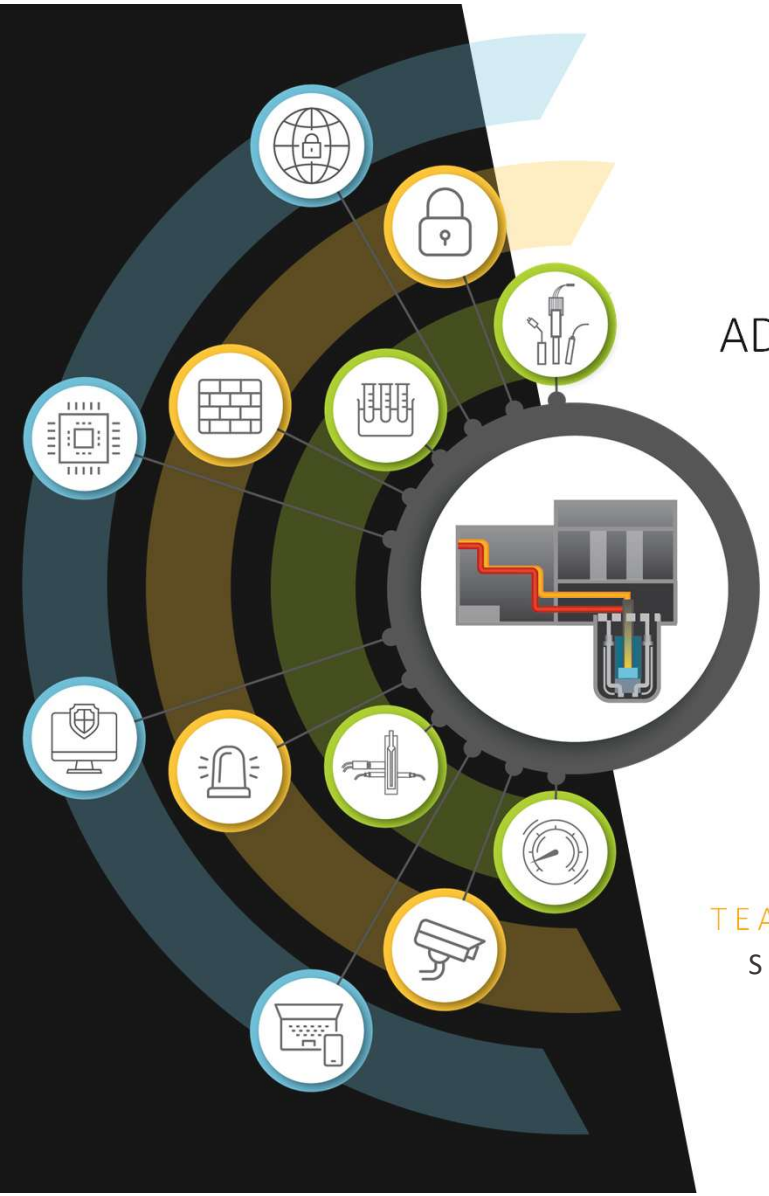


ADVANCED REACTOR SAFEGUARDS & SECURITY

Semi-Automation of Model-Based Engineering for Cybersecurity by Design: Progress Update

TEAM:

