ADVANCED REACTOR SAFEGUARDS & SECURITY

Risk-Informed Consequence-Driven Hybrid Cyber-Physical Protection System Security Optimization for Advanced Reactor Sites

PRESENTED BY

Shaheen Azim Dewji, Ph.D.

May 14-16, 2024

Info Release #1744859

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.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Motivation – Risk Informed + Consequence Driven

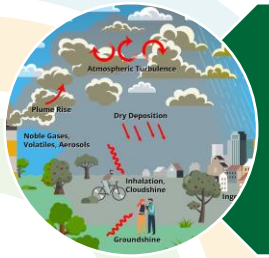
- **Relevant NRC Policy and Regulations**
  - NRC 10 CFR 73 – Physical Protection of Plants and Materials
    - 73.54: Cyber related protections
    - 73.55: Physical protections (PPS)
  - NRC 10 CFR 52 - "Licenses, Certifications, and Approvals for Nuclear Power Plants"
- **DOE and NRC Goals**
  - NEIMA section 103(a)(4)
  - *Proposed* NRC 10 CFR 53 - "Risk-Informed, Technology-Inclusive Regulatory Framework for Commercial Nuclear Plants"
    - 2 framework options (A, B)
    - Posed to allow more freedom to AR designers when seeking licensing and approval

SECY-23-0021: *PROPOSED RULE: RISK-INFORMED, TECHNOLOGY-INCLUSIVE REGULATORY FRAMEWORK FOR ADVANCED REACTORS*

Project Objectives

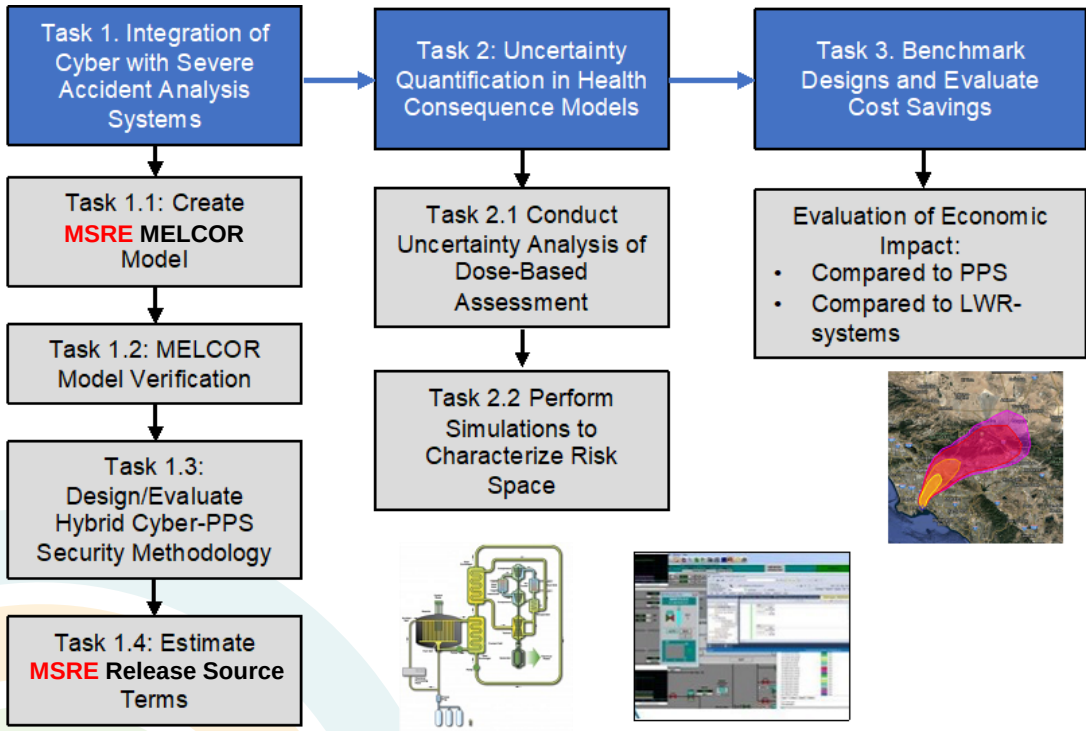
Objective 1: Assess fundamental systems-level correlations between sabotage-based security events in the traditional PPS-security space and sabotage-based security events with the new hybrid cyber-PPS space to integrate cybersecurity risk-informed reactor sabotage consequence analysis into traditional PPS design methodology.

