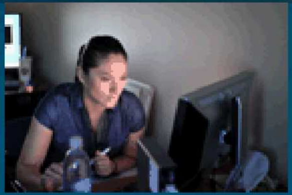
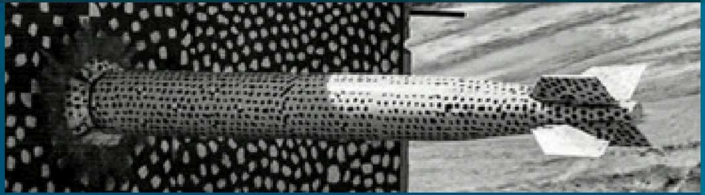
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-9150C

Modeling and Simulation Case Studies

An Integration of System Response





Douglas M. Osborn, PhD

INMM Workshop on Emerging Issues in Nuclear Security
Harvard University

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

SAND2019-XXXX-P

DOE-NE Light Water Reactor Sustainability (LWRS) Program

The LWRS Program conducts research to develop technologies and other solutions to improve the economics and reliability, sustain the safety, and extend the operation of our nation’s fleet of nuclear power plants. It has two objectives with respect to long-term operations:

1. To provide science and technology-based solutions to industry to overcome the current labor-intensive business model and associated practices; and
2. To manage the aging of systems, structures, and components (SSCs) so nuclear power plants can continue to operate safely and cost effectively.

The Light Water Reactor Sustainability (LWRS) Program is focused on the following three goals:

1. Developing the fundamental scientific basis to understand, predict, and measure changes in materials and SSCs as they age in environments associated with continued long-term operations of existing nuclear power plants.
2. Applying this fundamental knowledge to develop and demonstrate methods and technologies that support the safe and economical long-term operation of existing nuclear power plants.
3. Researching new technologies to address enhanced nuclear power plant performance, economics, and safety.

LWRS R&D Pathways:

- Materials Research
- Plant Modernization
- Risk-Informed Systems Analysis

LWRS Initiatives:

- Physical Security
- Integrated Energy Systems

DOE-NE LWRS Program Physical Security Initiative (PSI)

Physical security of nuclear power plants is a vital aspect of maintaining a safe and reliable national nuclear energy capability. Physical security programs at U.S. nuclear sites have evolved to meet changes to their design basis threat (DBT) since the 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 U.S. nuclear power plants modernize their infrastructure and control systems, opportunities exist to apply advanced tools, methods, and automation to modernize physical security programs. Potential benefits expected from the LWRS PSI include higher fidelity models that may reduce conservatisms in security modeling, leverage automation as force multipliers, optimize security postures, and develop additional means to risk-inform approaches to evaluate security changes.

This LWRS 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 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.

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

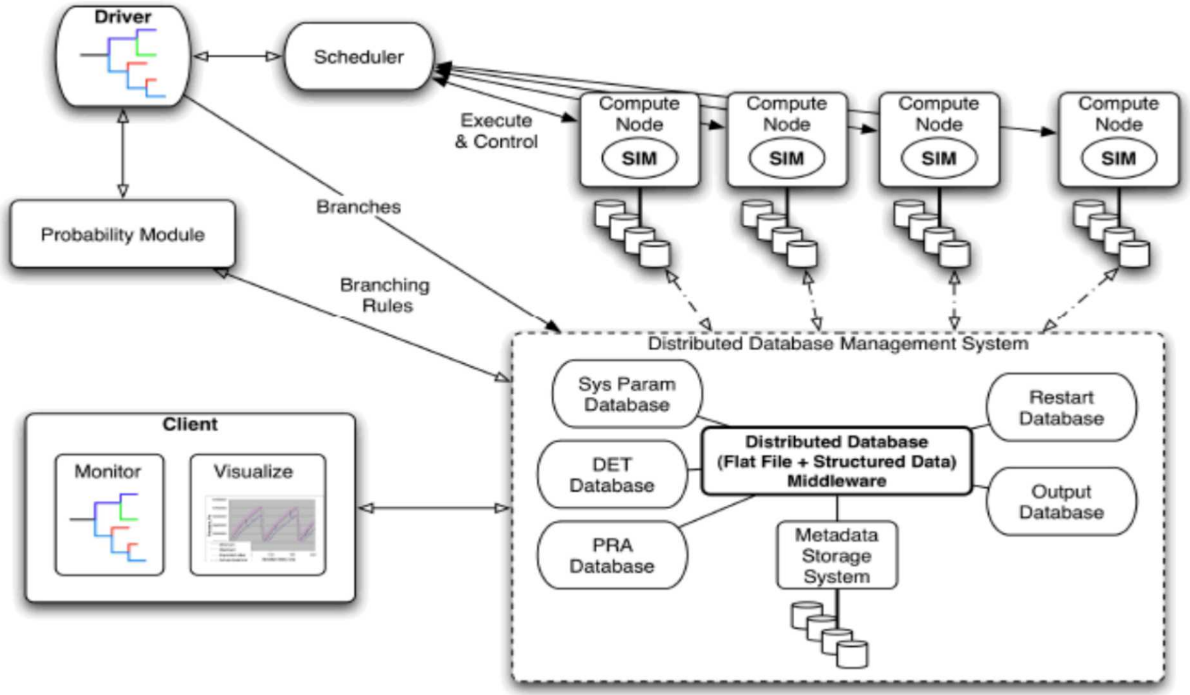
- FoF assumption – Adversary gains access to the control room → Immediate onset of core damage

