SAND2019-9283C

LWRS Physical Security Initiative

ANS UWC 2019
Amelia, FL
August 7, 2019

F. Mitch McCrory
LWRS Physical Security Initiative Lead
Sandia National Labs

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.

Why is LWRS focusing on Physical Security?

Physical security of nuclear power plants is an important aspect of maintaining a safe, secure, and reliable nuclear energy fleet. Physical security programs at US nuclear sites started to ramp up to meet changes in their design basis threat (DBT) in the early to mid-1980s. The events of September 11, 2001 saw more changes to the DBT and significant increases of physical security at nuclear power plant sites.

As the US nuclear power plants modernize their infrastructure and control systems to move past their original operating licenses, an opportunity exists to apply advanced tools, methods, and automation to modernize their physical security programs.

This initiative will leverage advances in modeling and simulation, sensor technologies, risk management tools, automation, and other technologic advances to provide the advance technical basis necessary to modernize and optimize physical security capabilities. This initiative will include efforts in the following areas:

LWRS LIGHT WATER REACTOR SUSTAINABILITY

New DOE-NE LWRS Physical Security Initiative (PSI) includes efforts in the following areas:

- R&D of **risk-informed techniques** for physical security to account for a dynamic adversary.
- R&D of **advanced modeling and simulation tools** to better inform physical security scenarios.
- **Assess benefits** from proposed enhancements, novel mitigation strategies, and potential changes to best practices, guides, or regulation.
- Enhance and **provide a technical basis** for stakeholders to employ new methods, tools, and technologies to achieve optimized physical security.

LWRS LIGHT WATER REACTOR SUSTAINABILITY

Collaborations

Industry Collaborations
Utilities • Two site visits planned/completed for first-hand review of various physical security postures • Other engagements in progress
NEI • Ongoing collaboration
NRC • Coordinating with NRC NSIR and RES on LWRS R&D plans
EPRI • Ongoing collaboration with EPRI
Owners Groups • Some limited engagement with future engagement planned at the Owners Group requests
Vendors • Some limited engagement with future engagement planned at the Owners Group requests

LWRS LIGHT WATER REACTOR SUSTAINABILITY

Collaborations

LWRS Industry Working Group
Provide a venue for LWRS to obtain feedback from industry, regulatory, vendor, supplier, and other stakeholders
Support development of the R&D program
Provide periodic input on plans and activities of the initiative
Support pilot projects through industry participation
Validate and provide feedback on specific methods, techniques, and technologies
Facilitate development and demonstration with vendors and suppliers as technologies are readied for commercial deployment and demonstration

Leverage NNSA and DOD R&D in this effort
Advanced M&S
Remote Weapons
Architectures

Focus Areas *(Work in Progress)*

Near-Term Efforts

Already Completed

- First of a kind Industry training on physical security systems (13 utilities, NEI, others)
- Review current security practices though nuclear site visits
- Engage with JCNRM and other standard's bodies to ensure R&D reflected where possible

This FY

- Modeling and Simulation input data to identify areas to remove unnecessary conservatisms, i.e., adversary time lines
- Physical Security Economic Model and Validation – to identify security cost drivers for evaluation in prioritizing research efforts
- Identify potential inefficiencies in security sensor maintenance and identify potential technical basis gaps that prevents increasing maintenance periodicity

FY20

- Initiate LWRS Physical Security Working Group
- Explore the technical basis necessary for implementation advanced security technology
    - Remote weapon systems

Focus Areas *(Work in Progress)*

3-5 Year Efforts*

- Risk Informing Physical Security – identifying conservatisms in physical security scenarios and perform the research necessary to create/document the technical basis to remove unnecessary conservatisms (Started in FY19)
    - Analyzing security narratives from start of security event through significant core damage – not all vital areas created equal
    - Explore barriers to utilization of FLEX equipment
    - Develop risk-informed methods that adequately address the human side of security
    - Explore barriers to credit operator action
        - Consequence mitigation
        - Explore required emergency procedure
        - Human reliability analysis in a security event
    - Other
- Regulatory Drivers – which regulatory drivers need technical basis R&D to remove unnecessary conservatisms