Objective 2: Demonstrate the new risk-informed approach on a molten salt reactor (MSR) concept using enhancements to state-of-the-art severe accident and consequence analysis computer codes, with expanded uncertainty analyses to satisfy licensing requirements under proposed language of 10 CFR 53.



Objective 3: Pursue a cost-savings evaluation for licensing and operating lifetime by benchmarking against the current policy-driven reactor PPS requirements as specified by 10 CFR 73 for the same notional site layout.

Schedule and Current Progress



YEAR	Y1				Y2				Y3			
TASK	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Task 1.1 MELCOR MSRE input												
Task 1.2 Verification												
Task 1.3 Hybrid cyber-PPS												
Task 1.4 Source-term model												
Task 2.1 Dose uncertainty												
Task 2.2 Risk quantification												
Task 3 Economic assessment												

Team Capabilities

Shaheen Dewji (PI)
Jarred Jordan, Martin Graffigna
- Atmospheric dispersion modeling; dose assessment; dose coefficient development for new radionuclide chemical forms

Fan Zhang (Co-PI)
Stephen Yoo
- Cybersecurity; predictive maintenance; autonomous control; robotics research

Karen Vierow Kirkland (Co-PI)
TAMU Student (TBD)
- Reactor thermohydraulics, reactor accident progression analysis, MELCOR validation, PRA/PSA UQ for ARs

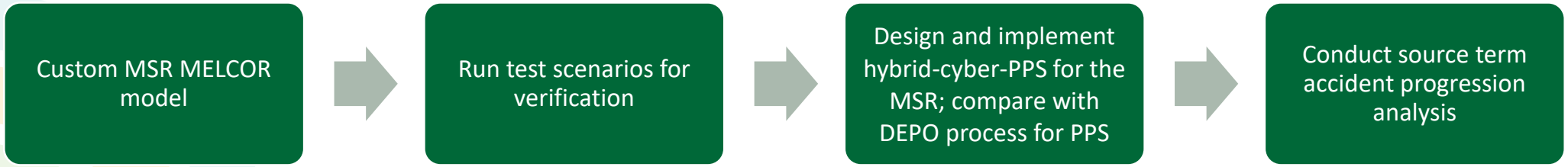
Chris Faucett (Lead Collaborator)
Severe accident modeling and analysis; MELCOR modeling; integrated security/safety advanced reactor vulnerability analyses; safeguards/proliferation resistance

Michael Rowland (Collaborator)
Advanced Reactors; supply chain; cyber security operations center; blended attack exercises

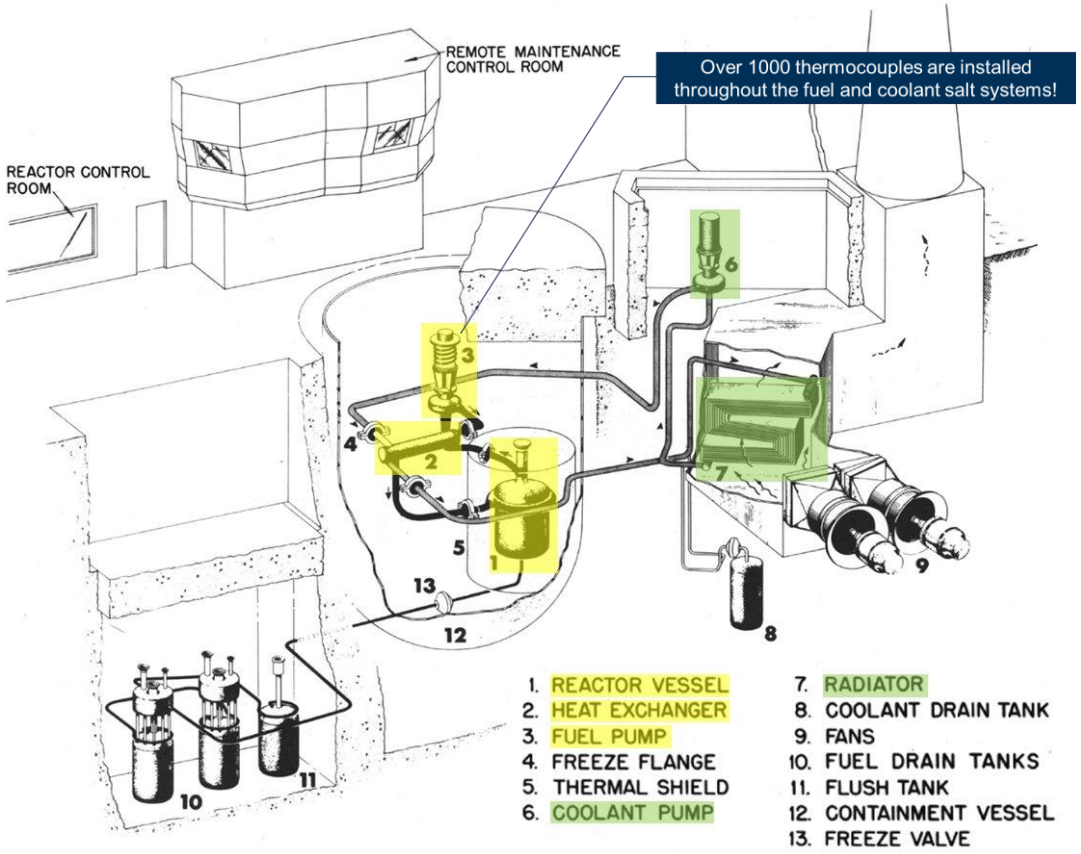
John Fulton (Collaborator)
Jay Dharsandia
Atmospheric transport and consequence; MACCS program development