Technical Report: September, 2019

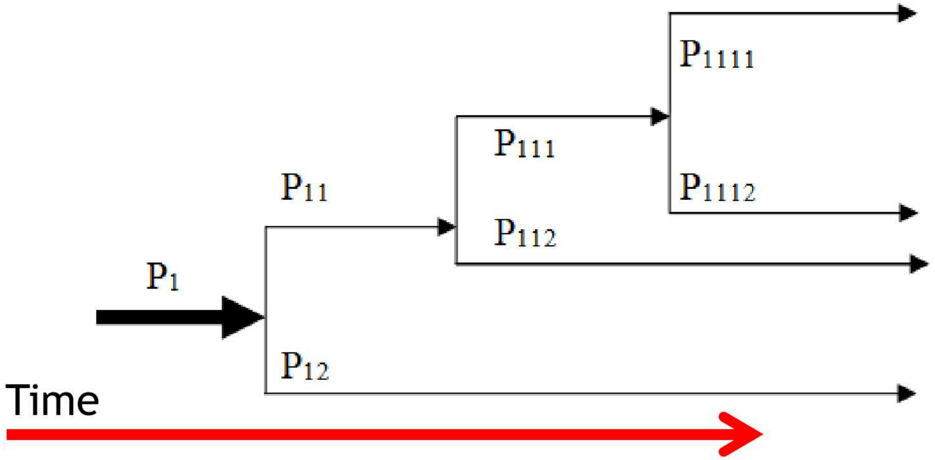
Analysis Method

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

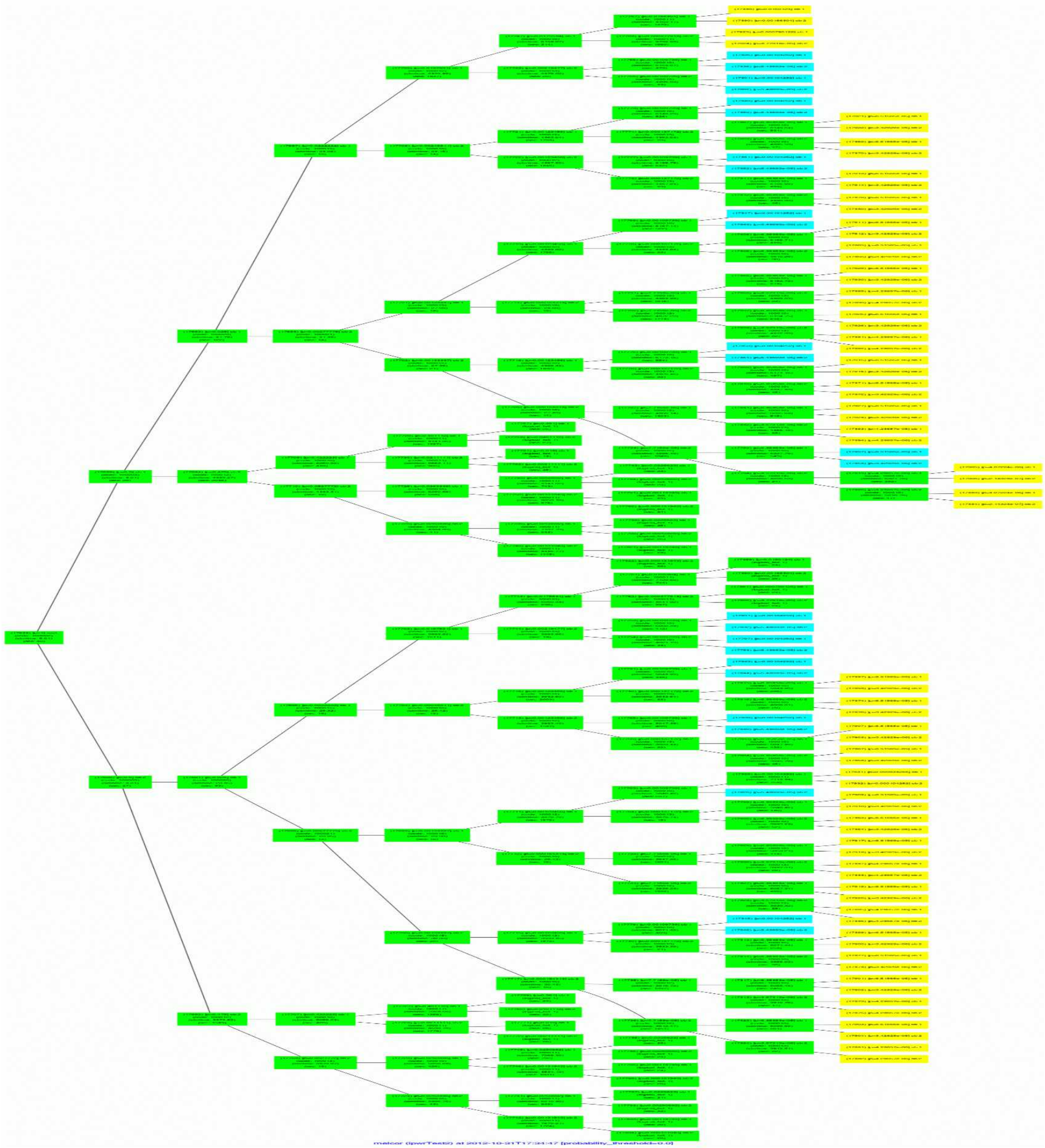
Branching Visualization

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


melcor (ipwrTest2) at 2012-10-31T17:34:47 [probability_threshold=0.0]