*Note that as research matures and is validated, it will be made available

Focus Areas *(Work in Progress)*

Long-Term Research

- Research into potential physical security architectures game changers
  - What does a PIDAS-less security architecture look like – is there a technical basis that could support this?
- Advanced Tiered Physical Security Architectures
- Other

Risk-Informed Nuclear Security

- Traditional Risk Equation:

$$\text{Risk} = \bigcup_{i=1}^{i=l}\{\langle p_i(\varphi_i), x_i\rangle\}$$

Where:

i = The i^{th} scenario category ($i = 1,\ldots,l$)
p_i = The joint distribution of the probability density function for the i^{th} scenario
φ_i = The frequency of the i^{th} scenario
x_i = The consequence or evaluation measure of the i^{th} scenario

- Security Risk Equation:

$$\text{Risk} = \bigcup_{i=1}^{i=l}\left\{\sum_{j=1}^{j=m}\langle T_i\left(v_{j,i}\right), x_{j,i}\rangle\right\}$$

Where:

i = The i^{th} scenario category ($i = 1,\ldots,l$)
j = The j^{th} target set ($j = 1,\ldots,m$); 1 = primary target
T_i = The threat for the i^{th} scenario
$v_{j,i}$ = The vulnerabilities of the i^{th} scenario for a j^{th} set of targets
$x_{j,i}$ = The consequence or evaluation measure of the i^{th} scenario for a j^{th} set of targets

Source: GAO analysis of the Department of Homeland Security information. | GAO-19-468

Integrated System Response Modeling

Goal: Develop modeling and simulations for existing plant security regimes using identified target sets to link dynamic assessment methodologies by leveraging nuclear power plant system level modeling with force-on-force modeling, and 3D visualization for developing table-top scenarios

Impact: Create an integrated force-on-force and nuclear power plant system response framework for a holistic approach in determining security related events as they relate to the potential for the onset of core damage

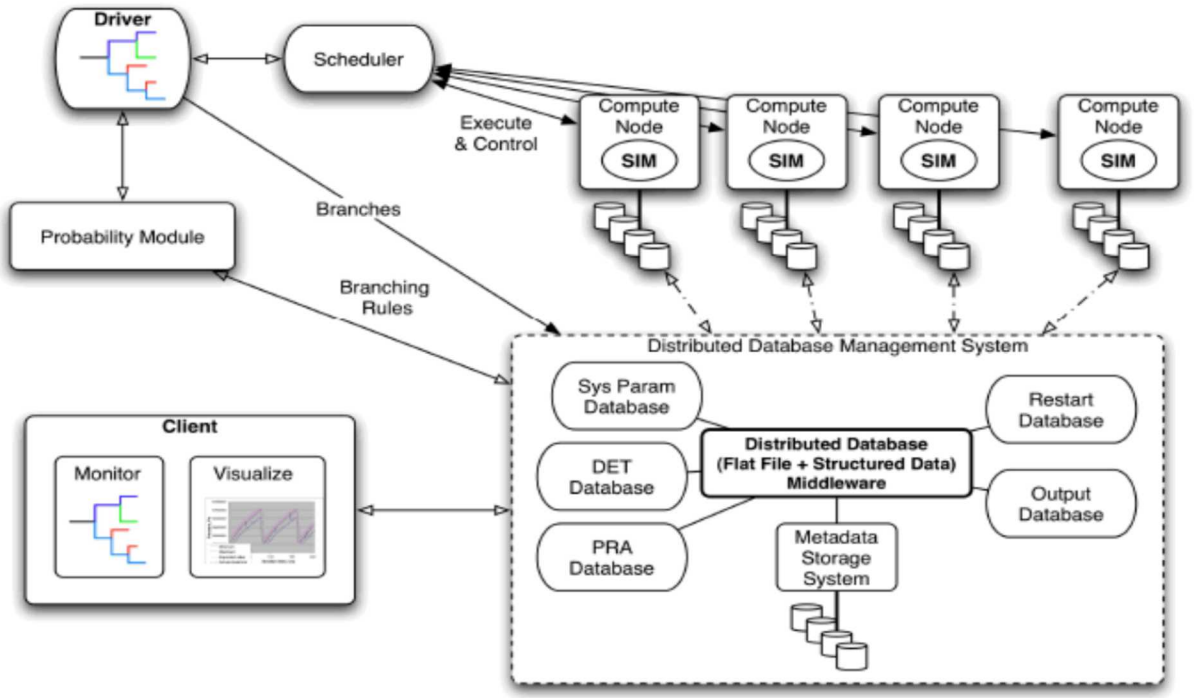
- FoF assumption – Adversary gains access to the control room → Immediate onset of core damage