Shannon Eggers, Sonali Sinha Roy, Kevin O'Rear, Ross Hays, Joe Oncken

April 2026

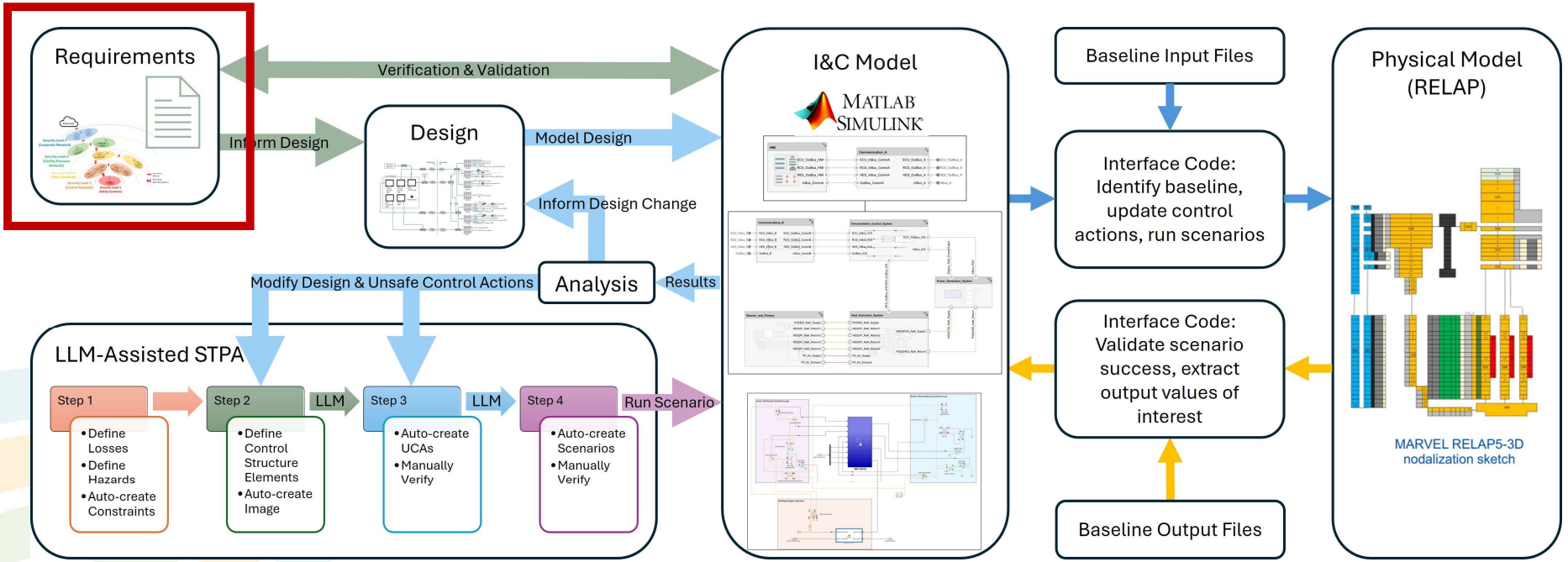
INL/MIS-26-91723

Idaho National Laboratory | U.S. DEPARTMENT OF ENERGY

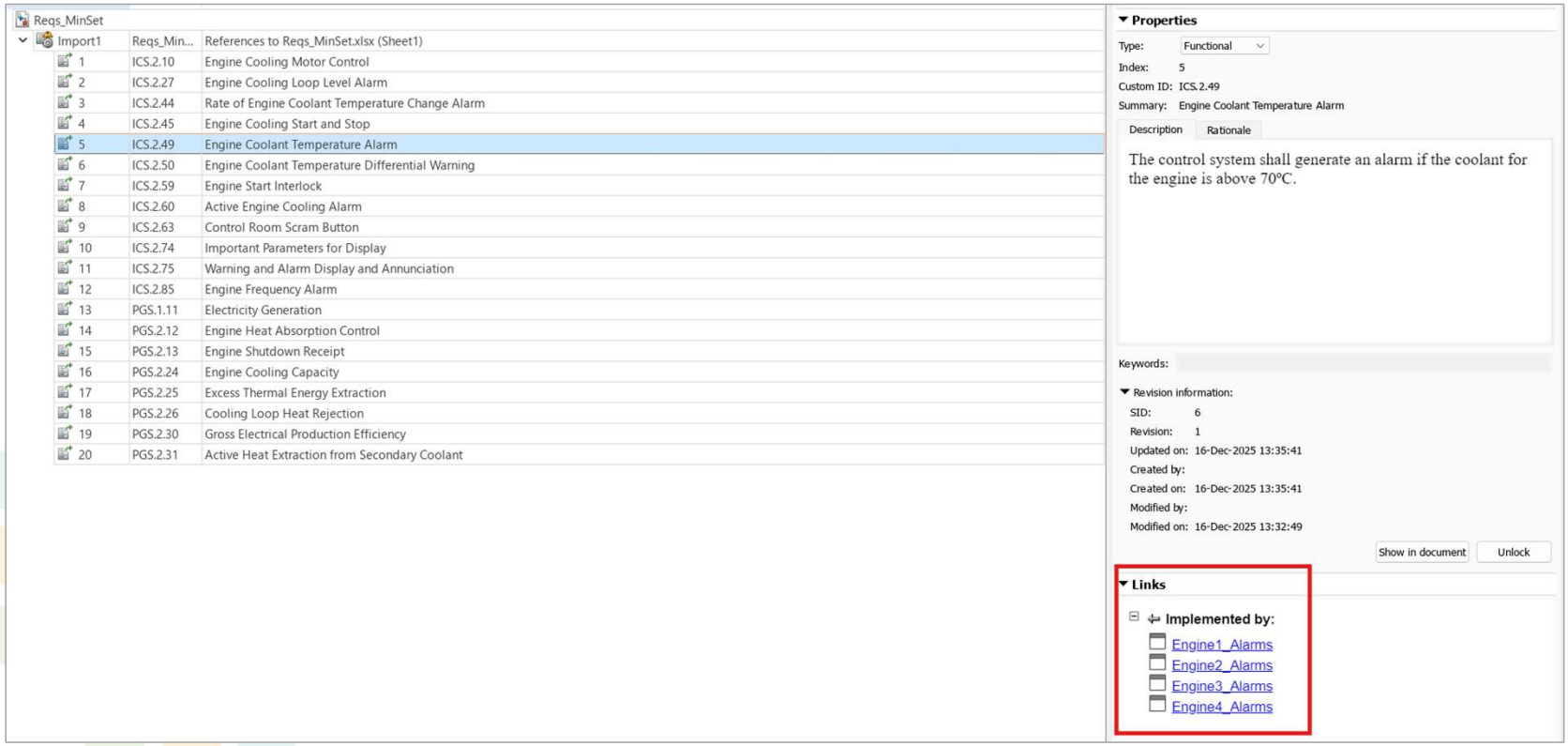
Motivation

Cybersecurity risks in nuclear systems are often identified too late in the design process, when changes are expensive and options are limited. A model-based engineering (MBE) approach that integrates digital risk management across the systems engineering lifecycle addresses this gap, providing early visibility and enabling coordinated design decisions that balance safety, performance, and security.