Task 1 Breakdown

- **Cyber security hardware modeling integration into severe accident analysis**
  - User-specified control functions in MELCOR
  - Dividing control volumes such that conditions around sensors can be accurately assessed
  - Hazard identification via HAZCADS
- **Simulate attacks on the control system**
  - Directly changing mechanical operation
    - LWR ex: Reducing pump speed, modifying system temperature and pressure parameters, etc.
  - False system parameter data from sensors



MSRE General



- Primary system
- Secondary system

- Radiator: Heat is transferred from coolant salt to air
- Drain-tank system: Containing the fuel and coolant salts when the circulating systems are not in operation

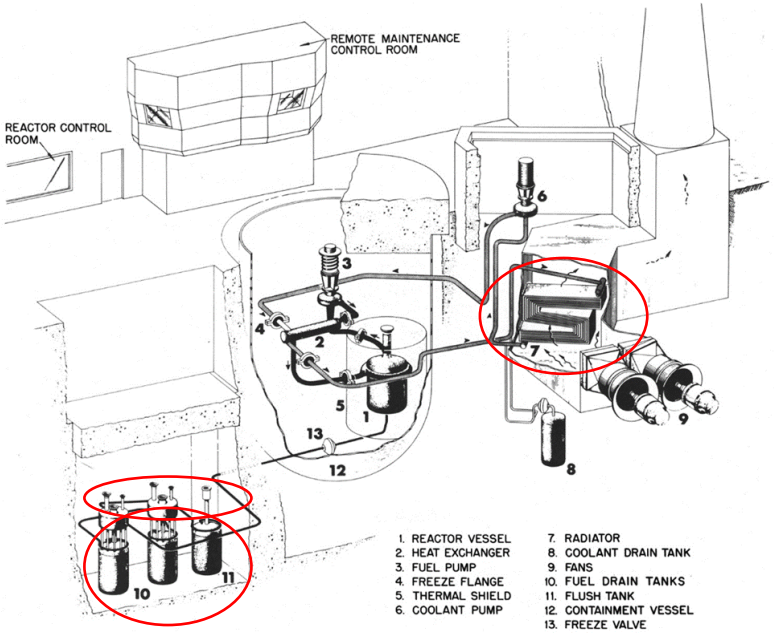
- "Digital computer and data handling equipment are included in the instrumentation. This equipment has no control function."

ORNL-TM-728, MSRE Design and Operations Report, Part I, Description of Reactor Design

MSRE I&C Systems

- Control rods and rod drives
- Safety instrumentations
  - Nuclear safety system
  - Temperature instrumentation for safety system inputs
  - Radiator door emergency closure system
  - Reactor fill and drain system
  - Helium pressure measurements in the fuel salt loop
  - Afterheat removal system
  - Containment system instrumentation
  - Health-physics radiation monitoring
- Control instrumentations
  - Nuclear instrumentation
  - Plant control
- Electrical power system

