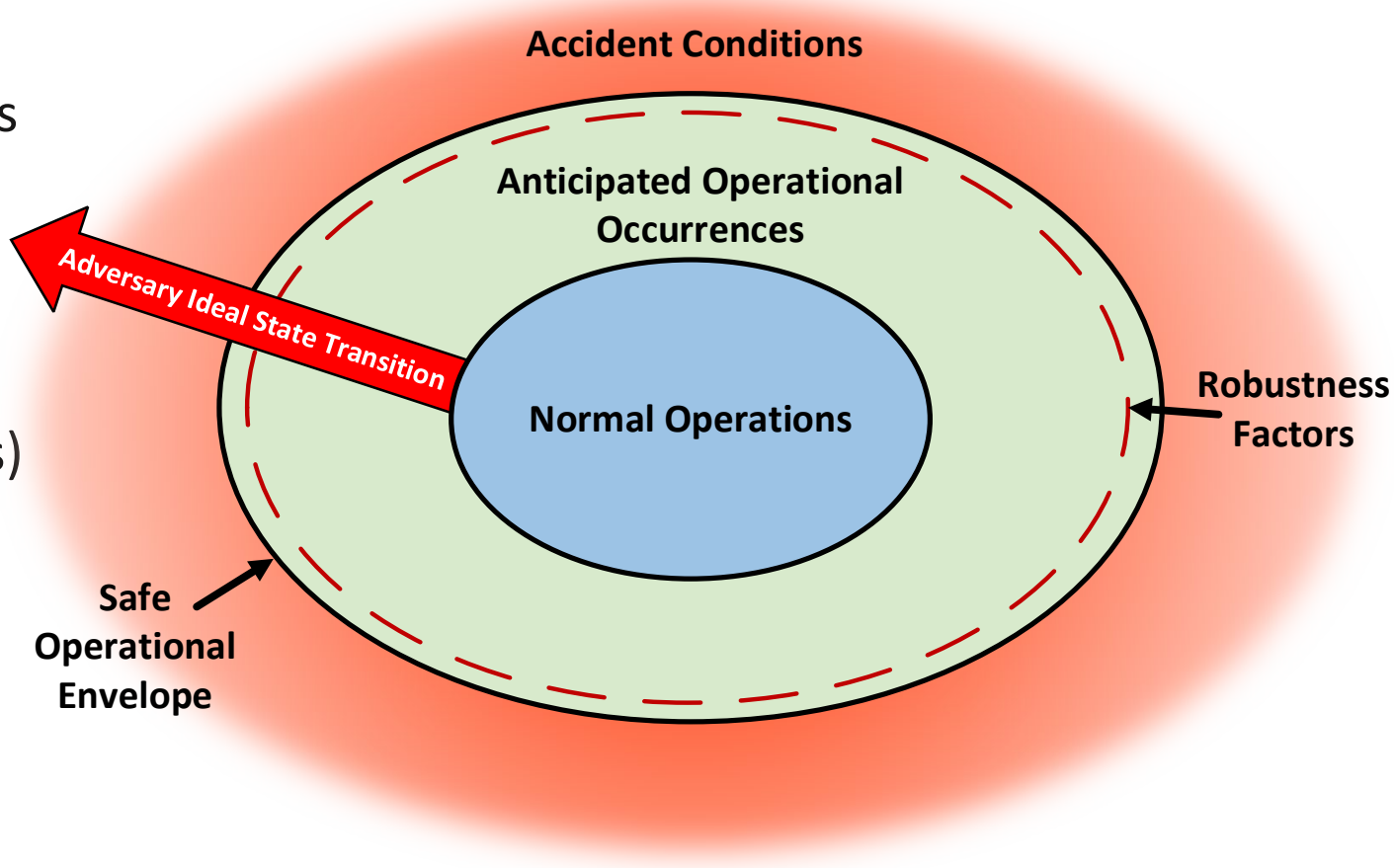
$$C(n,r) = \frac{n!}{(n-r)!r!}$$

$$C(100,5) = \frac{100!}{(100-5)!5!} = 75{,}287{,}520$$



Problem Search Space

- The Advanced Reactor Cyber Analysis and Development Environment (ARCADE):
- Maps the physics based robustness factors which prevent cyber consequences from progressing
- Identifies the gaps in the robustness factors which can be eliminated by non-cyber Independent Protection Layers (IPLs)
- Evaluates the effectiveness of non-cyber IPLs
- Identifies break out events which are not able to be mitigated with non-cyber IPLs