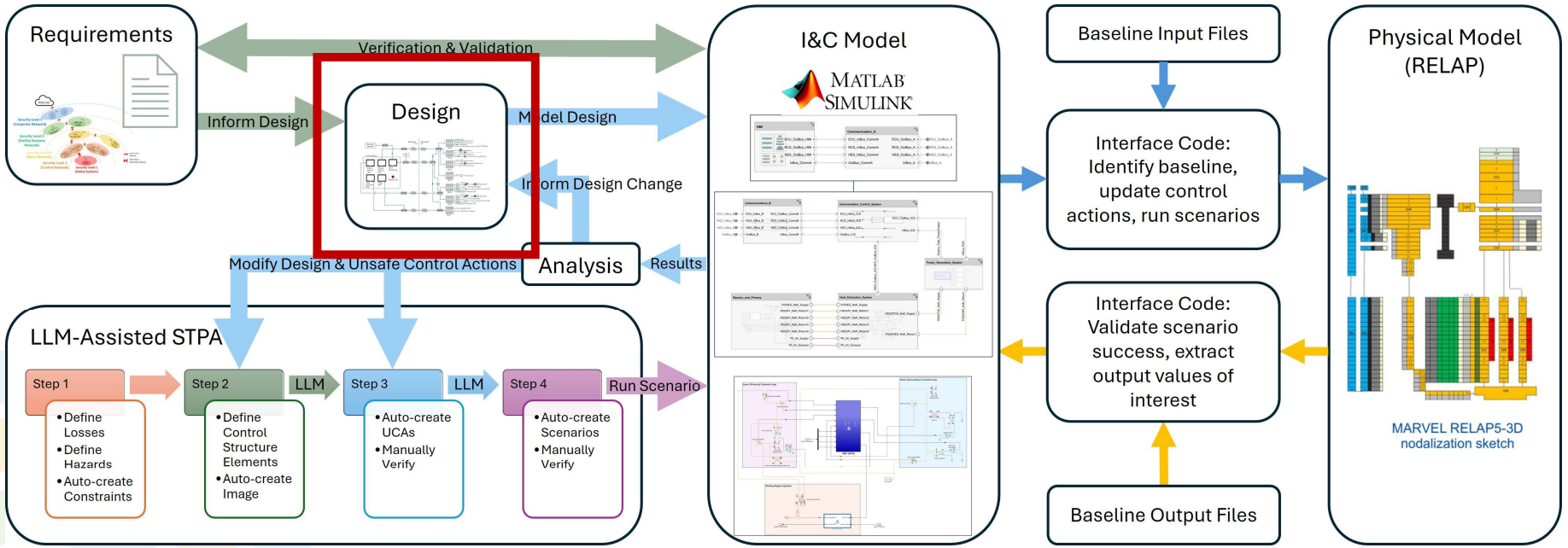
Overall MBE Ecosystem



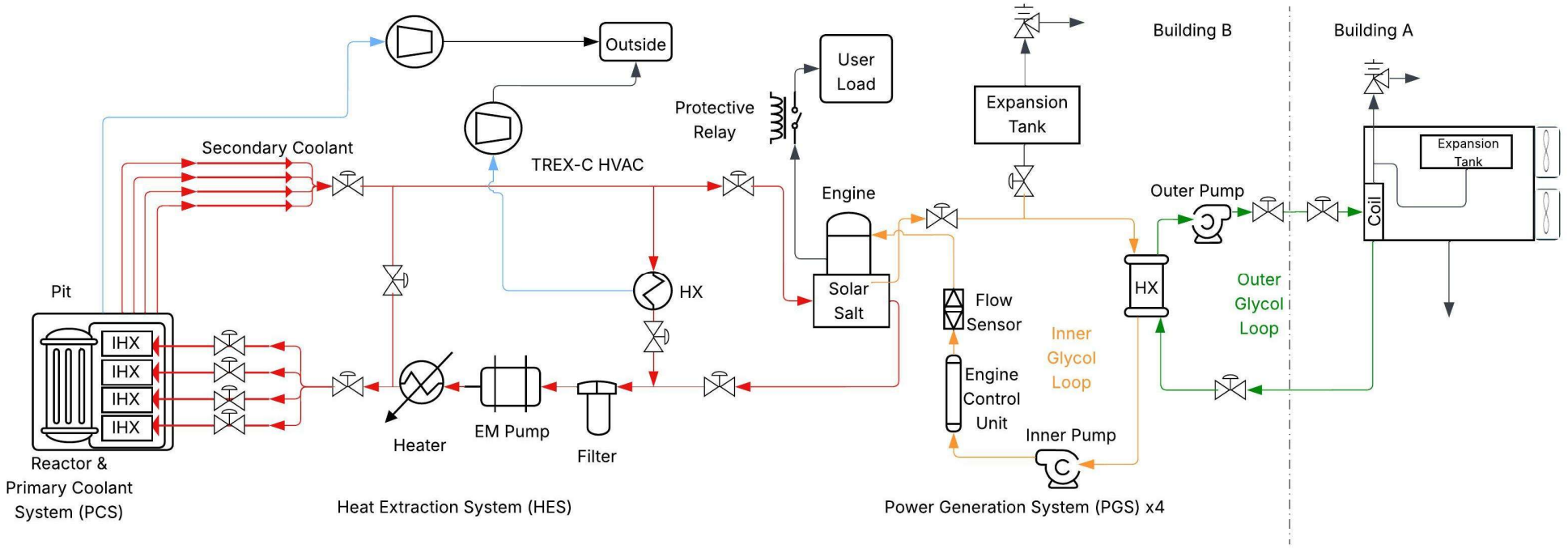
Requirements Integration



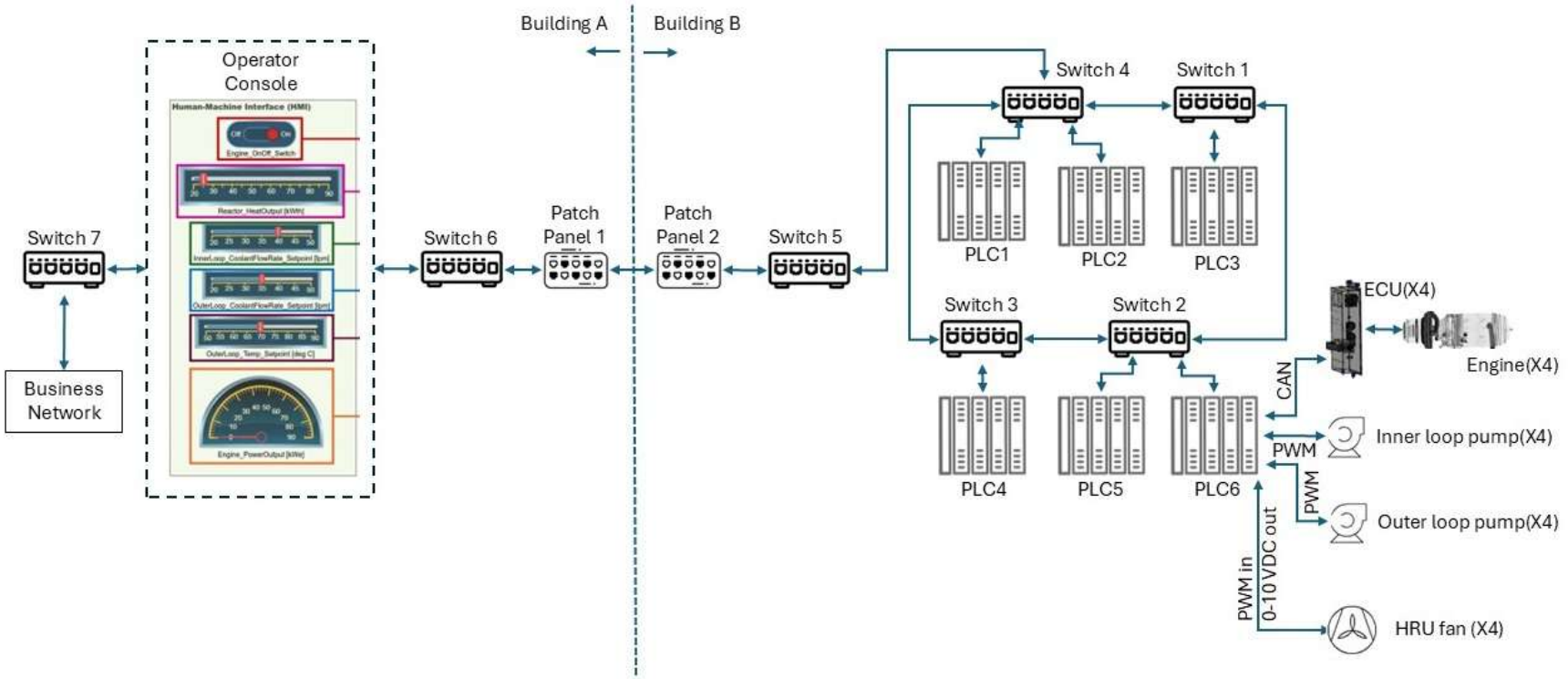
Engineering Design



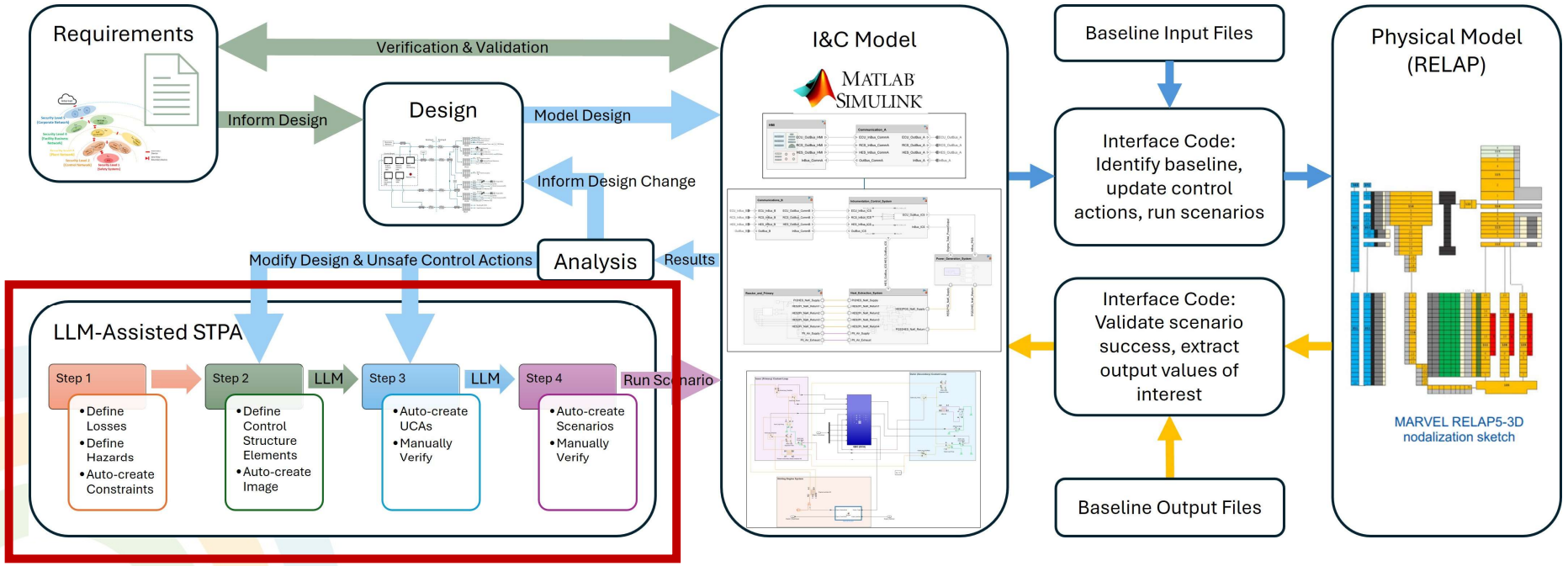
High-Level Piping & Instrumentation Diagram