Distinguished differences compared to conventional NPPs



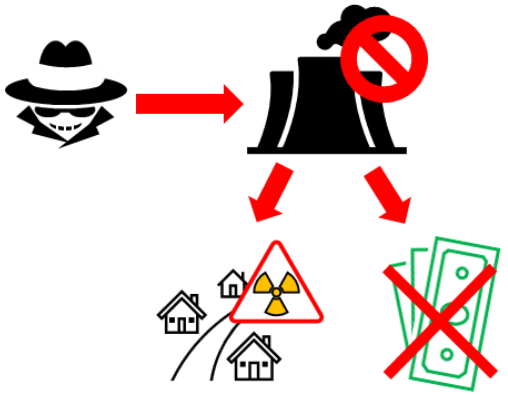
ORNL-TM-732, MSRE Design and Operations Report, Part V, Reactor Safety Analysis Report

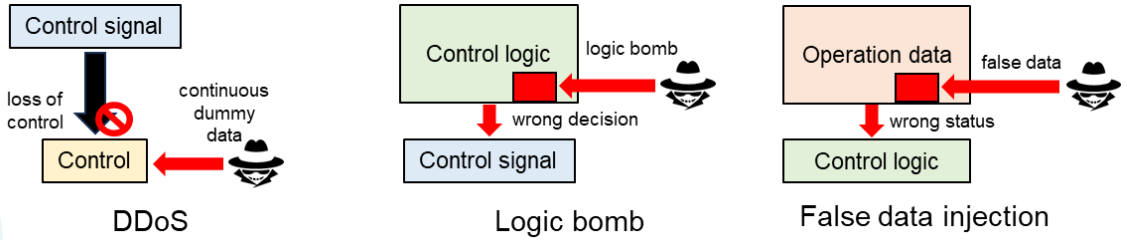
MELCOR

- Current progress
  - Gaining access to code
  - Examining MSRE systems to be implemented within MELCOR
- Upcoming progress
  - Implementation of MSRE within MELCOR
  - Application of both cyber-physical systems
- Investigate methods for cyberattack inclusion
  - Control functions

Cyber-Attacks

- Potential Attacker Goals
  - Make the system abnormal
  - (If possible) deal physical damage to the system
    -> Economic loss, hazards
- How can they achieve that potential goal?
  - Disable controls (Distributed Denial of Service, DDoS)
  - Modify logic (Logic Bombs)
  - Manipulate data/controls (False data injection attack)





MSRE Initial Accident Scenarios

- Nuclear Incidents
  - Uncontrolled rod withdrawal
  - "Cold-slug" accident
  - Filling accidents
  - Fuel additions
  - UO_2 precipitation
  - Graphite loss or permeation
  - Loss of flow
  - Loss of load
  - Afterheat
  - Criticality in the drain tanks

Distinguished

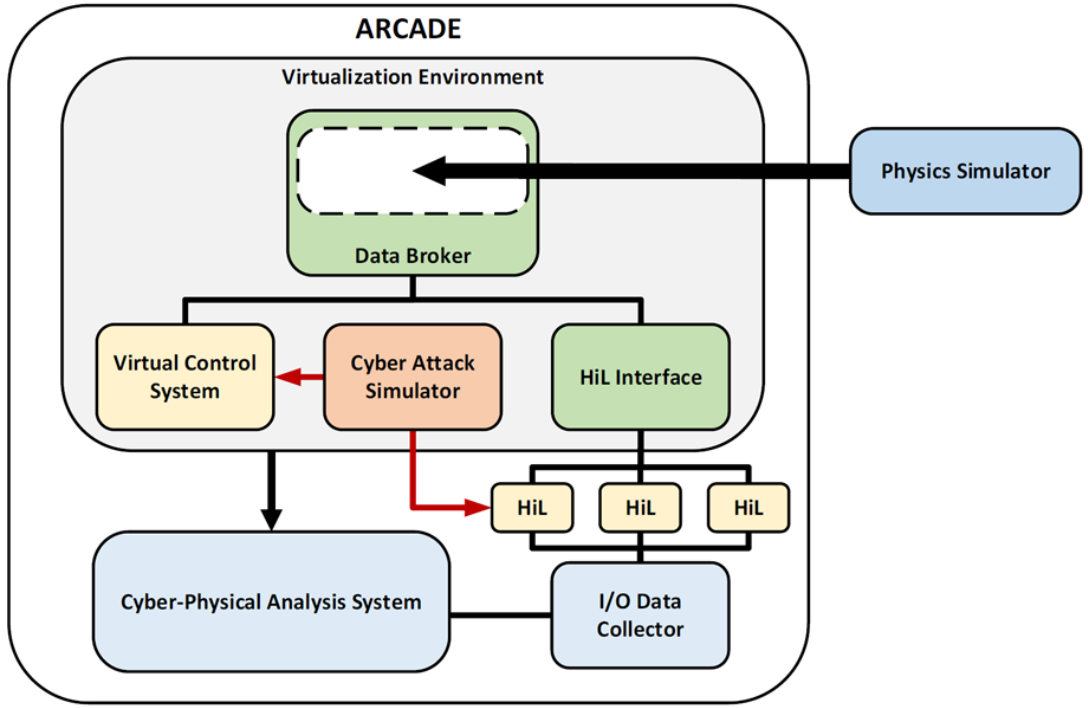
- Non-Nuclear Incidents
  - Freeze-valve failure
  - Freeze-flange failure
  - Excessive wall temperatures and stresses
  - Corrosion
  - Material surveillance testing
  - Detection of salt spillage
- Other
  - Secondary container damage
  - Acts of nature