Solution Optimization and Constraints

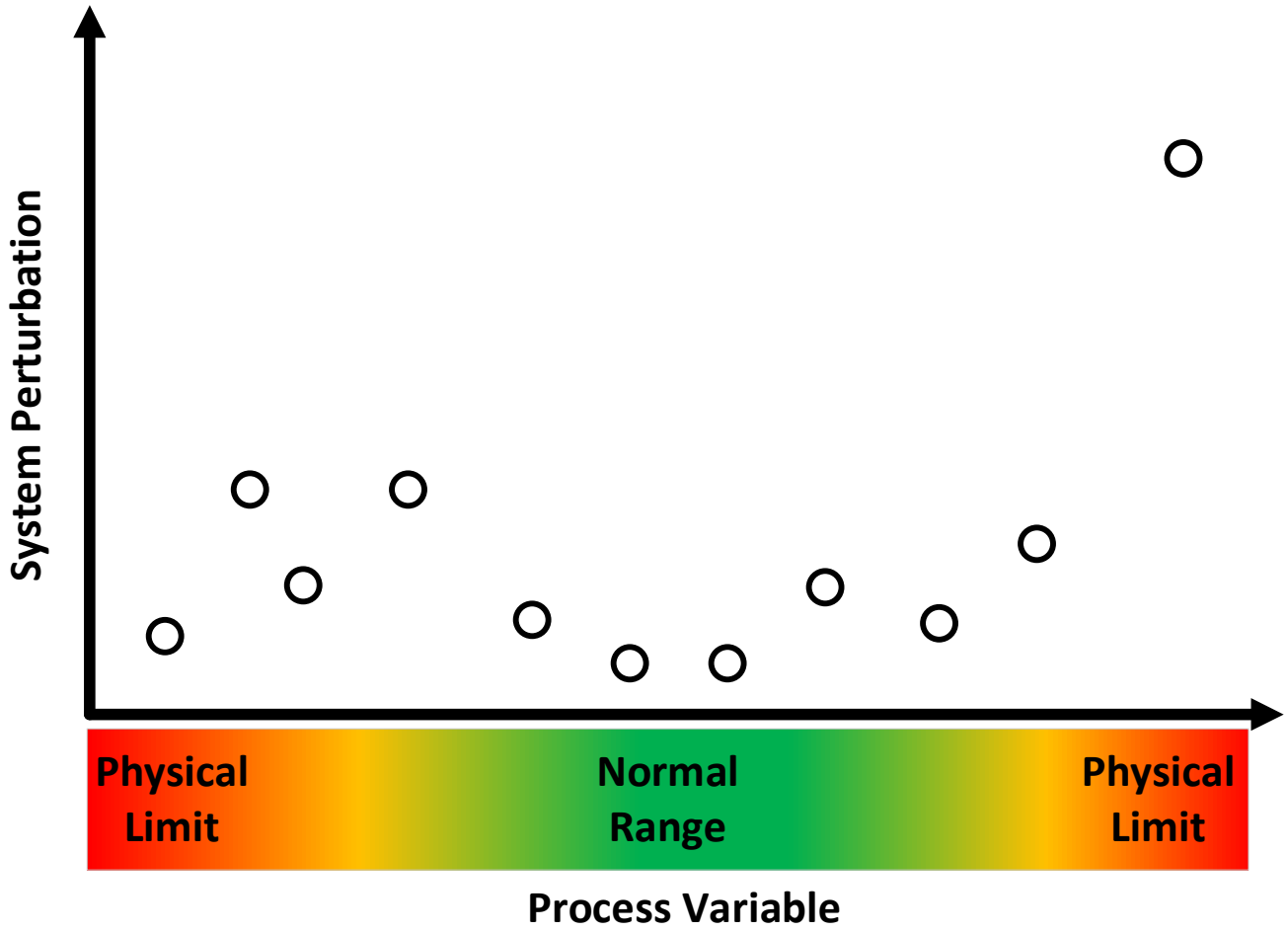
- The Unsafe Control Action (UCA) concept from the System Theoretic Process Analysis (STPA) process provides a categorization of all possible threats against a system.
  - This concept structures the efforts to automate the execution of all possible cyber-threat control actions.
  - STPA is context and human driven. Careful consideration must be made when automating UCA simulations to eliminate the need for context.
  - Temporal UCA's drive most of the contextual requirements and require special consideration during searches to maintain efficiency.
- Search must be intelligent, only investigating pathways which are likely to cause harm.
- Massive parallelism is required to efficiently parse the problem space.

Unsafe Control Action Categories

U1	U2	U3	U4
Providing causes hazard	Not providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long