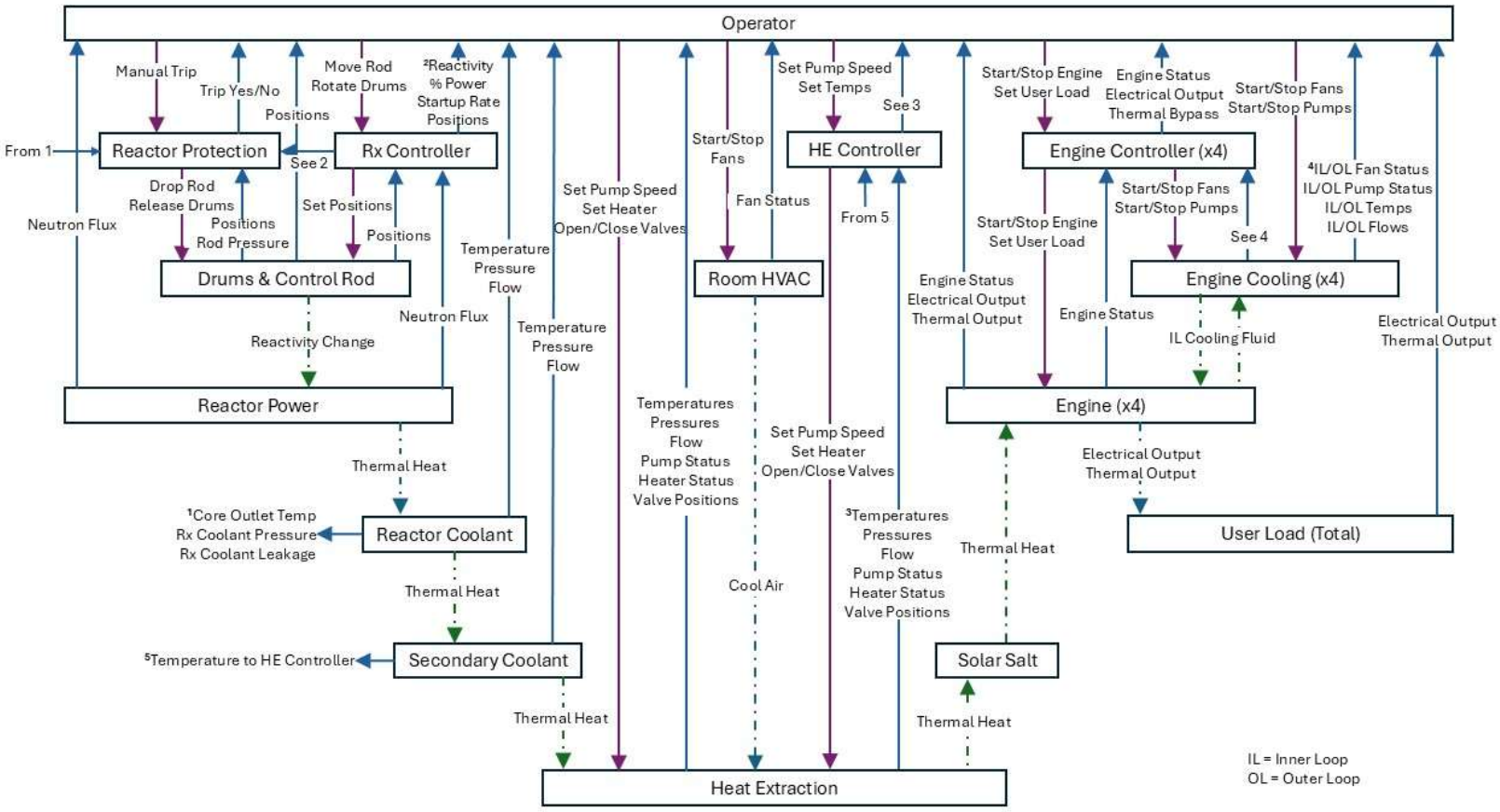
High-Level Baseline Architecture



LLM-Assisted STPA



LLM-Assisted STPA



LLM-Assisted STPA

STPA Microreactor Analysis

Heat Pipe Microreactor Database

AI Generate All (Hazards + UCAs + Scenarios)

Step 1: Define Purpose | Step 2: Control Structure | Step 3: UCAs | Step 4: Loss Scenarios

Step 1: Define Analysis Purpose

Losses

+ Add Loss | Delete All

ID	Description	Actions
L-1	Radiation Release	Edit Delete
L-2	Mission Loss (loss of electrical generation)	Edit Delete

Hazards

+ Add Hazard | AI Generate Hazards | Delete All

ID	Description	Related Losses	Actions
H-1	Reactor exceeds maximum allowable power level	L-1, L-2	Edit Delete
H-2	Reactor power oscillations exceed stability limits	L-1, L-2	Edit Delete

STPA Microreactor Analysis

Heat Pipe Microreactor Database

AI Generate All (Hazards + UCAs + Scenarios)

Step 1: Define Purpose | Step 2: Control Structure | Step 3: UCAs | Step 4: Loss Scenarios

Step 2: Identify Control Structure

CSV Import Instructions

Important: Import Controllers/Processes FIRST before importing Control Actions, Feedback, or Flow!
CSV files should have these columns:

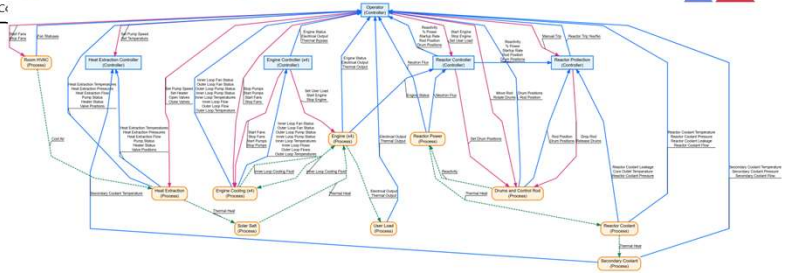
- **Controllers/Processes:** name, type, hierarchy_level, description
- **Control Actions:** action_name, source_id, destination_id, description
- **Feedback:** feedback_name, source_id, destination_id, description
- **Process Flow:** flow_name, source_id, destination_id, description

Note: source_id and destination_id must be valid integer IDs from the controllers_processes table

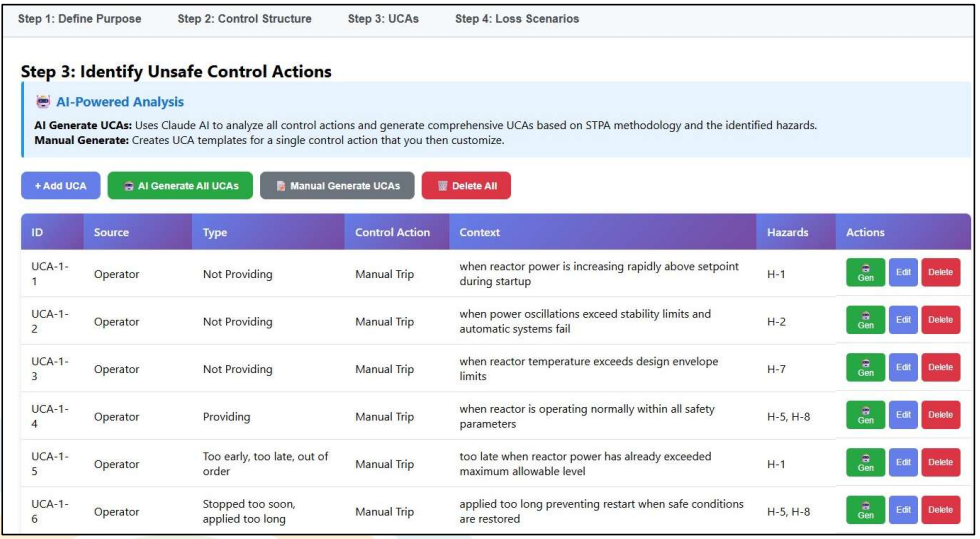
Controllers and Processes

+ Add Controller/Process | Import CSV | Choose File No file chosen | Export CSV | Delete All

Name	Type	Hierarchy Level	Description	Actions
Operator	Controller	1		Edit Delete
Engine Controller (x4)	Controller	2		Edit Delete
Heat Extraction C(				



LLM-Assisted STPA



Step 1: Define Purpose | Step 2: Control Structure | Step 3: UCAs | Step 4: Loss Scenarios

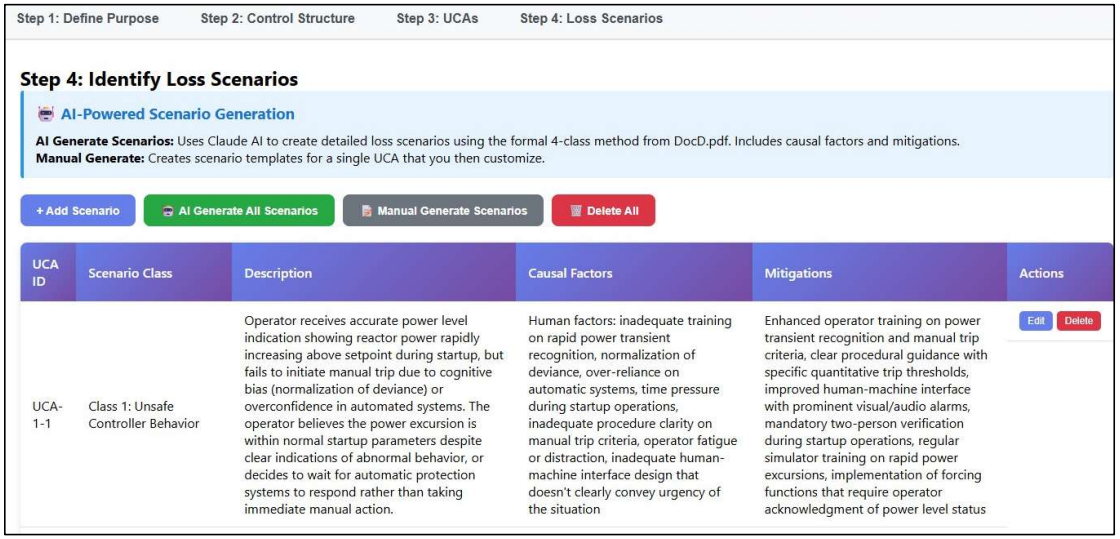
Step 3: Identify Unsafe Control Actions

AI-Powered Analysis

AI Generate UCAs: Uses Claude AI to analyze all control actions and generate comprehensive UCAs based on STPA methodology and the identified hazards.
Manual Generate: Creates UCA templates for a single control action that you then customize.