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

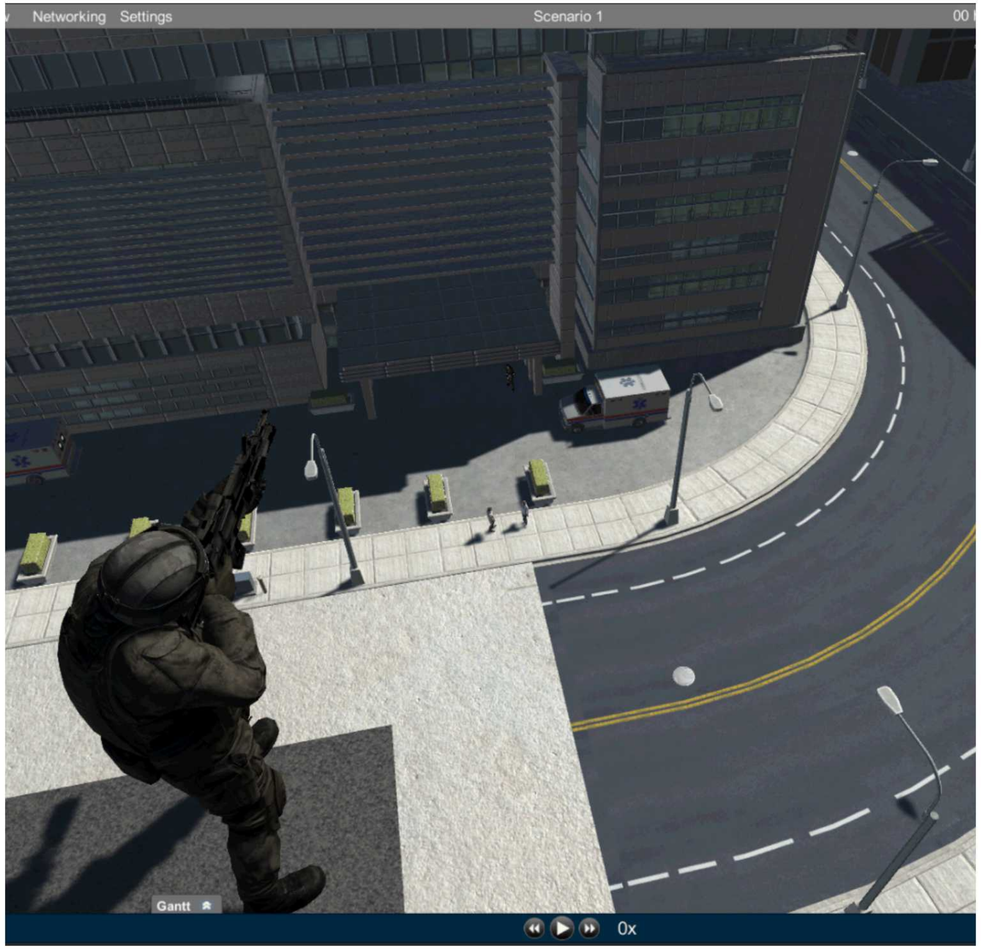
- Shows things a map cannot. See right

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

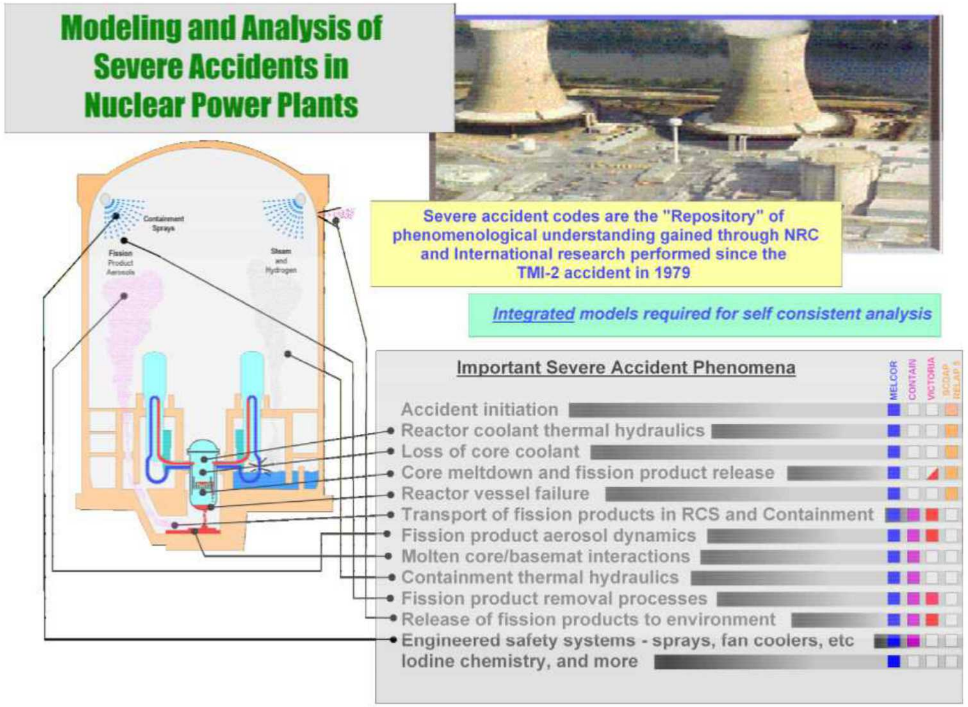
- Applied to containment design basis accident simulation too
- Reactor types: PWR, BWR, HTGR, PWR-SFP, BWR-SFP, HTGR, SFR

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



Modeling and Analysis of Severe Accidents in Nuclear Power Plants

Severe accident codes are the "Repository" of phenomenological understanding gained through NRC and International research performed since the TMI-2 accident in 1979