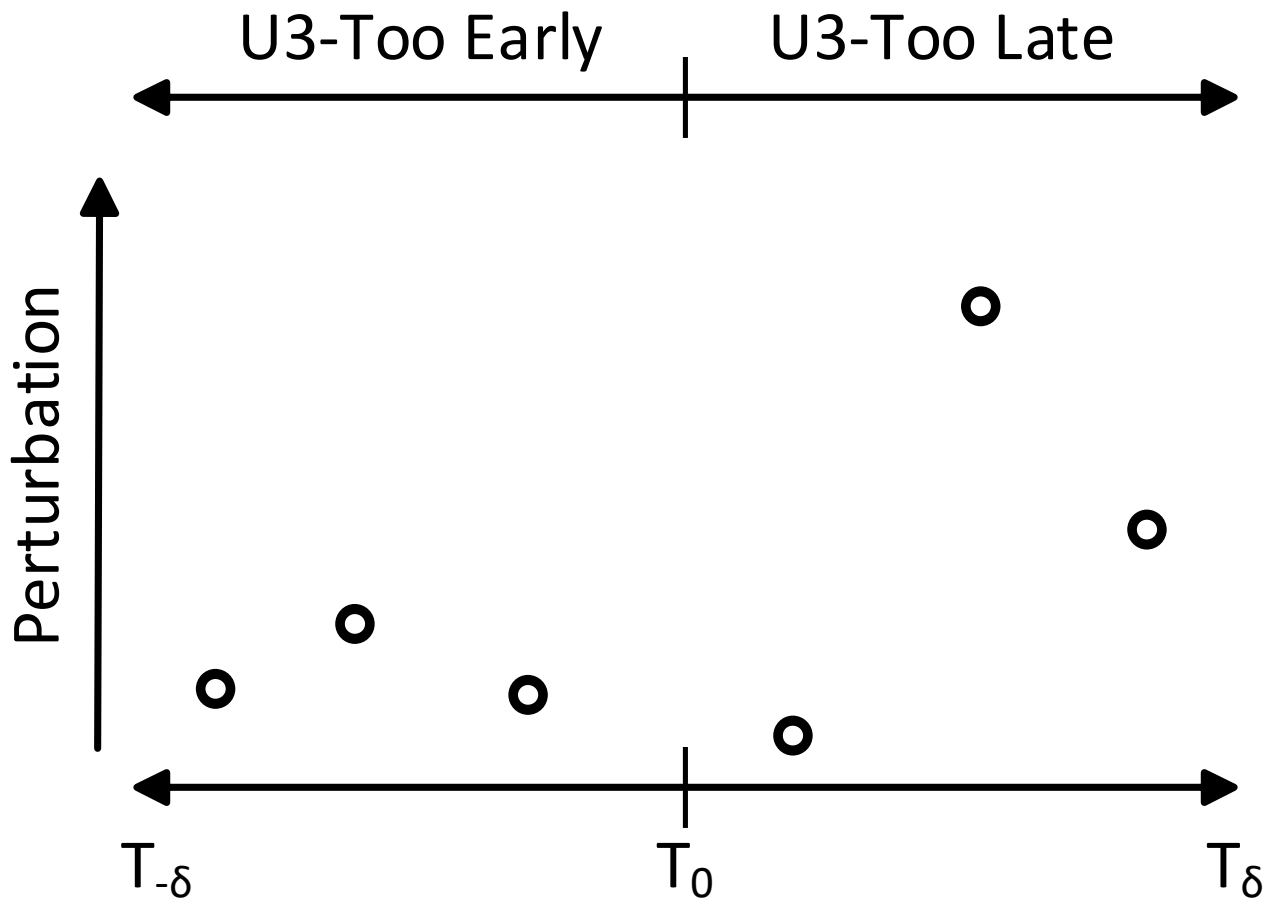
Starting the Search

- The first sweep of UCA searches will be based on single UCA events in the U1 category under steady state conditions.
- The search will be regimented across the physical limits of the process control. The granularity will be controlled by the user.
- System perturbation will be measured across the plant as maximum deviation from optimal and maximum derivative (dx/dt)
- The UCAs with significant perturbation will be subject to searches in U2-U4 UCA categories.



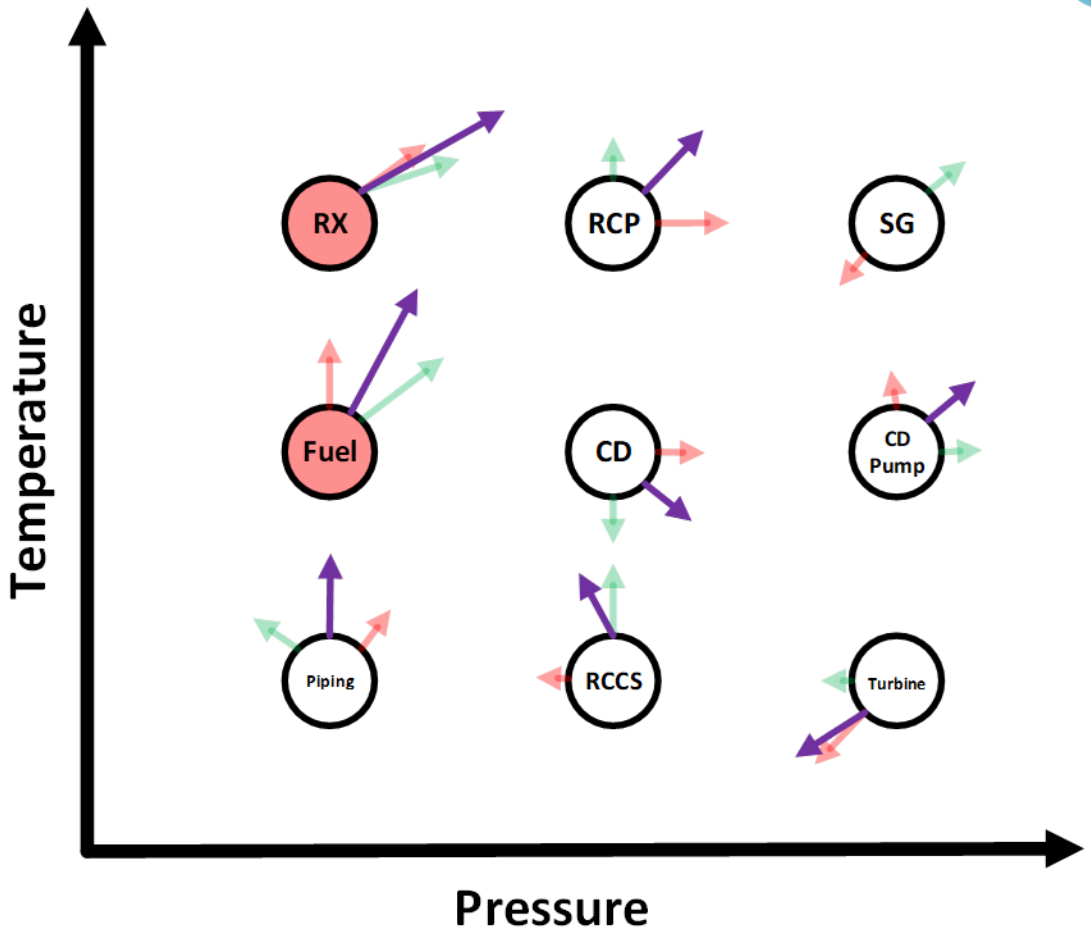
Temporal UCA Searches

- Temporal UCA searches will center on the time T_0 which the control surface responded to the previous UCA.
- The search will span from $T_{-\delta}$ to T_{δ} which can be set by the user or automatically determined from the control surface settling time of the previous UCA.
- The sweeps for U4 are similar, a delta is determined by the user or automatically with the baseline length of actuation being determined from the previous UCA.