Candidates

Most probable!

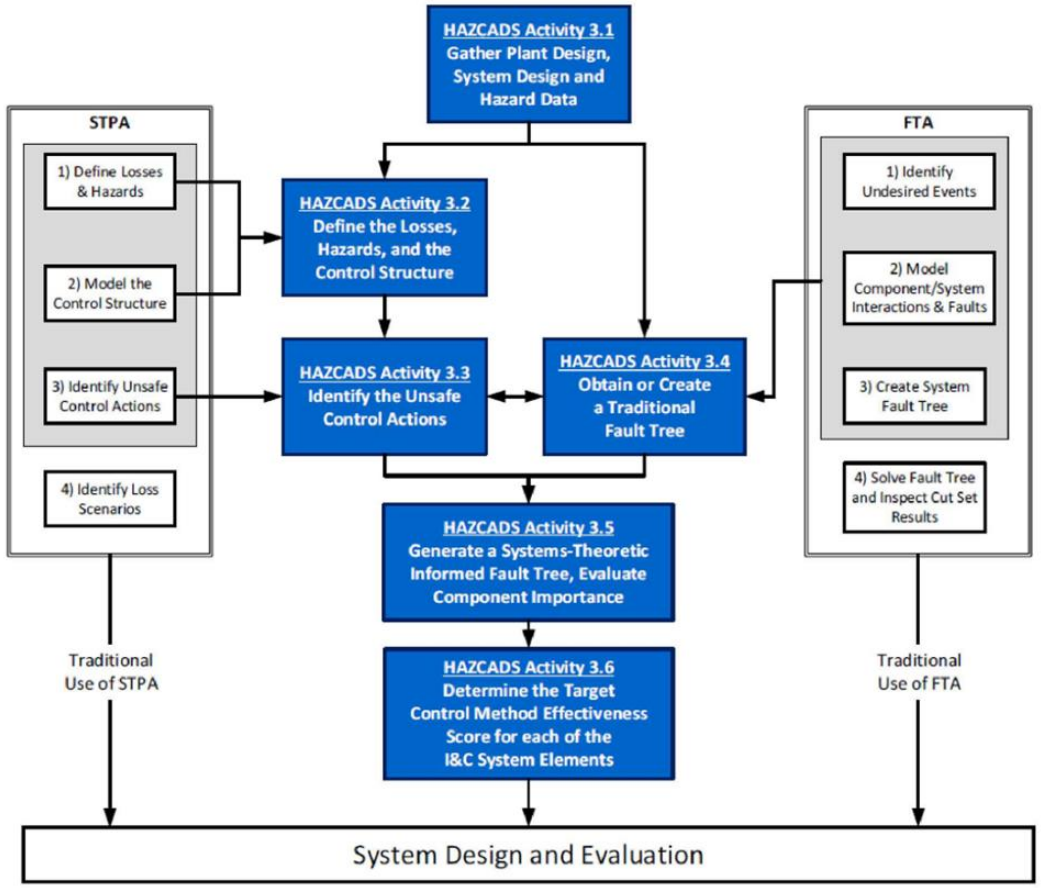
ARCADE - MELCOR

- Minimega
  - Virtual machine (VM) running tool
  - Runs various systems for ARCADE
- ARCADE
  - Physics simulator: Asherah
  - Virtualization environment
    - Data broker: Connects physics simulator to distributed control system
    - Hardware-in-the-loop (HiL): Solution for machines that cannot be emulated



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.