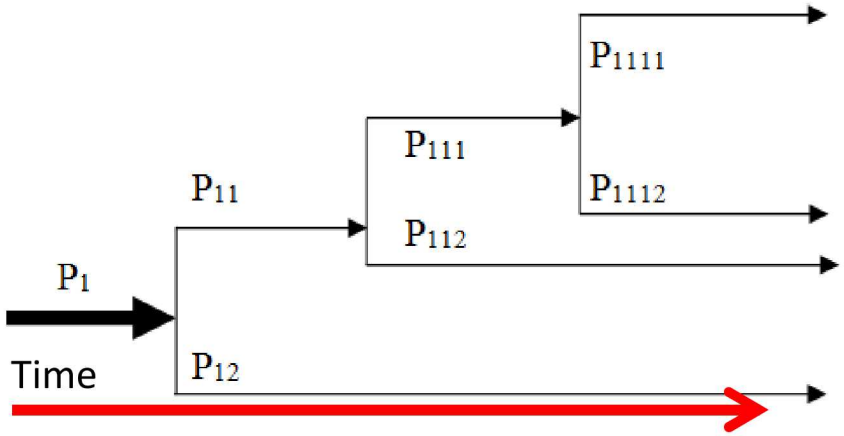
Technical Report: September, 2019

SAND2019-9150C

Analysis Method

- Discrete dynamic event trees is an accelerated uncertainty propagation methodology
  - Predetermined set-points cause the dynamic code (e.g., MELCOR) to stop and restart multiple runs to characterize uncertainties.





Key Point:
Speedup is derived because uncertainties in phenomena experienced late in an event **need not** be simulated from t=0