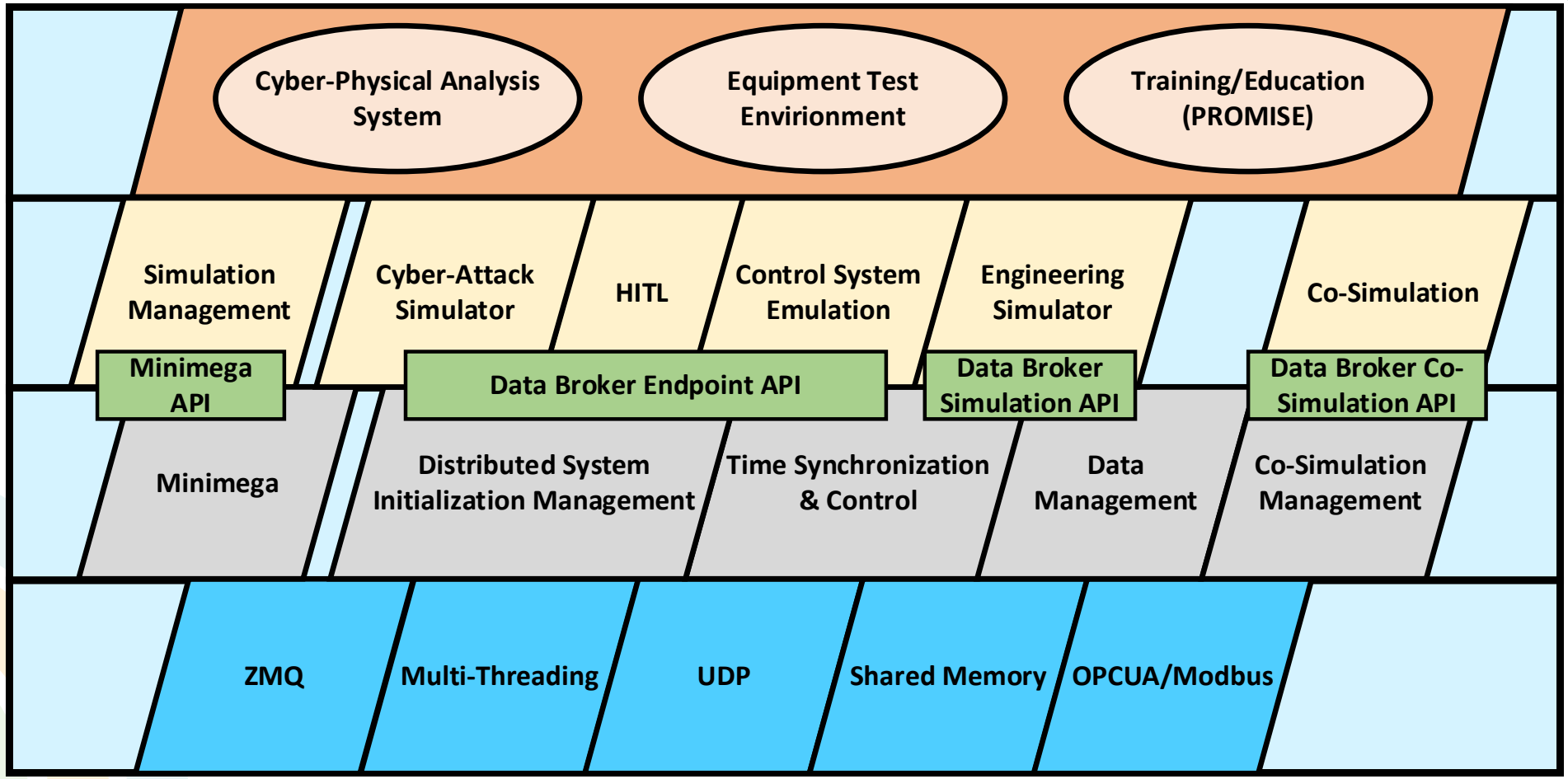


UCA Combination Searches

- The subsequent UCA searches focus on combinations of UCAs which could cause consequences.
- Matrixes of all single and combined timing UCA's are compared to discover potential constructive interference.
- UCA combinations with significant alignment are selected for simulation.
- Timing between UCAs is varied to validate maximal perturbation.
- Time based UCAs (U3 & U4) are re-evaluated on the combinations
- Process repeats until search maximum depth is reached.

