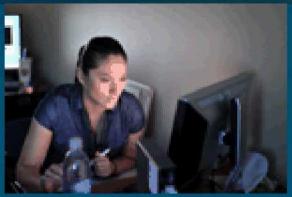
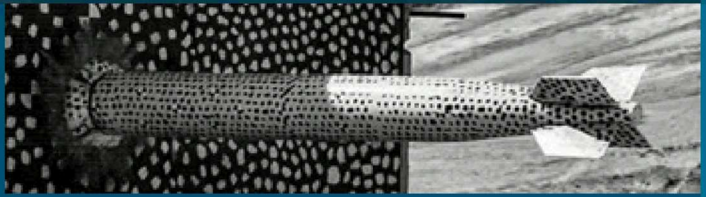
SAND2019-9713C

LWRS Program
Sandia Physical Security Efforts





Douglas M. Osborn, PhD

National Security and Emergency Preparedness Summit
Scottsdale, AZ

SAND2019-XXXXXC

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.

Evaluate existing USG technologies

Evaluate current challenges and constraints associated with the physical security regime in the domestic Light Water Reactor nuclear industry

- Identify existing DoD, DOE-NNSA, and DHS data and methods for potential use with domestic fleet

Conduct initial assessment and provide recommendations on areas for improvements to reduce cost to implement an effective security program

- Identify near-term and long-term LWRS R&D efforts

Initial evaluation to develop and validate methods which can be used to implement an updated and optimized physical security regime for the domestic fleet

- Create validated data sets on M&S techniques for applications by the domestic LWRs

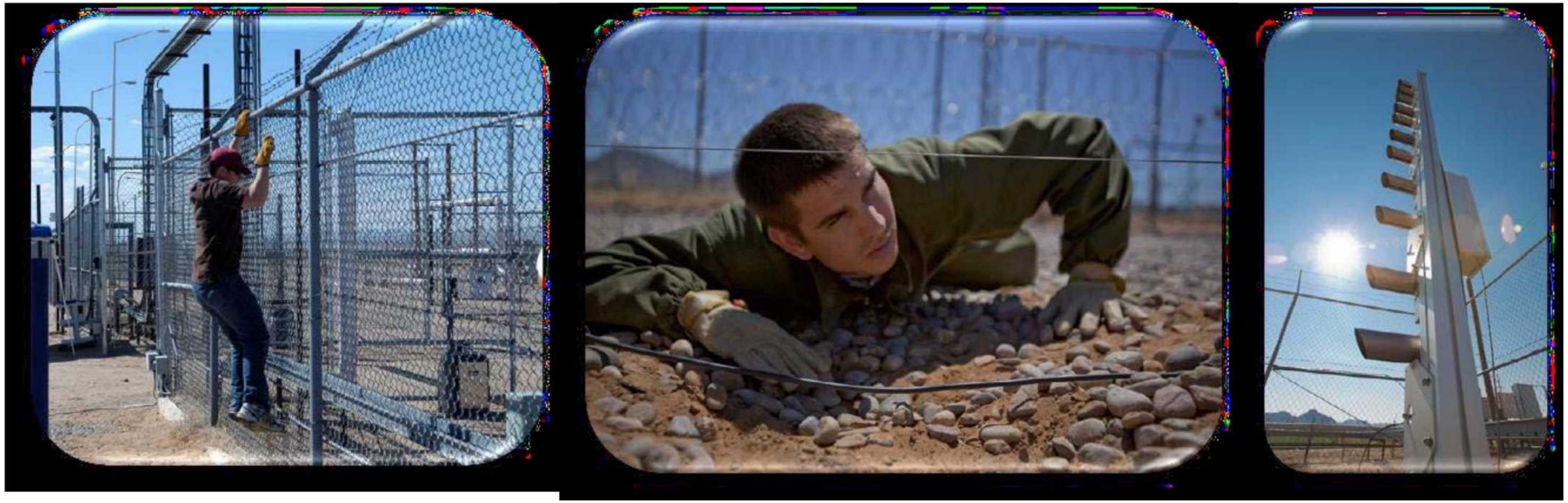
Provide technical training on physical security technologies, modeling, and enhancements