Integrated models required for self consistent analysis

Important Severe Accident Phenomena	MELCOR	CONTAIN	VICTORIA	SCDAP RELAP 5
Accident initiation	■	□	□	■
Reactor coolant thermal hydraulics	■	□	□	■
Loss of core coolant	■	□	□	■
Core meltdown and fission product release	■	□	◩	■
Reactor vessel failure	■	□	□	■
Transport of fission products in RCS and Containment	■	■	■	□
Fission product aerosol dynamics	■	■	■	□
Molten core/basemat interactions	■	■	□	□
Containment thermal hydraulics	■	■	□	□
Fission product removal processes	■	■	■	□
Release of fission products to environment	■	■	■	□
Engineered safety systems - sprays, fan coolers, etc	■	■	□	□
Iodine chemistry, and more	■	□	□	□

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

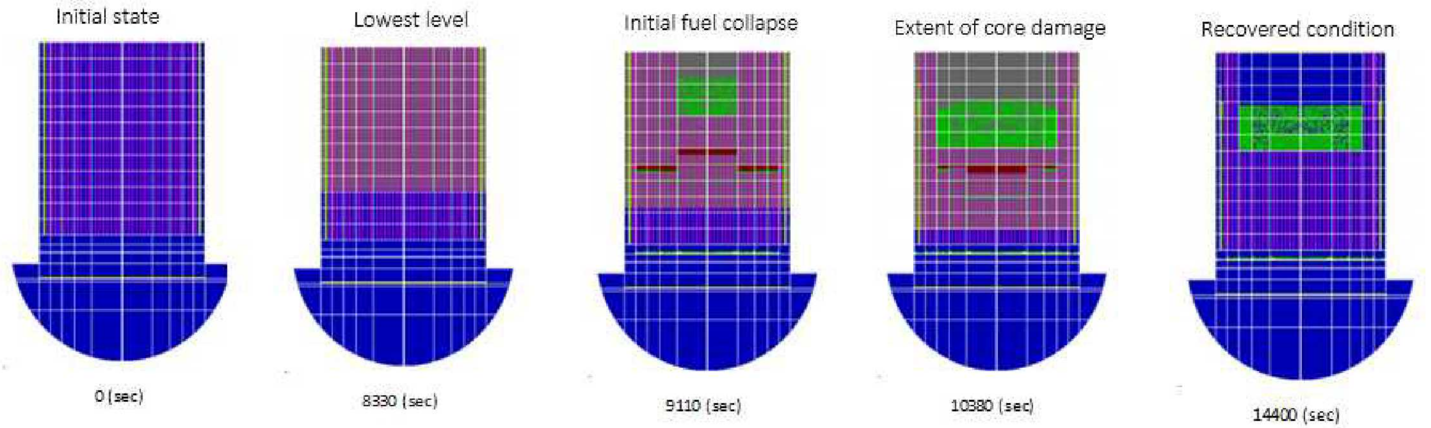
Update the TMI-2 MELCOR model for use with ADAPT in the Lone Pine scenario

- MELCOR deck has been converted and generic scenarios
- ADAPT is the dynamic event/fault tree scheduler

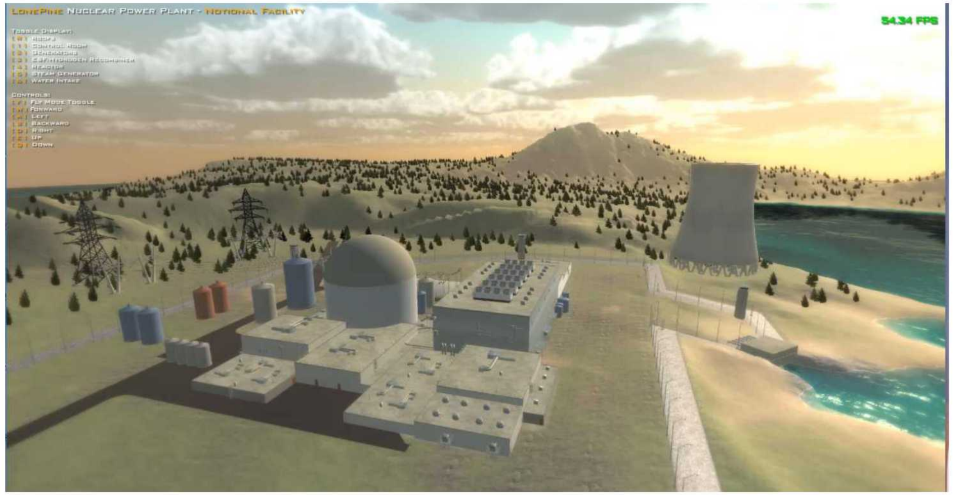
Updates to the SCRIBE 3D model and force-on-force scenarios are complete