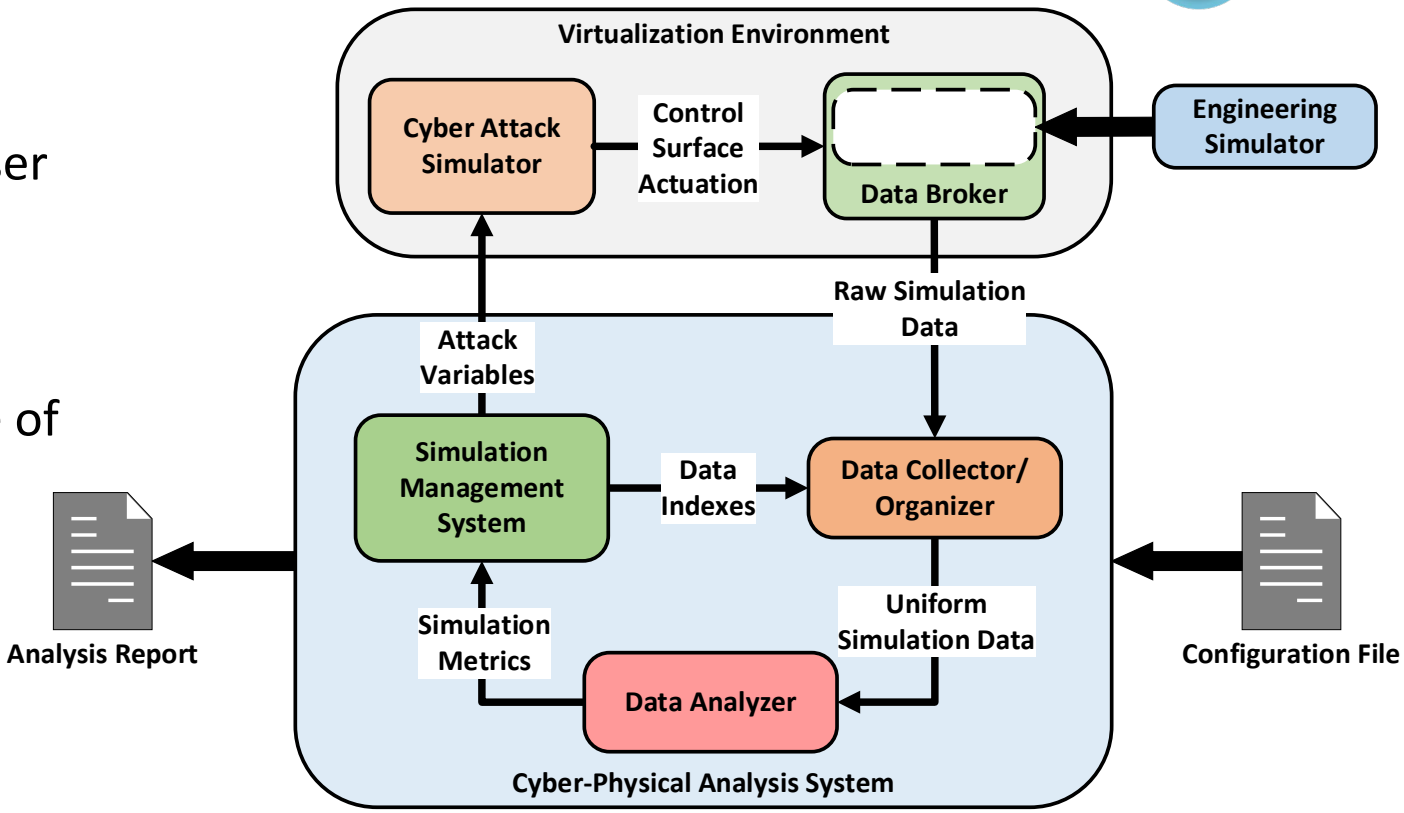


ARCADE System Development



ARCADE Current Capabilities

- Data analysis system has closed the loop on automated UCA sequence searches
  - Input is a configuration file in which the user defines the boundaries of the search
  - Output is a complete analysis report.
- Able to search through U1 UCAs and is capable of activating U2 UCAs
- Single machine compute limited
- Compatible with Flownex and Simulink based simulators



Asherah Nuclear Power Plant Simulator

What Asherah is:

- Asherah is developed & maintained by the University of Sao Paulo
- Simulink model of a 2,772 MWt two-loop PWR, loosely based on the TMI Unit 1 B&W design.
- Can be run with or without internal Simulink controllers
- External controllers and human machine interfaces can be interfaced with using ModbusTCP or OPC UA
- Tuned using PARCS/RELAP

What Asherah is not:

- Qualified plant simulator
- Based exactly on an existing plant
- Complete simulation of all controllers, alarms, and annunciators found in an actual plant