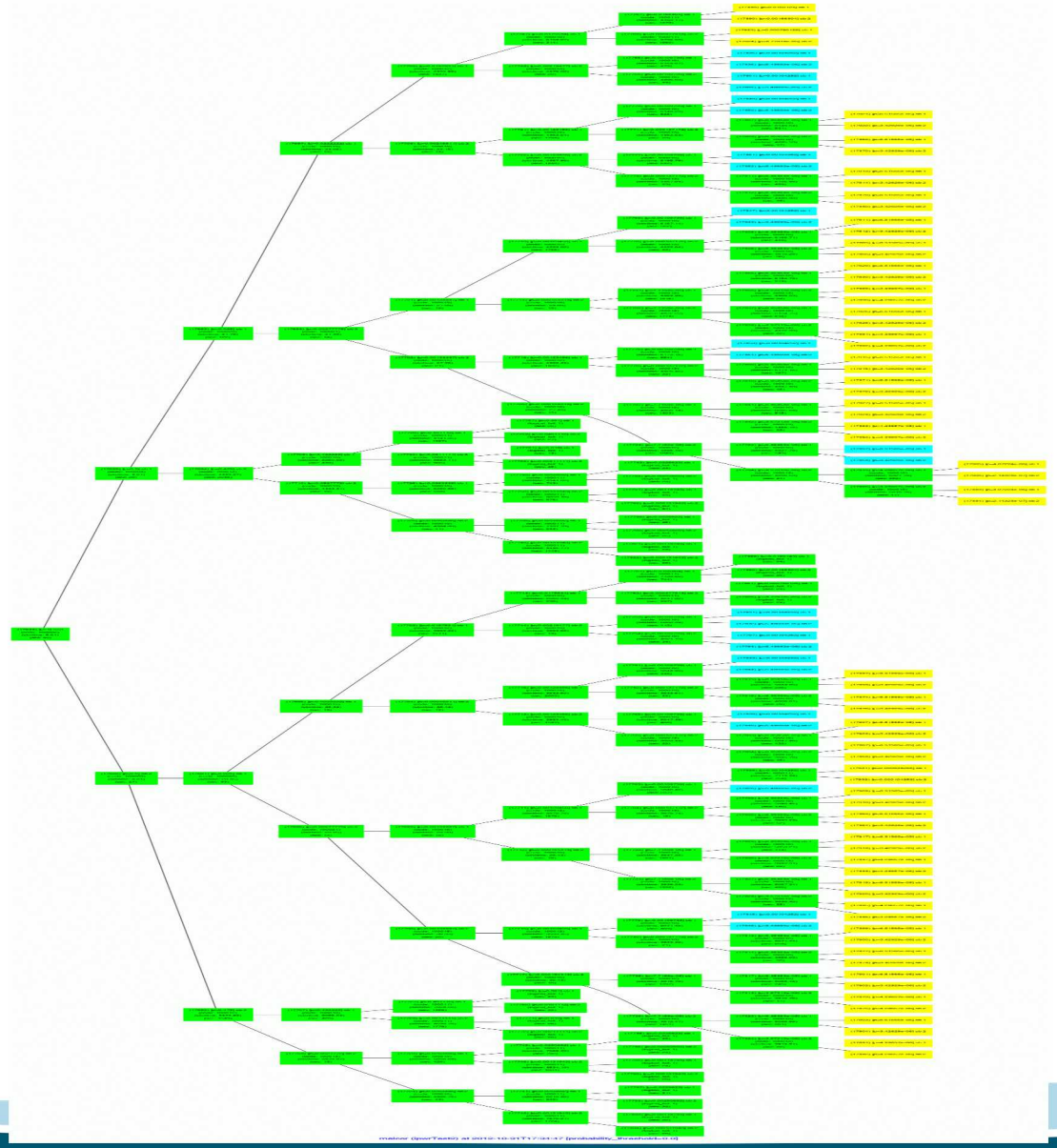
New system response simulations are branched mid-transient

High Level Procedure

1. Create stable dynamic system response simulations
   - The models need to be robust enough not crash the simulation when variables are changed mid-simulation
2. Decide key uncertain parameters of interest for system response models
   - Response force tactics (Force-on-force simulation)
   - Reactor Decay Heat Levels (reactor simulation)
   - Manual operations of equipment (reactor simulation)
   - Delay features (Force-on-force simulation)
   - Others …
3. Create and discretize cumulative distribution functions for key parameters
   - Similar to stratified sampling but simulations are not all started from t=0.
4. Program binary branch points into scheduler code
   - Starts, stops, and branches system response simulations as necessary