HAZCADS



- Combination of STPA & FTA
  - STPA
    - Control-focus
    - Identification of unsafe control actions
  - FTA
    - Device-focus
    - Component/system interactions and faults
- Characteristics
  - Traceability: explain a range of hazards with different potential consequences
  - Flexibility: being able to formally optimize analytical results for a selected set of undesired losses

HAZCADS: Hazards and Consequences Analysis for Digital Systems. EPRI, Palo Alto, CA: 2018. 3002012755.

Scenario Development

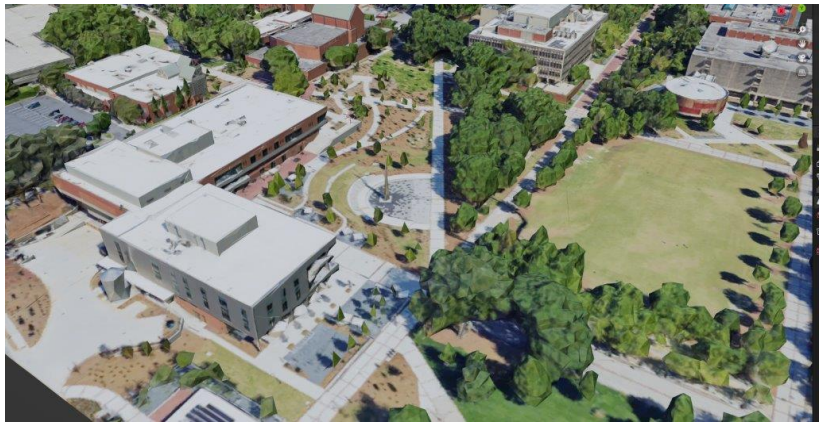
- Physical Scenarios
  - Verification/Validation of security methodology
  - Conventional scenarios + MSRE-specific scenarios
- Cyber Scenarios
  - DDoS attack & false data injection attack scenarios
  - Digital I&C systems in MSRE
- ARCADE: Testbed
- HAZCADS
  - Development of scenarios
  - Classification of physical/cyber scenarios

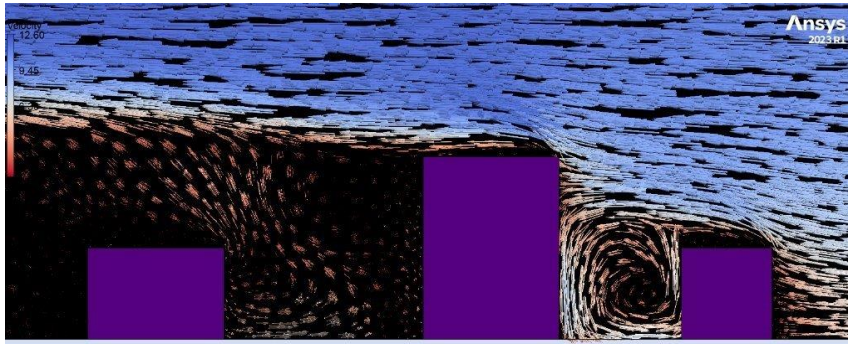
Task 2 Breakdown

- **Expanded dose-based health consequence models for siting boundaries with uncertainty analysis**
  - Define dose coefficients for new AR MSR sources
  - Updated age-specific dose coefficients beyond ICRP 60 (adult male)
  - Compare to requirements within 10 CFR 50.34 & 10 CFR 52.79
- **Risk-informed consequence analysis**
  - Atmospheric Transport, Internal dose particle size/chemical form transformation
    - Optimize simulation of plume behavior for urban centers
    - MACCS, HYSPLIT, custom simulation and behavior modeling (CFD for nearfield)
- **Determine the highest contributors of risk to the public's health and safety**
  - DEPO + HAZCADS (bounding risk-informed scenarios) → MELCOR (source term) → MACCS (dose/risk-consequence)← FGR 16 (risk-consequence)