+ Add UCA | AI Generate All UCAs | Manual Generate UCAs | Delete All

ID	Source	Type	Control Action	Context	Hazards	Actions
UCA-1-1	Operator	Not Providing	Manual Trip	when reactor power is increasing rapidly above setpoint during startup	H-1	Gen Edit Delete
UCA-1-2	Operator	Not Providing	Manual Trip	when power oscillations exceed stability limits and automatic systems fail	H-2	Gen Edit Delete
UCA-1-3	Operator	Not Providing	Manual Trip	when reactor temperature exceeds design envelope limits	H-7	Gen Edit Delete
UCA-1-4	Operator	Providing	Manual Trip	when reactor is operating normally within all safety parameters	H-5, H-8	Gen Edit Delete
UCA-1-5	Operator	Too early, too late, out of order	Manual Trip	too late when reactor power has already exceeded maximum allowable level	H-1	Gen Edit Delete
UCA-1-6	Operator	Stopped too soon, applied too long	Manual Trip	applied too long preventing restart when safe conditions are restored	H-5, H-8	Gen Edit Delete



Step 1: Define Purpose | Step 2: Control Structure | Step 3: UCAs | Step 4: Loss Scenarios

Step 4: Identify Loss Scenarios

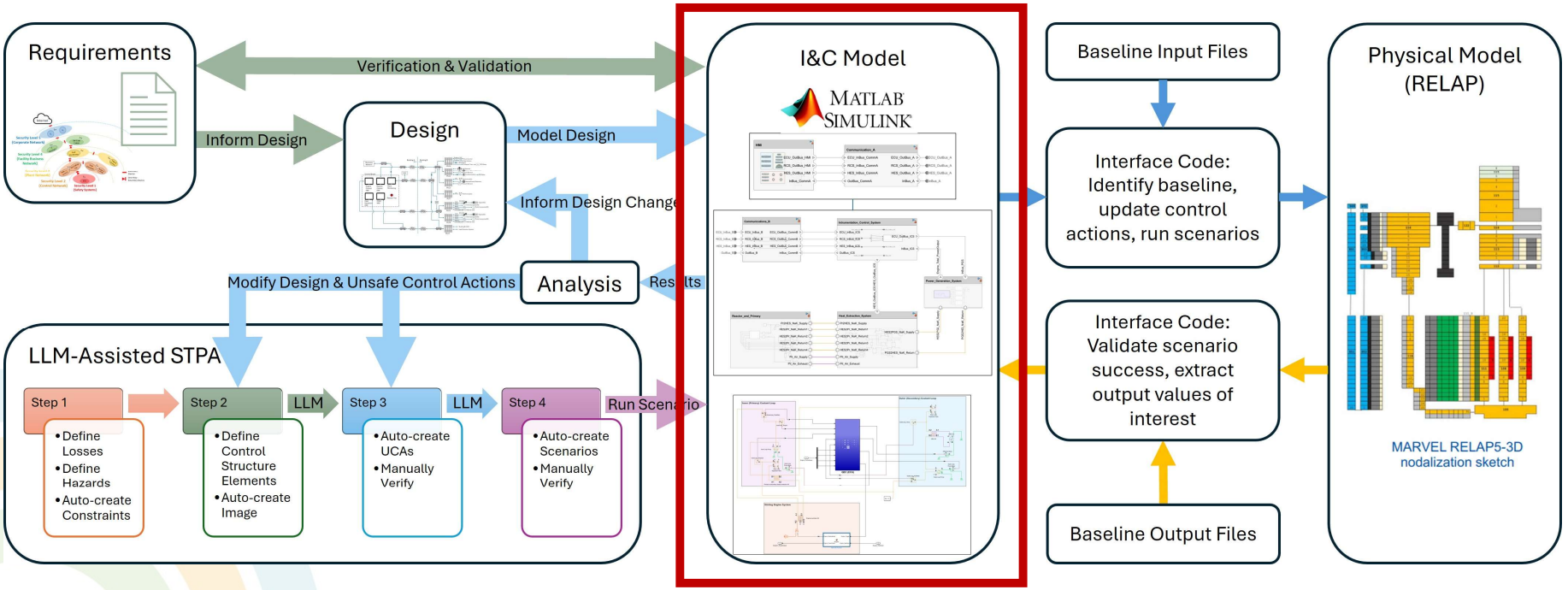
AI-Powered Scenario Generation

AI Generate Scenarios: Uses Claude AI to create detailed loss scenarios using the formal 4-class method from DocD.pdf. Includes causal factors and mitigations.
Manual Generate: Creates scenario templates for a single UCA that you then customize.

+ Add Scenario | AI Generate All Scenarios | Manual Generate Scenarios | Delete All

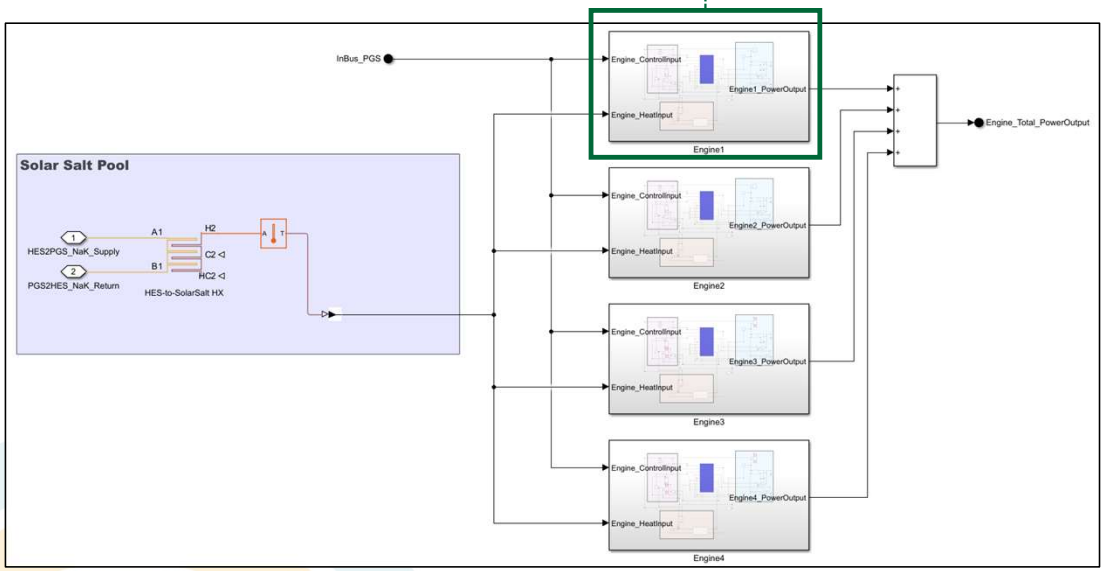
UCA ID	Scenario Class	Description	Causal Factors	Mitigations	Actions
UCA-1-1	Class 1: Unsafe Controller Behavior	Operator receives accurate power level indication showing reactor power rapidly increasing above setpoint during startup, but fails to initiate manual trip due to cognitive bias (normalization of deviance) or overconfidence in automated systems. The operator believes the power excursion is within normal startup parameters despite clear indications of abnormal behavior, or decides to wait for automatic protection systems to respond rather than taking immediate manual action.	Human factors: inadequate training on rapid power transient recognition, normalization of deviance, over-reliance on automatic systems, time pressure during startup operations, inadequate procedure clarity on manual trip criteria, operator fatigue or distraction, inadequate human-machine interface design that doesn't clearly convey urgency of the situation	Enhanced operator training on power transient recognition and manual trip criteria, clear procedural guidance with specific quantitative trip thresholds, improved human-machine interface with prominent visual/audio alarms, mandatory two-person verification during startup operations, regular simulator training on rapid power excursions, implementation of forcing functions that require operator acknowledgment of power level status	Edit Delete