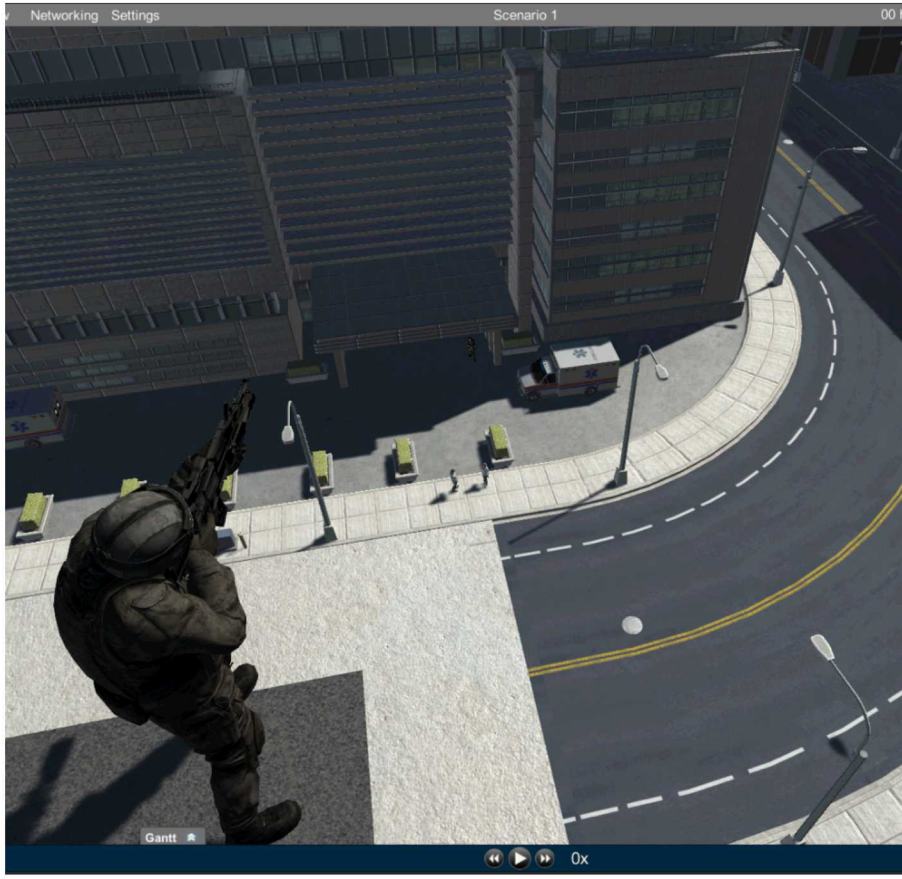
Example of Discrete Dynamic Event Tree Branching

- Branching Visualization
- A Sandia-developed schedule, ADAPT, uses control functions within a nuclear power plant system response code to determine when branching criteria are satisfied
- Branching criteria could be
  - Time
  - SCRAM ignition
  - Number of valve cycles
  - Initiation of cladding oxidation
- However, branching must be binary, but staged binary branches can create for non-binary branching