Particle Transport Simulations

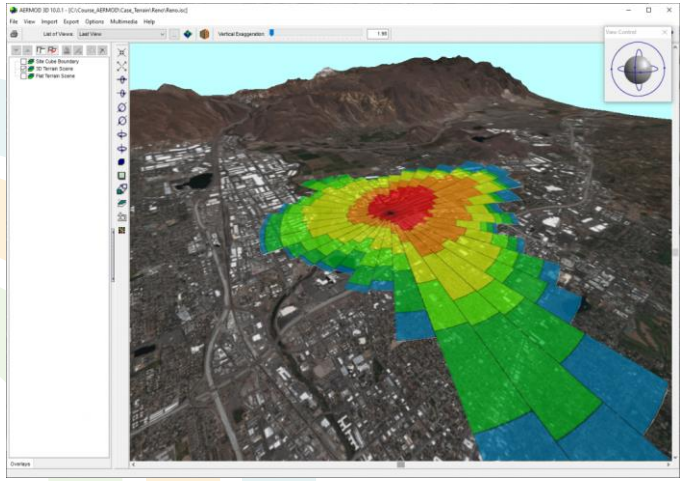
- CFD drawbacks
  - Long-distance particle transport is not ideal for standalone CFD programs
  - Low customizability
    - Difficult implementation of alternative release materials
    - Meshing inconsistencies and software instability
      - Numerous attempts to retrieve a usable mesh from 3D data
  - Implementation of weather data
    - Weather data is a low resolution for expected results
  - Custom CFD development
    - Advanced knowledge needed
    - CFD-AI hybrid techniques (e.g. PINN)

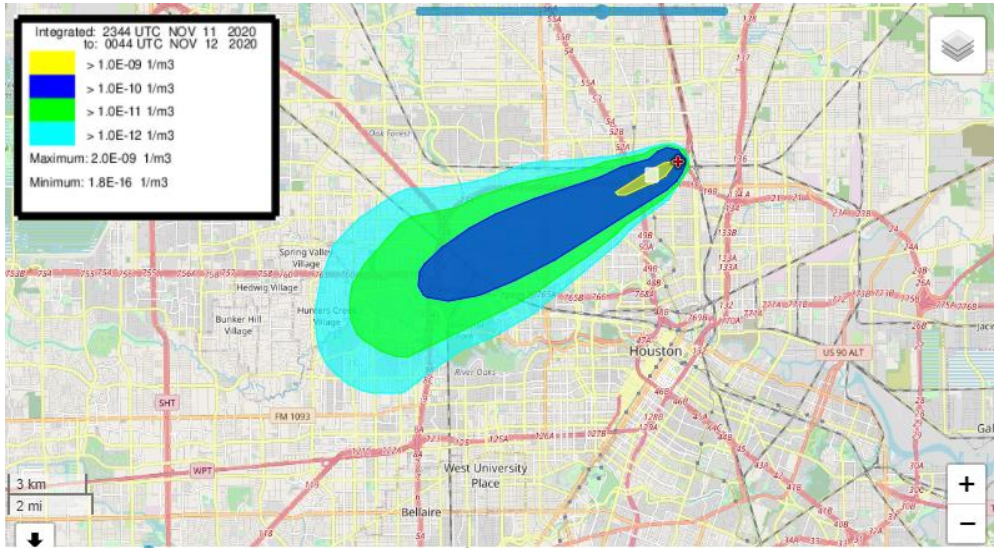




Path Forward

- Established accident modelling software
  - AERMOD
    - Written in FORTRAN
  - MACCS/HYSPLIT
    - Build off software knowledge gained from previous NEUP project