I&C Model

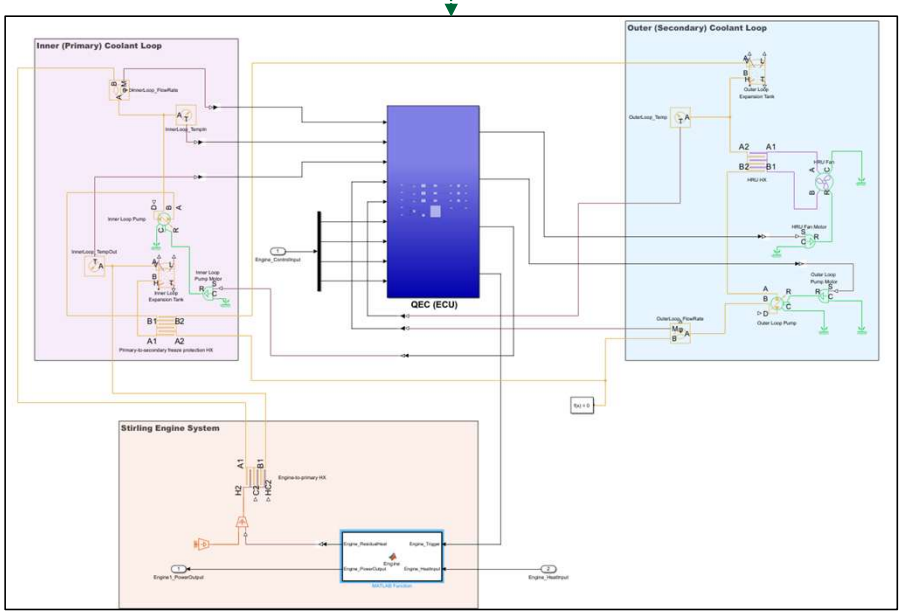

Requirements
Verification & Validation
Inform Design
Design
Model Design
Inform Design Change
Analysis
Modify Design & Unsafe Control Actions
LLM-Assisted STPA
Step 1
•Define Losses
•Define Hazards
•Auto-create Constraints
Step 2
•Define Control Structure Elements
•Auto-create Image
LLM
Step 3
•Auto-create UCAs
•Manually Verify
LLM
Step 4
•Auto-create Scenarios
•Manually Verify
Run Scenario
I&C Model
MATLAB SIMULINK
Baseline Input Files
Interface Code: Identify baseline, update control actions, run scenarios
Interface Code: Validate scenario success, extract output values of interest
Baseline Output Files
Physical Model (RELAP)
MARVEL RELAP5-3D nodalization sketch