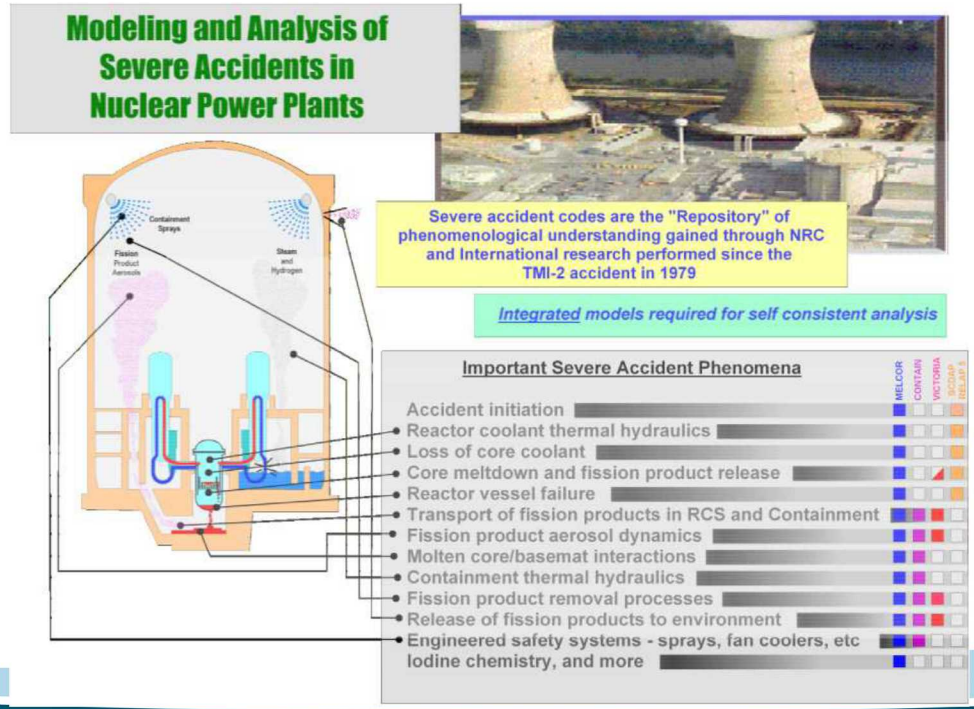
SCRIBE 3D

- Provides tools to visualize & record all events, actions, discussions during a tabletop exercise
- Data Collection
  - Can play back in real time or at various speeds.
  - Transcript reports and video automatically generated
- Full recording of scenario
  - To show others or for later use
  - Allows participants to better understand the impact of their decisions
- Does timeline automatically
  - One person is usually completely dedicated to doing the tabletop's timeline
- Saving/Loading during exercise
  - Can go back and modify scenarios to show how different decisions would affect security
- Solves line of sight issues
  - Shows things a map cannot. (See right)
- Solves timing issues
  - Traditionally it was difficult to figure out where moving entities would be at specific times
- Easy to use
  - Anyone can be trained to use it



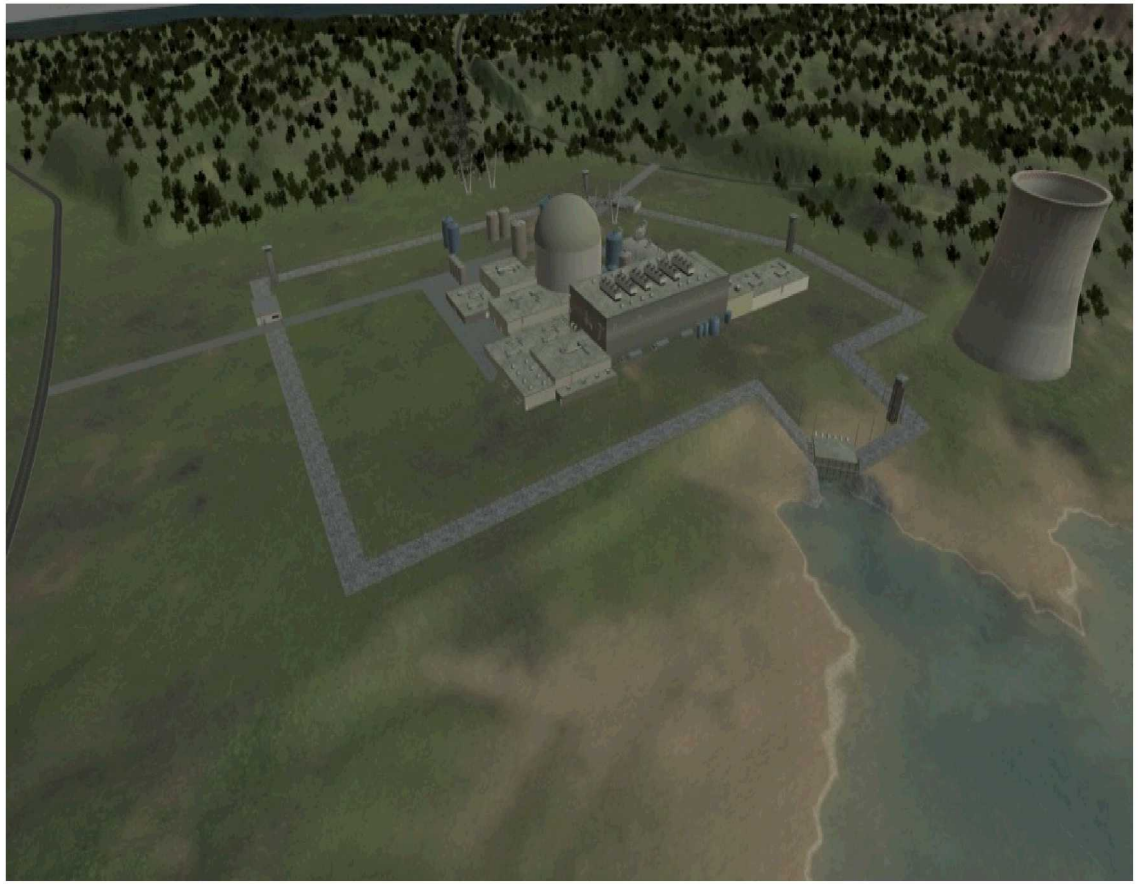
Nuclear Power Plant System Simulator - MELCOR