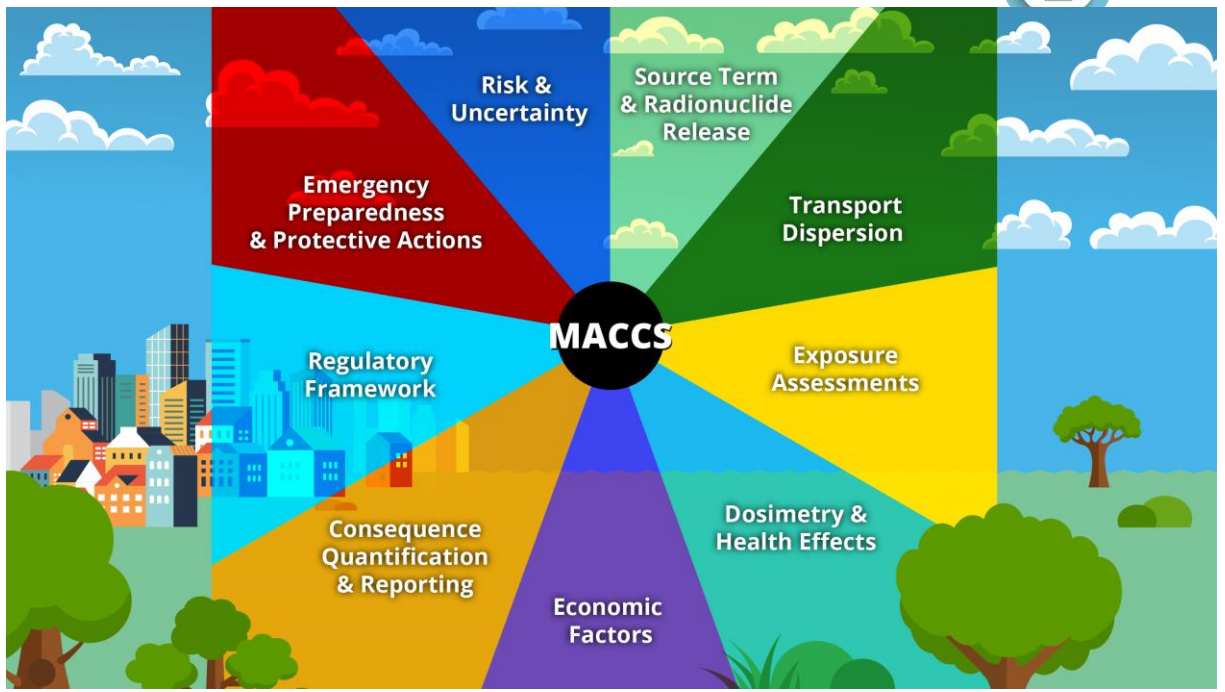


Required Information

- Largely reliant on information from source terms and transport simulations
  - Large focus on the near-field effects
- Consequences
- Turbo FRMAC and MACCS.
- Risk of early fatalities and injuries
  - MACCS
- Risk of latent cancer fatalities
  - MACCS and REDCAL

Task 3: Benchmark Designs and Evaluate Cost Savings

- Approach:
- Benchmark, evaluation, and estimation of cost impact/savings compared to traditional LWR methodology
  - Risk-informed PPS design for LWRs vs hybrid cyber-PPS methodology for MSRs
- Broader economic impacts will be investigated in MACCS
  - Close proximity of ARs to urban population centers must be considered
  - Comparative health and cost-based risk metric (J-value [Waddington et al. 2017] vs. GDP in MACCS)



maccs.sandia.gov

Impact and Deliverables

- **(1)** New, optimized risk-informed methodology framework utilizing hybrid cyber-PPS design for AR licensing requirements
  - Expanded cyber-PPS module ← → MELCOR for use by the broader AR license community
  - Dose-driven consequence analysis for near-field siting using higher fidelity tools (CFD + HYSPLIT)
- **(2)** Multidisciplinary project scope
  - Cybersecurity, reactor modeling, consequence assessment, economics
- **(3)** Contribution to the research community
  - Training and support of graduate students and their research
    - Technical ability and soft skills
  - Submitting results and key findings to conferences and peer-reviewed journal publications

Upcoming Milestone Deadlines

Overall Project Outcomes:

- An enhanced methodology framework for a cyber-PPS informed design optimization that will reduce upfront and operational security costs;
- A framework for incorporating consequence analysis into cyber-security regulations required by new regulatory licensing language;
- A means to define the level of risk for MSRs, as a framework, which is based on an integrated analysis of security and safety effects;
- Uncertainty estimates and FOMs for health and economic consequence analyses from dose-based siting boundaries; and
- Training of graduate students combining PPS and cybersecurity, accident progression safety analysis, and consequence analysis.
- Deliverables will include:
  - A new, optimized risk-informed methodology framework utilizing hybrid cyber-PPS design for optimized AR licensing requirements;
  - An expanded module including cyber-PPS integration in MELCOR for use by the broader AR and licensing communities;
  - Quarterly progress and annual reports to the sponsor;

YEAR	Y1				Y2				Y3			
TASK	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Task 1.1 MELCOR MSRE input												
Task 1.2 Verification												
Task 1.3 Hybrid cyber-PPS												
Task 1.4 Source-term model												
Task 2.1 Dose uncertainty												
Task 2.2 Risk quantification												
Task 3 Economic assessment												