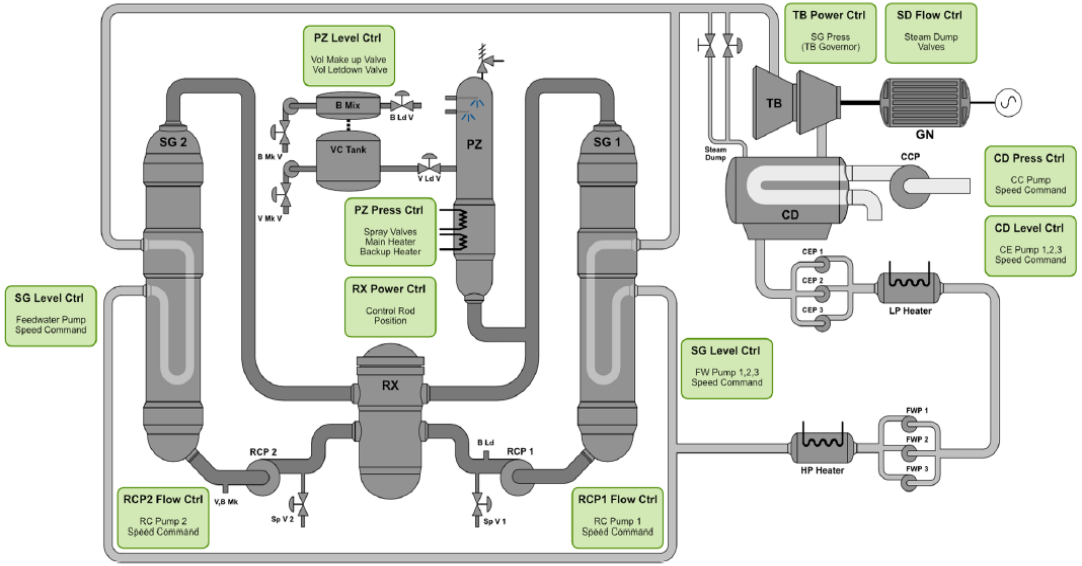
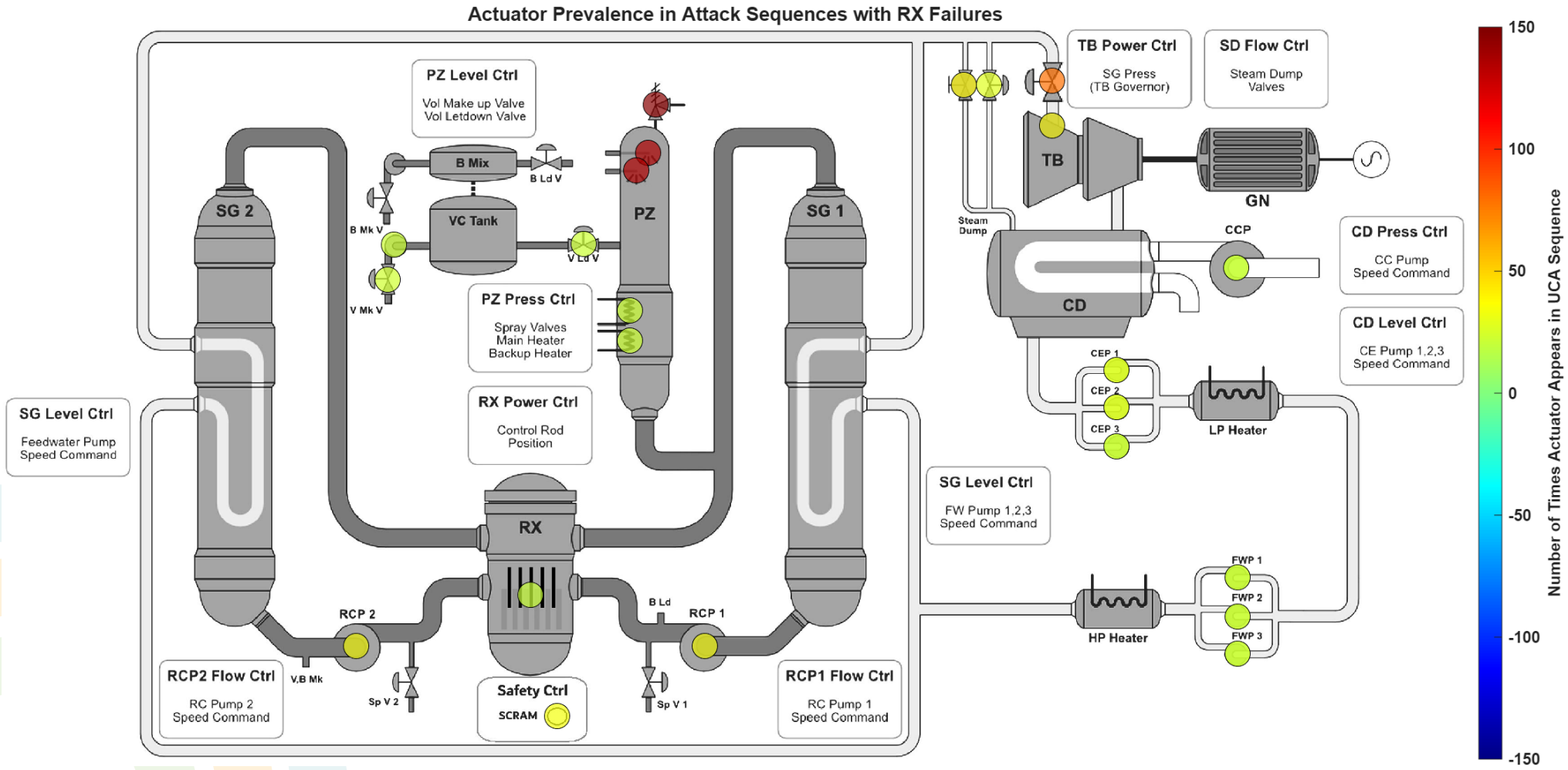
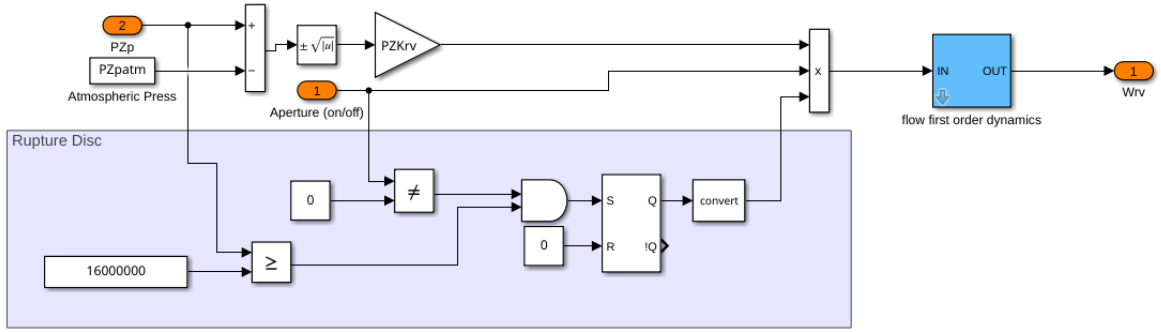


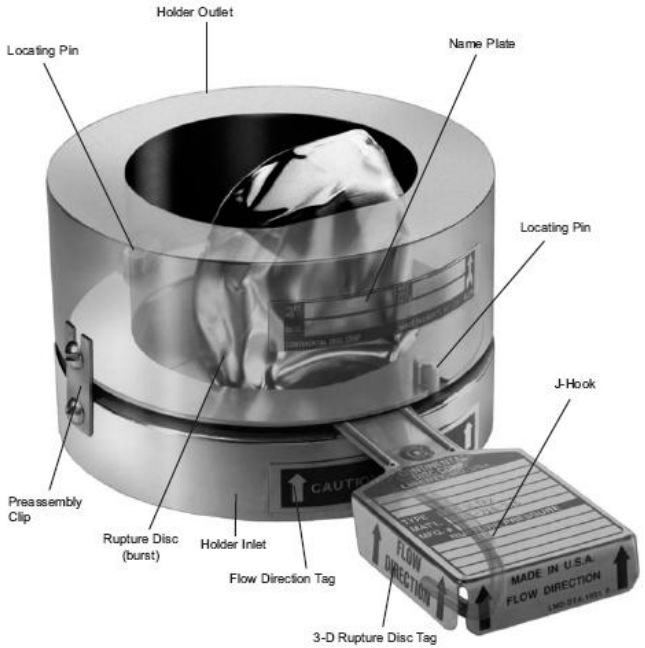
Image: Silva RB, Shirvan K, Piqueira JR, Marques RP. Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment. International Conference on Nuclear Security (ICONS), 10-14 Feb 2020 in Vienna Austria 2020.