- NRC sponsored simulation code for analysis of accidents in nuclear power plants
  - Applied to containment design basis accident simulation too
  - Reactor types: PWR, BWR, HTGR, PWR-SFP, BWR-SFP, HTGR, SFR
- Fully Integrated, engineering-level code
  - Thermal-hydraulic response in the reactor coolant system, reactor cavity, containment, and confinement buildings;
  - Core heat-up, degradation, and relocation;
  - Core-concrete attack;
  - Hydrogen production, transport, and combustion;
  - Fission product release and transport behavior
- Desktop application
  - Windows/Linux versions
  - Relatively fast-running
    - One or two days common
    - One or two weeks possible
    - Project to improve code performance
  - SNAP for post-processing, visualization, and GUI



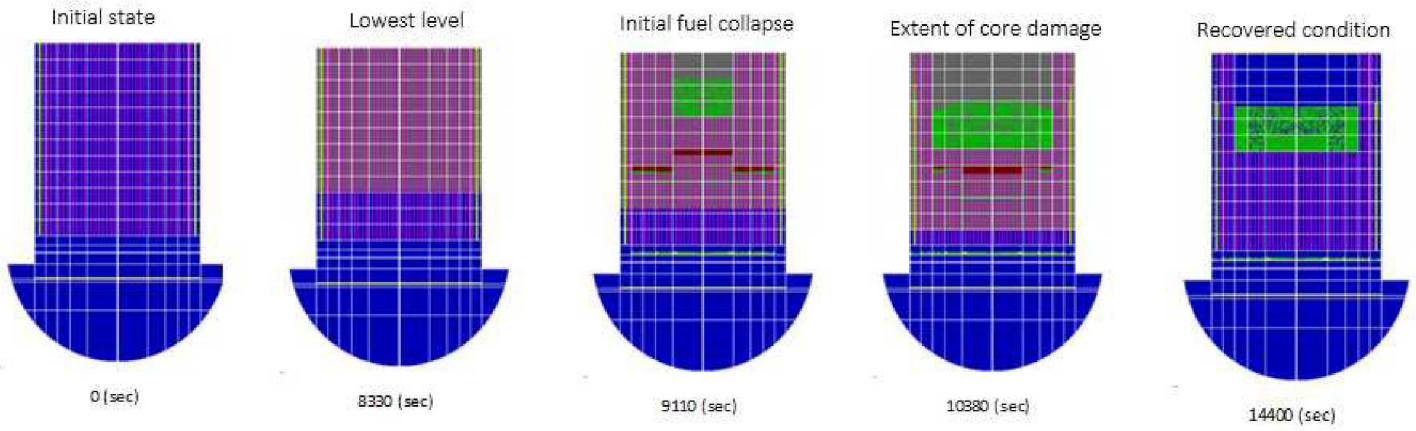
Scenario – Lone Pine Nuclear Power Plant Site

- Lone Pine Nuclear Power Plant
  - Hypothetical pressurized water reactor (PWR) built in 1972 to produce 1150 MW_e in a fictional country
  - Open source information that is purposefully incomplete for physical protection system and protective strategy
  - Initially created for discussions between the USG and other countries on nuclear power plant security
- Allows for open discussions on;
  - Physical protection system technologies and deployment
  - Protective strategy and response for adversary scenarios
- Allows for open source modeling comparisons



Progress

- Update the TMI-2 MELCOR model for use with ADAPT in the Lone Pine scenario
  - MELCOR deck has been converted and generic scenarios
  - ADAPT is the dynamic event/fault tree scheduler
- Updates to the SCRIBE 3D model and force-on-force scenarios are complete
- Initiated linking SCRIBE 3D to ADAPT
  - Potential Issue: SCRIBE 3D is a Unity software platform and has only been run on Windows OS
    - ADPAT is a LINUX based software