System Composer

Simulink

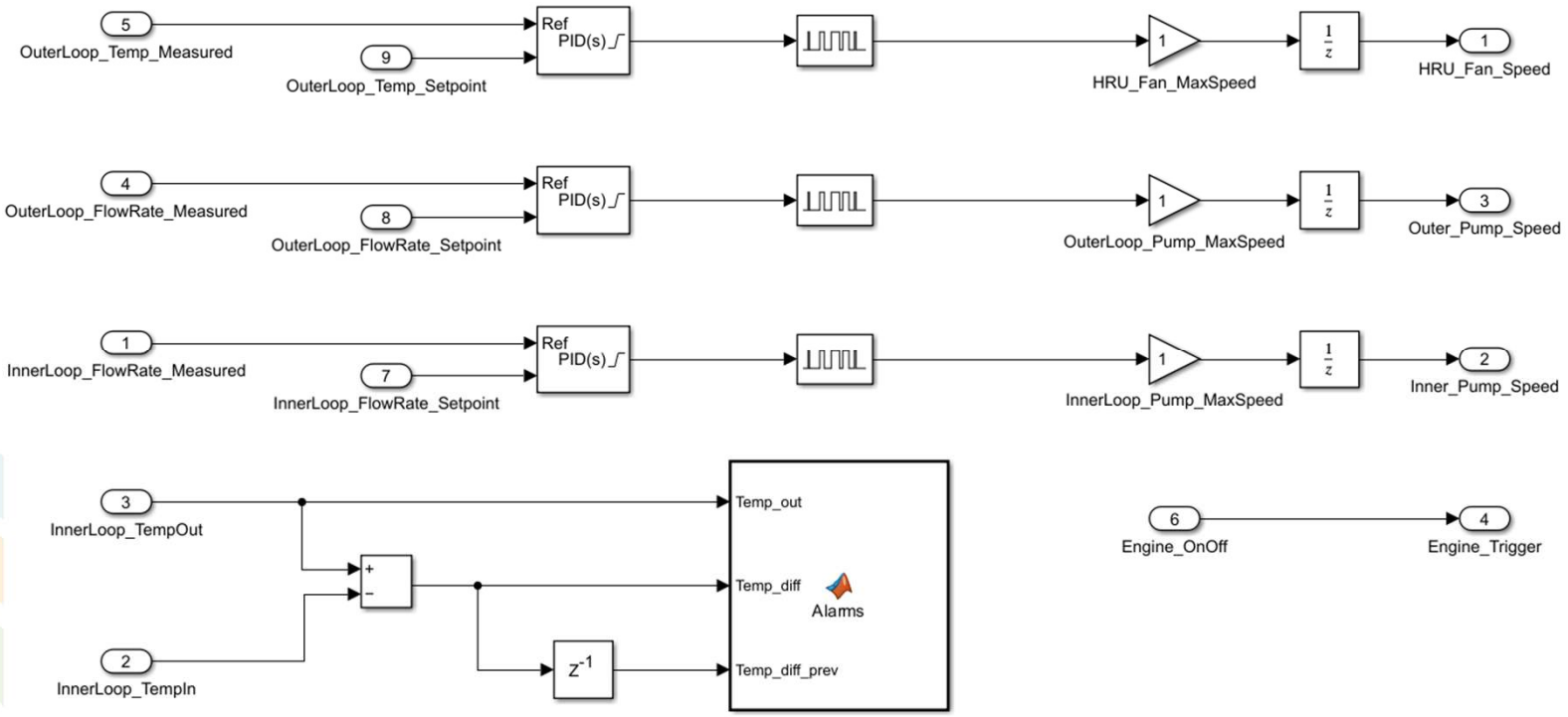


Power generation system with 4 engines

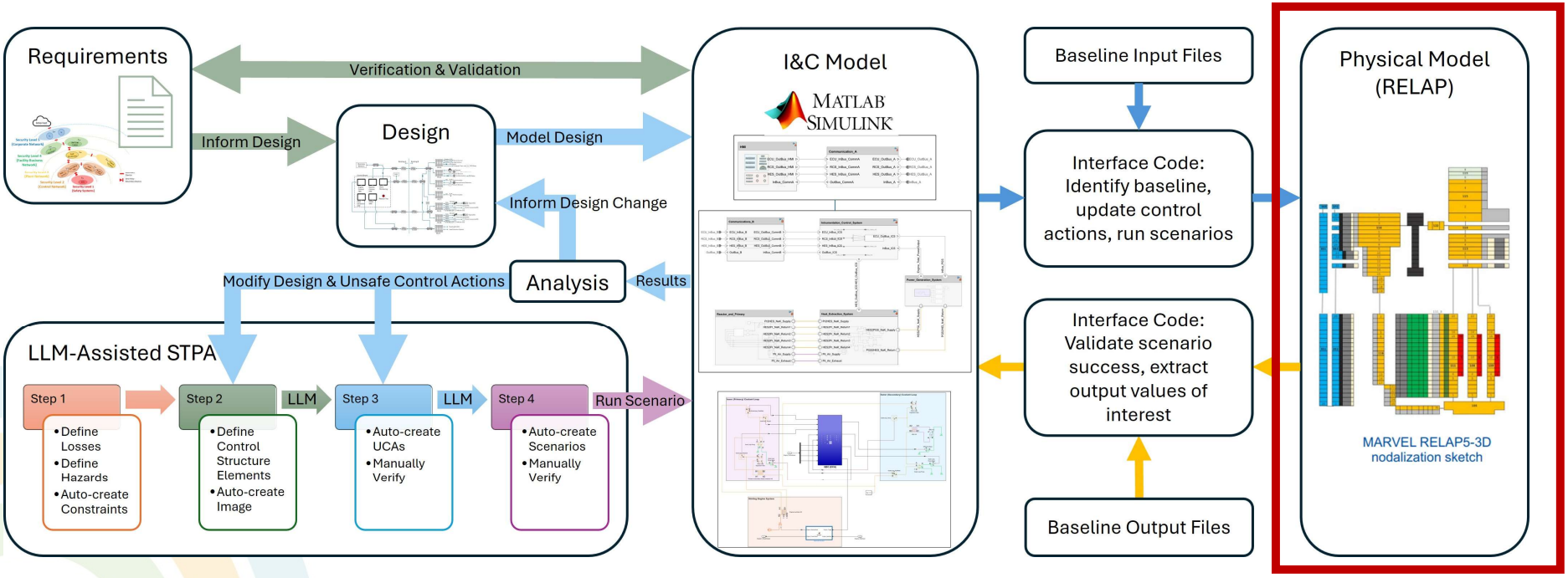


Individual engine model

Control Logic for the engine control system



Physical Model



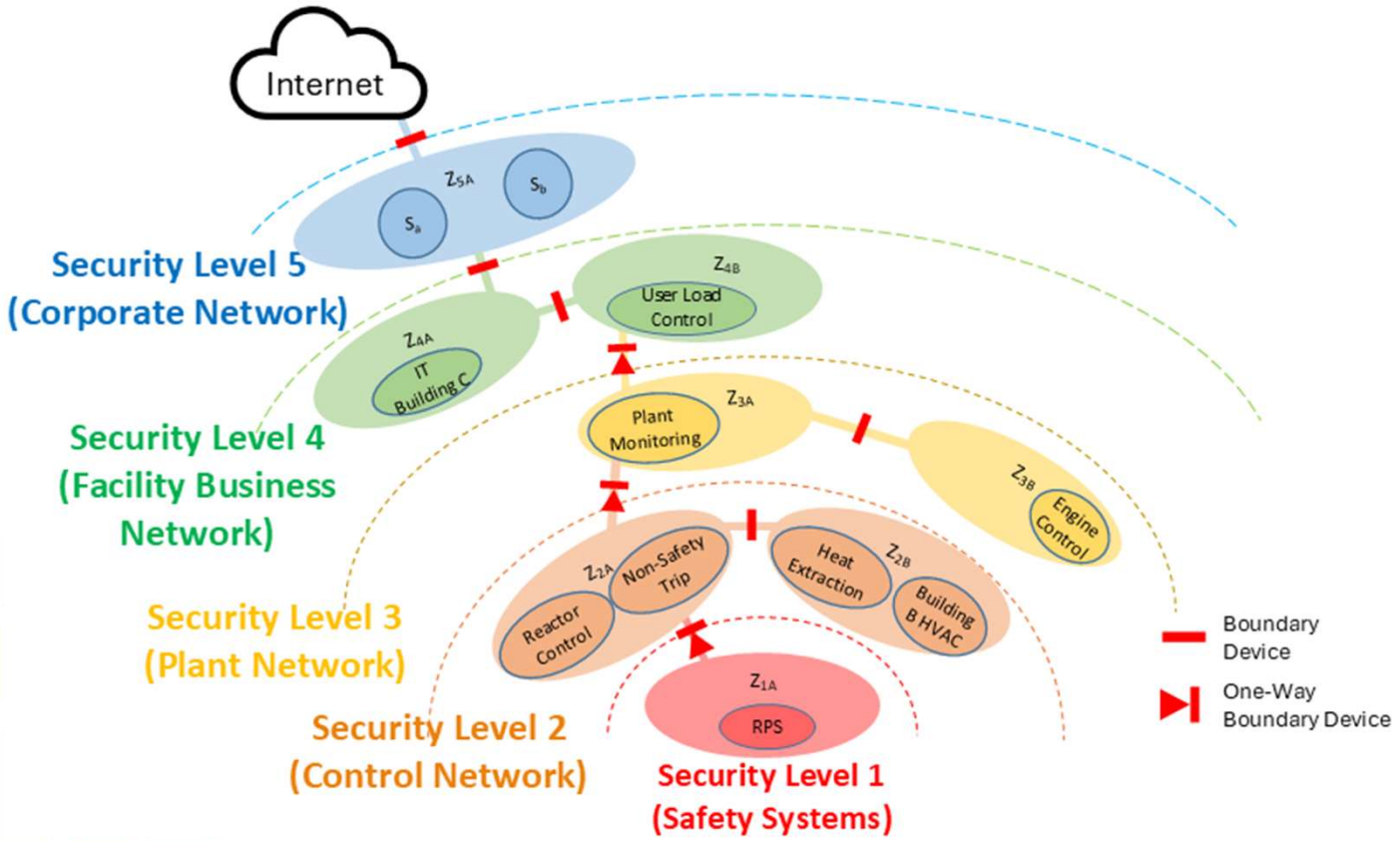
RELAP5-3D


Perturbed Control Action
Updated RELAP Model
Execute RELAP on HPC
Updated RELAP Results
Change in System Response
Existing RELAP Safety Model
Baseline RELAP Results