Asherah Analysis Results



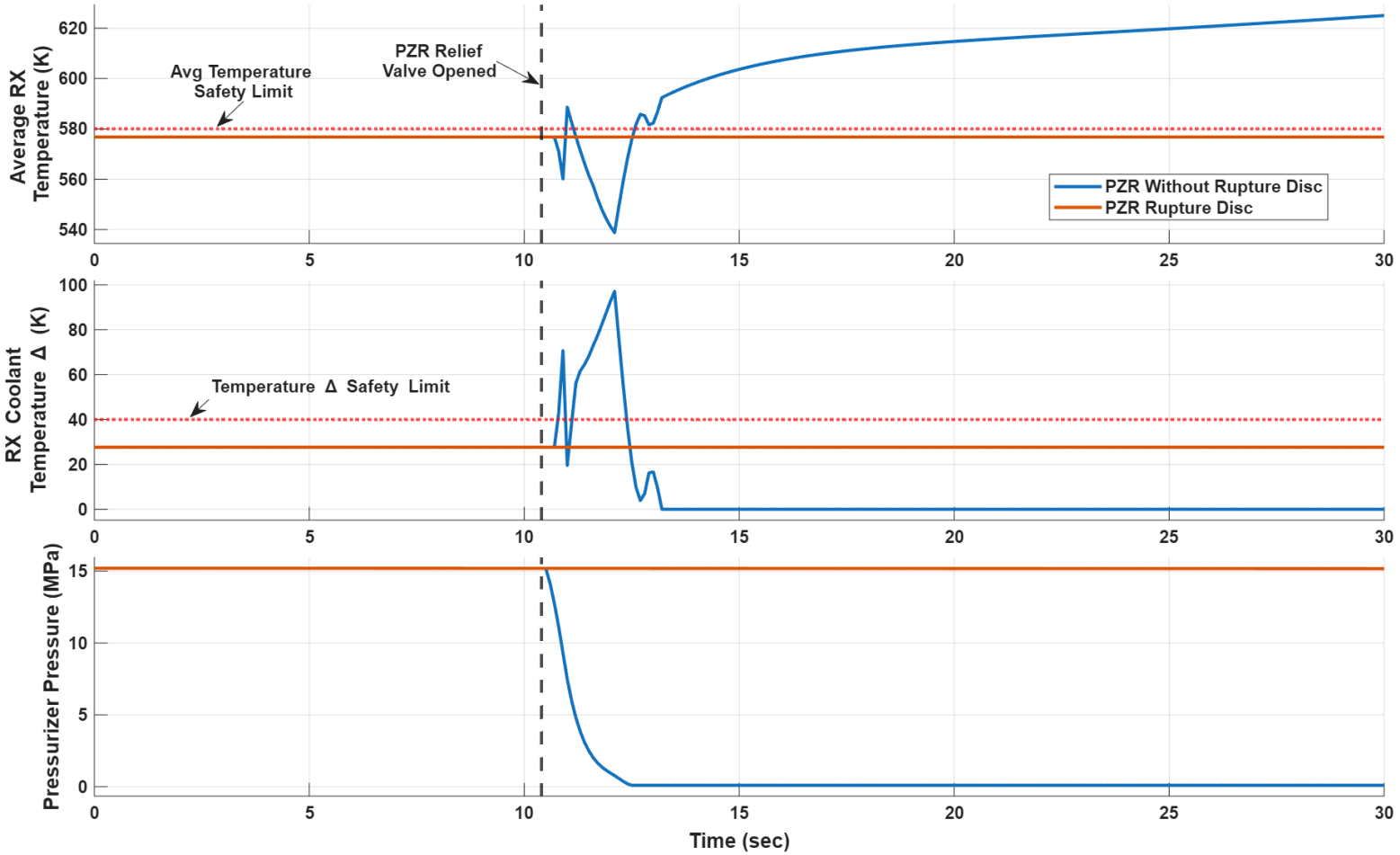
Asherah Modifications





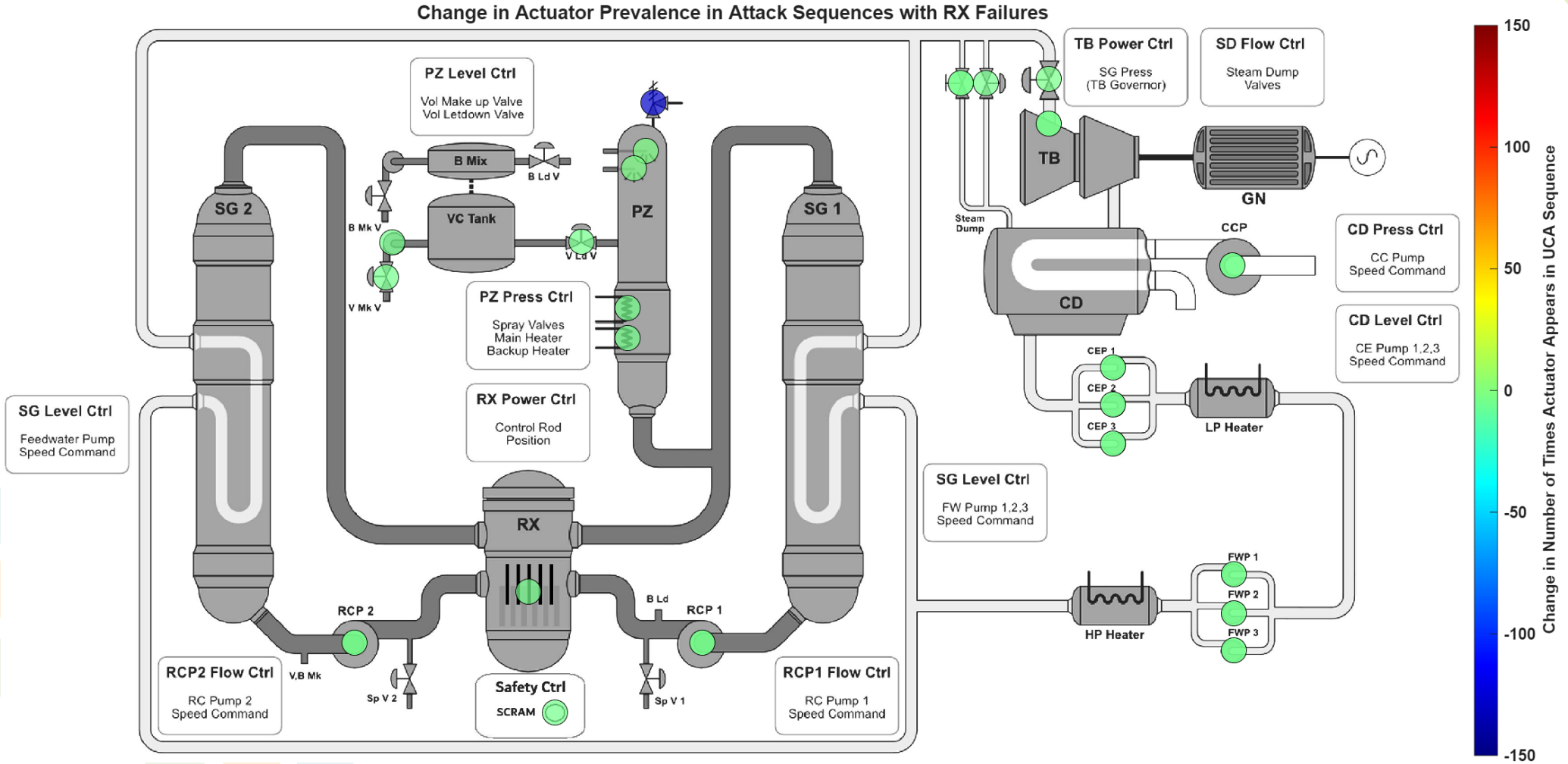
- Based on the results of the analysis, Asherah was modified to prevent adversary harm through the pressurizer relief valve.
- The valve was modified to include a rupture disc in-line with the valve which:
- Prevents the adversary from using the valve to cause harm.
- Allows the release of pressure during an actual over pressure event.
- While this inexpensive modification may not meet the operational requirements of the plant, it is an example of using ARCADE for engineering decisions and evaluating their impact on safety and security.