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

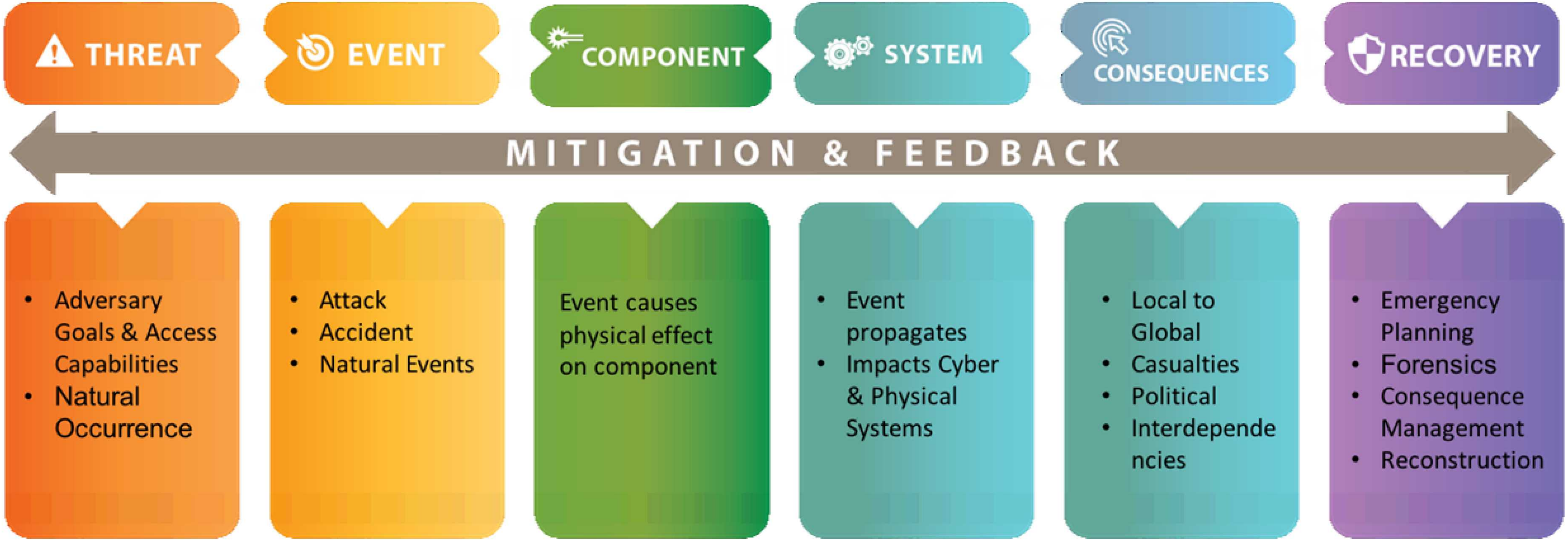


TMI-2-like melt progression
Lone Pine NPP reactor design



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

Integrated Cyber Physical Impact Analysis



THREAT

- Adversary Goals & Access Capabilities
- Natural Occurrence

EVENT

- Attack
- Accident
- Natural Events

COMPONENT

Event causes physical effect on component

SYSTEM

- Event propagates
- Impacts Cyber & Physical Systems

CONSEQUENCES

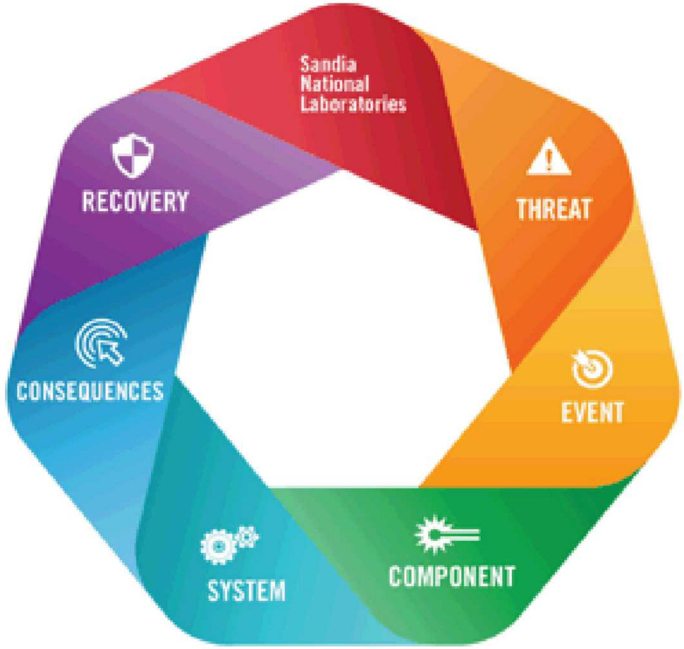
- Local to Global
- Casualties
- Political
- Interdependencies

RECOVERY

- Emergency Planning
- Forensics
- Consequence Management
- Reconstruction

MITIGATION & FEEDBACK

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.

Risk-Informed Nuclear Security

Traditional Risk Equation:

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

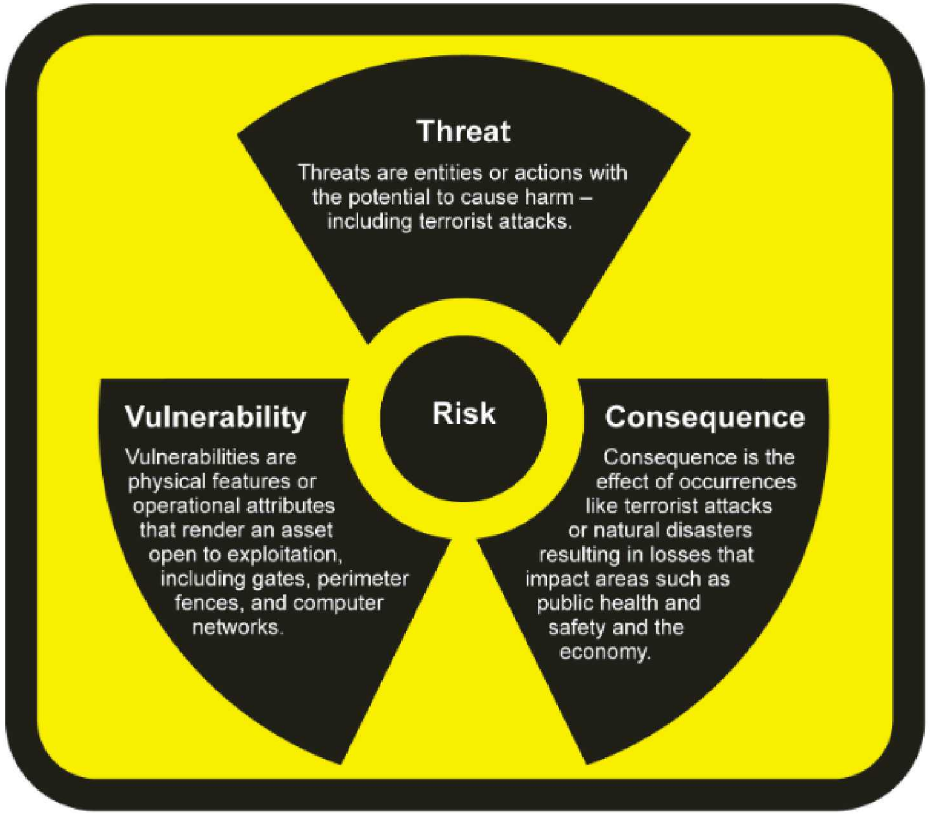
Where:

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



Threat

Threats are entities or actions with the potential to cause harm – including terrorist attacks.

Risk

Vulnerability

Vulnerabilities are physical features or operational attributes that render an asset open to exploitation, including gates, perimeter fences, and computer networks.

Consequence

Consequence is the effect of occurrences like terrorist attacks or natural disasters resulting in losses that impact areas such as public health and safety and the economy.

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

Security Risk Equation:

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

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

Questions