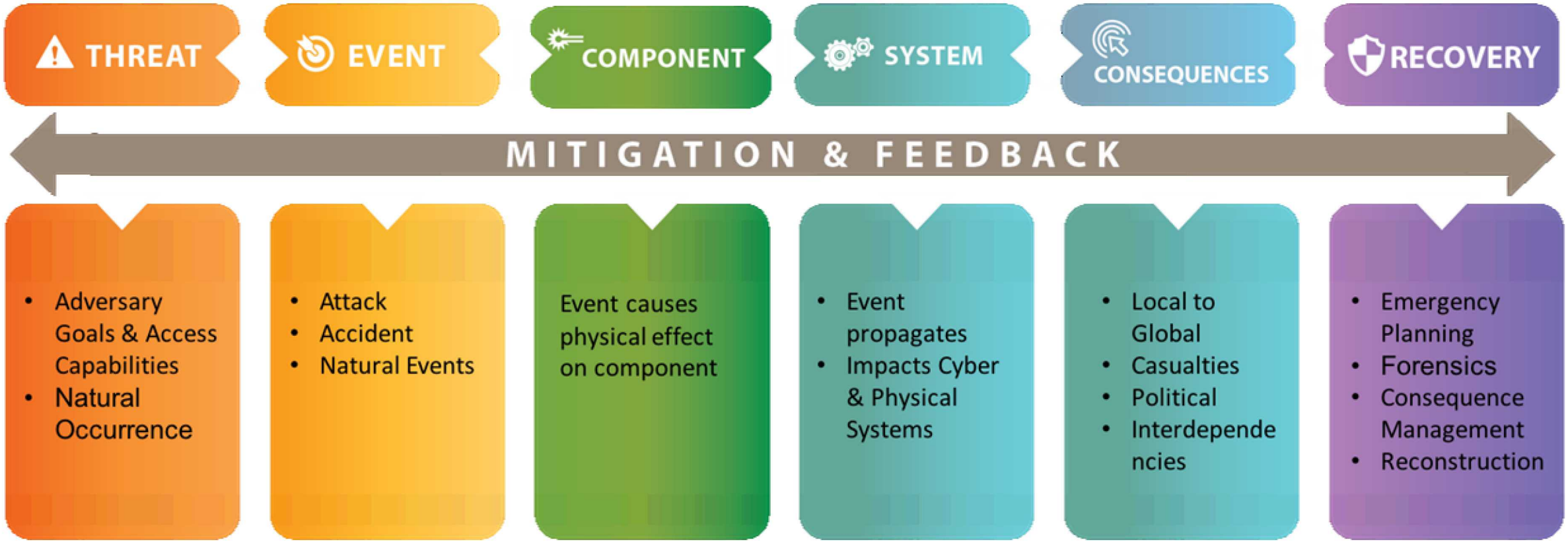


TMI-2-like melt progression
Lone Pine NPP reactor design

Lone Pine Nuclear Power Plant
Notional Facility
Shown in Scribe 3D

LWRS LIGHT WATER REACTOR SUSTAINABILITY

Integrated Cyber Physical Impact Analysis



Integrated Cyber Physical Impact Analysis

- **The ICPIA framework integrates capabilities such as:**
  - Threat modeling
  - Adversary-based Vulnerability Assessment
  - Enterprise network and control system Emulytics™
  - Physical modeling and simulation
    - Device to system scale; across domains
  - Interrelated critical infrastructure impacts

- **What It Is:**
  - Systems (tool) used to help project leaders break down a cyber-related question into its component pieces to identify the necessary effort and interfaces across the domains
  - Communication tool for discovery between a customer and a PM to help define the customer's problem, the information needed, modeling fidelity required and deliverables. How will the question be answered?
  - Tool to guide stakeholders to the modeling, simulation, and Emulytics™ tools that will support the necessary analysis
  - Framework to categorize existing tools and capabilities
- **What It Is Not:**
  - ICPIA is not an Emulytics™ tool that performs any actual analysis
  - A monolithic analysis tool – currently, the transfer of results from one domain to another is not automated.
  - Completely novel – Sandia and other organizations have integrated modeling and simulation framework utilizing multiple domains.

Questions