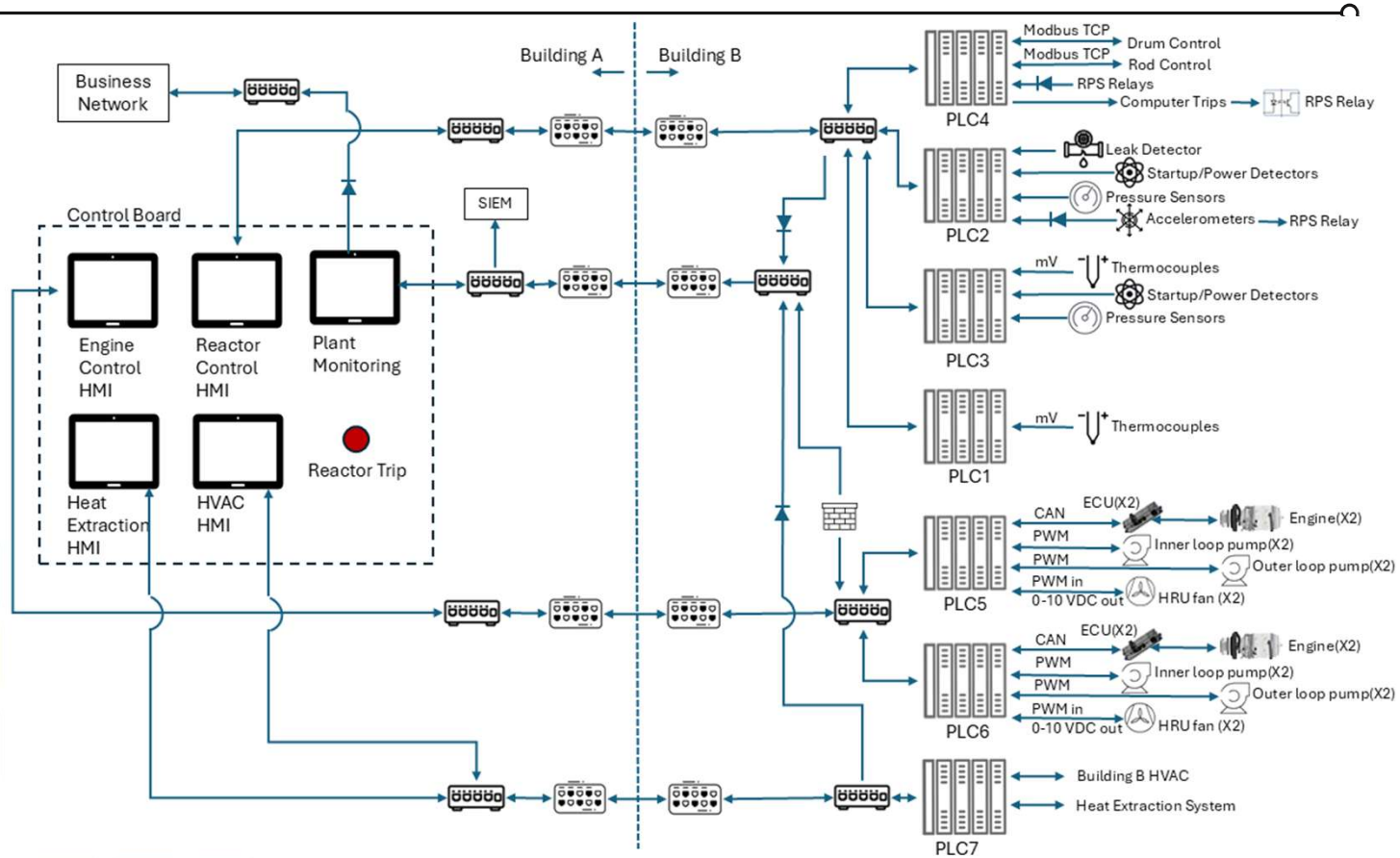
Example of UCA Reduction

Redesigns of the Network Architecture

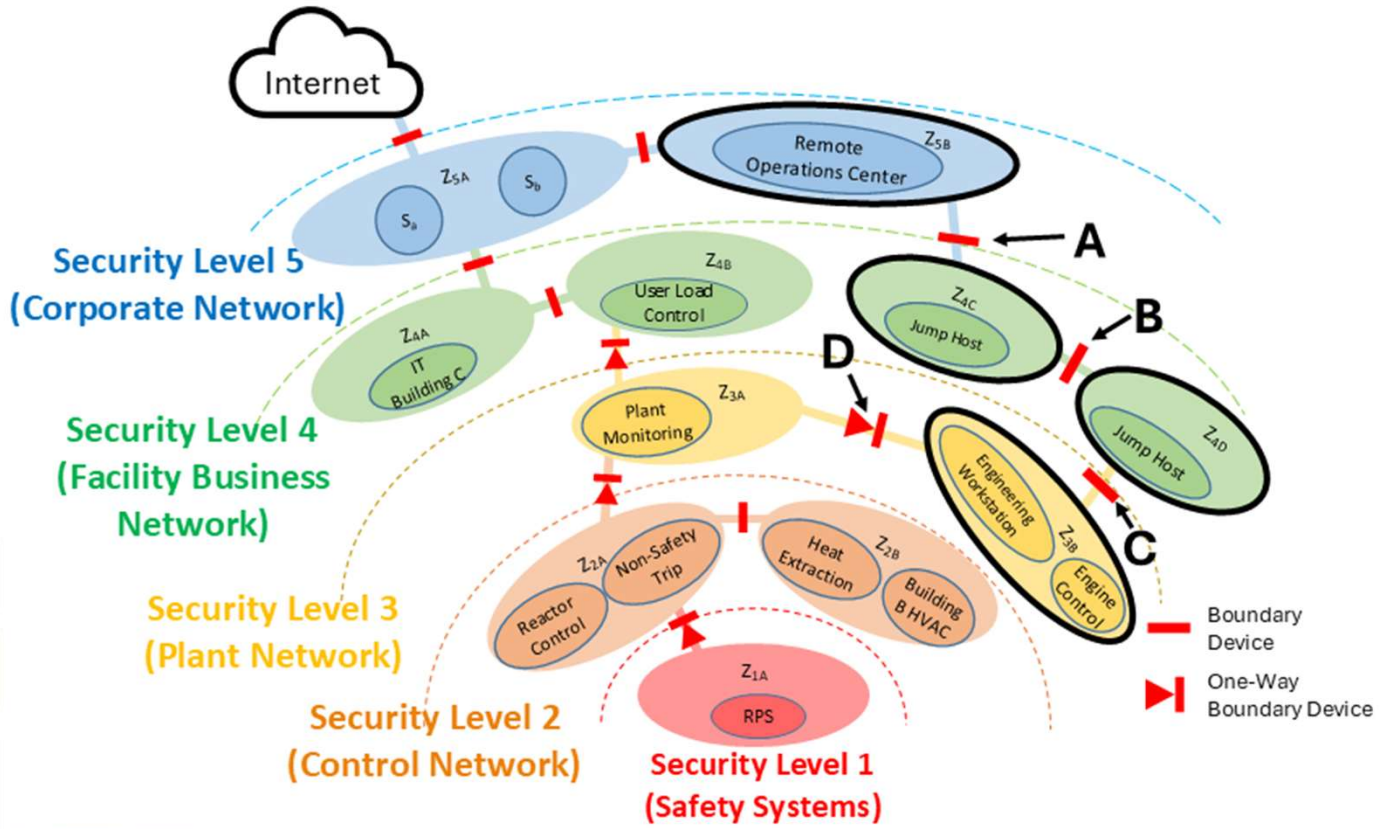
Defensive Cybersecurity Architecture (DCSA)



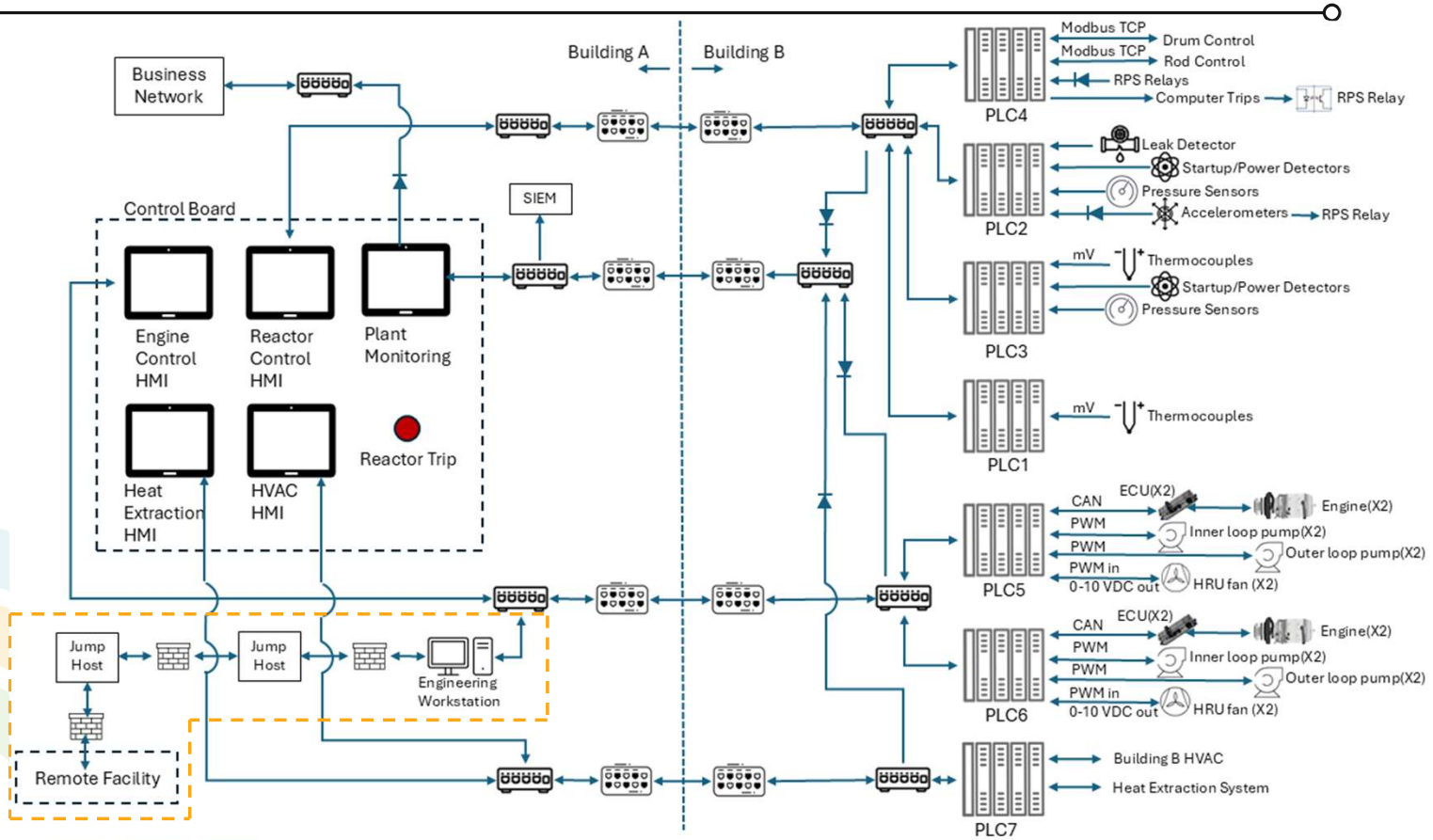
High-Level DCSA



Remote Architecture DCSA



High-Level Remote Operations DCSA



Ongoing & Future Work

- Streamline the LLM-based STPA application, including prompts.
- Improve integration with STPA and Simulink model.
- Finalize integration of RELAP and Simulink model.
- Enhance semi-automation of STPA application and design considerations.
- Evaluate enhancements to RELAP component, including agentic workflow.
- Utilize Model Context Protocol (MCP) servers for MBE tool interface with STPA application.
- Formalize the interfaces and modularity for reactor-agnostic analysis of system design.

FY26 Conference Papers

- IAEA CyberCon26 (Accepted)
  - Cybersecurity by design using a model-based engineering ecosystem
- ANS Annual Conference (Accepted)
  - Evaluating Large Language Models for Semi-Automated Systems Theoretic Process Analysis of a Microreactor
  - Designing a Remote Operations Network Architecture for a Microreactor
- INMM Annual Meeting
  - Model-Based Engineering for Safety and Security Analysis of a Microreactor
  - Assessment of Microreactor Control Architecture Leveraging Existing Models
- ANS Global Conference (Accepted)
  - Model-Based Engineering: A Process for Integrating Safety and Cybersecurity during Design

Questions