Modified Asherah Testing



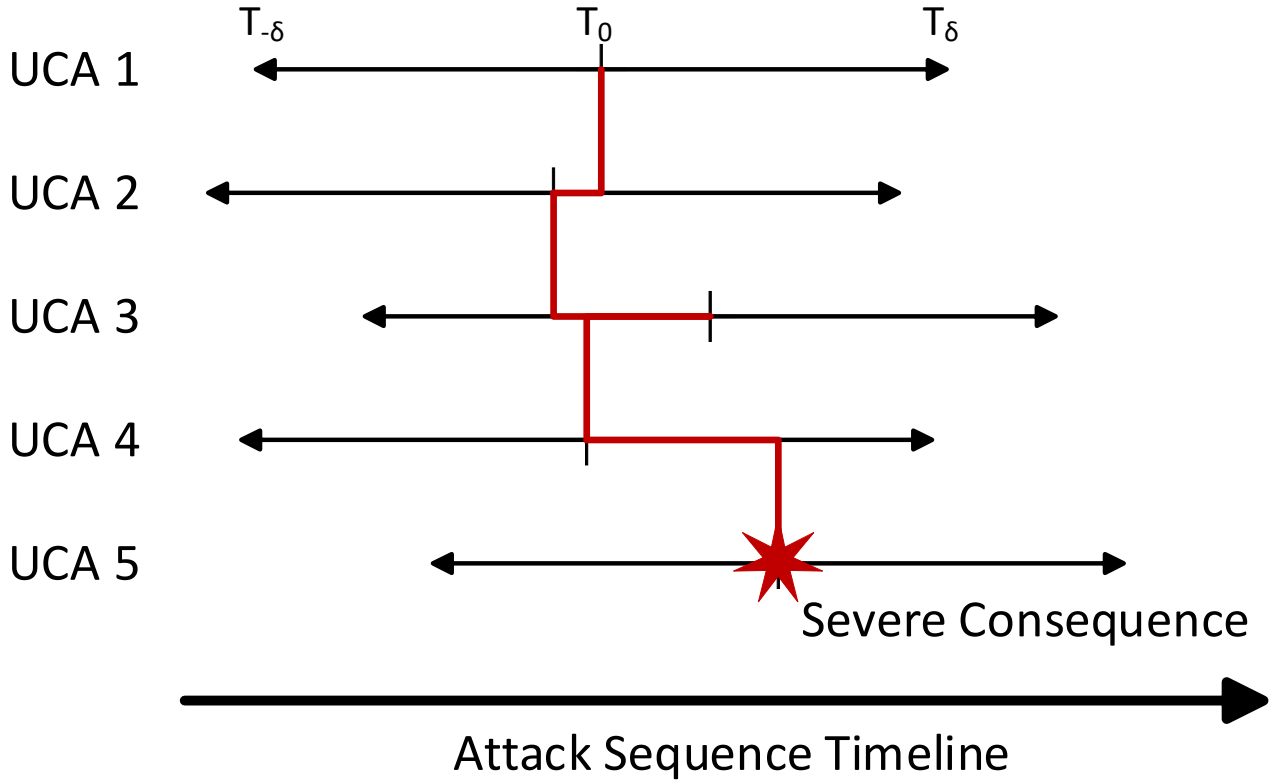
- The pressurizer (PZR) relief valve redesign was tested to evaluate its efficacy.
- The rupture disc design successfully prevents the single UCA threat of the valve being maliciously opened.

Asherah Risk Reduction Results



ARCADE Future Capabilities

- Support for additional simulators
- Cluster support for massively parallel searches.
- Temporal UCA's (U3-U4) allow searching through full spectrum of UCA's.
- Enable analysis of dynamic time-based failure modes and effects which are beyond all current human driven analysis methods.
- Validation of search method completeness



FY26 Milestones

- M2: Demonstration of Efficient Cybersecurity Design Using ARCADE
  - ✓On schedule
  - ✓Simulation results complete
  - Report start in May
- M4: Release of ARCADE Analysis System
  - ✓On schedule
  - ✓Opensource V2 of ARCADE released
  - ✓ARCADE Analysis Engine package ready for licensing
  - Licensing process started (April)

Questions