10 SNL staff provided the 5-day classroom, hands-on, and demonstration sessions

Attended by 14 utilities, NEI, EPRI, and INL

Complete and overall feedback is very positive

- Working with NEI to determine interest in future training efforts funded by industry



Revise Lone Pine Documentation

Lone Pine Nuclear Power Plant

- Hypothetical PWR built in 1972 to produce 1150 MW_e in a fictional country
- Open source information that is purposefully incomplete for PPS and protective strategy
- Initially created for discussions between the USG and other countries on NPP security

Allows for open discussions on;

- PPS technologies and their deployment
- Protective strategy and response for adversary scenarios

Allows for open source modeling comparisons

Integrated System Response Modeling

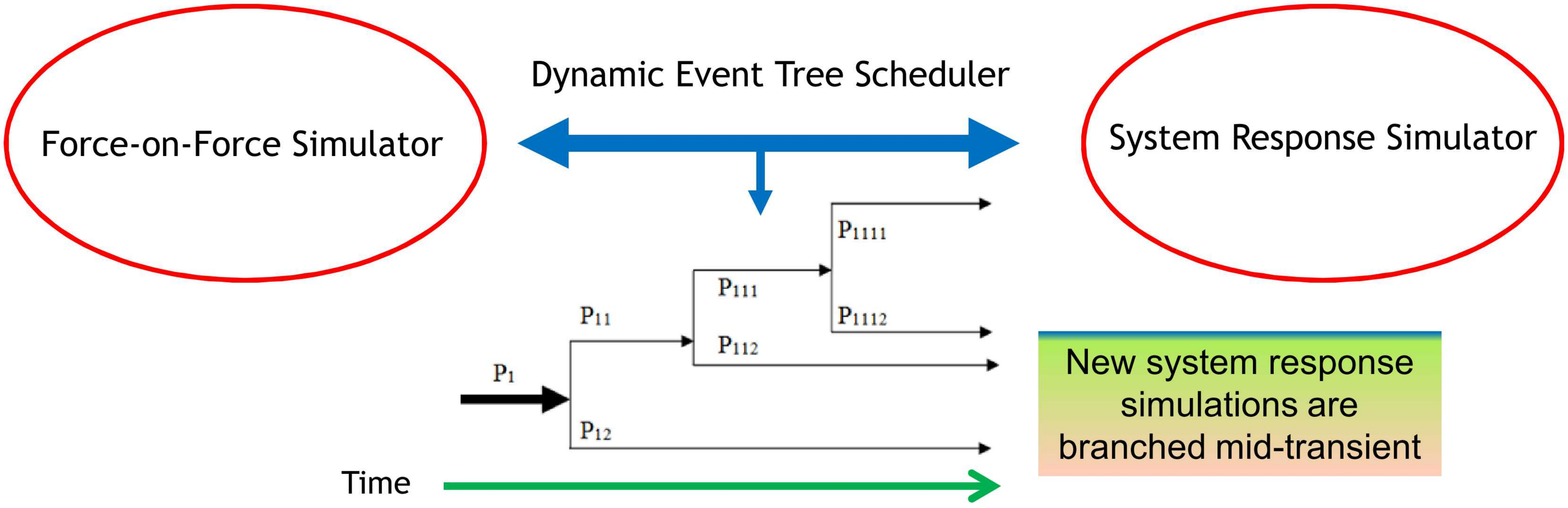
Goal: Develop modeling and simulations for existing plant security regimes using identified target sets to link dynamic assessment methodologies by leveraging nuclear power plant system level modeling with force-on-force modeling, and 3D visualization for developing table-top scenarios

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

Methodology



Discrete dynamic event trees is an accelerated uncertainty propagation methodology

- Predetermined set-points cause the dynamic simulator 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

High Level Procedure

1. Create stable dynamic 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 dynamic 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 dynamic event tree scheduler
   - Starts, stops, and branches system response simulations as necessary

Dynamic Event Tree Scheduler – ADAPT

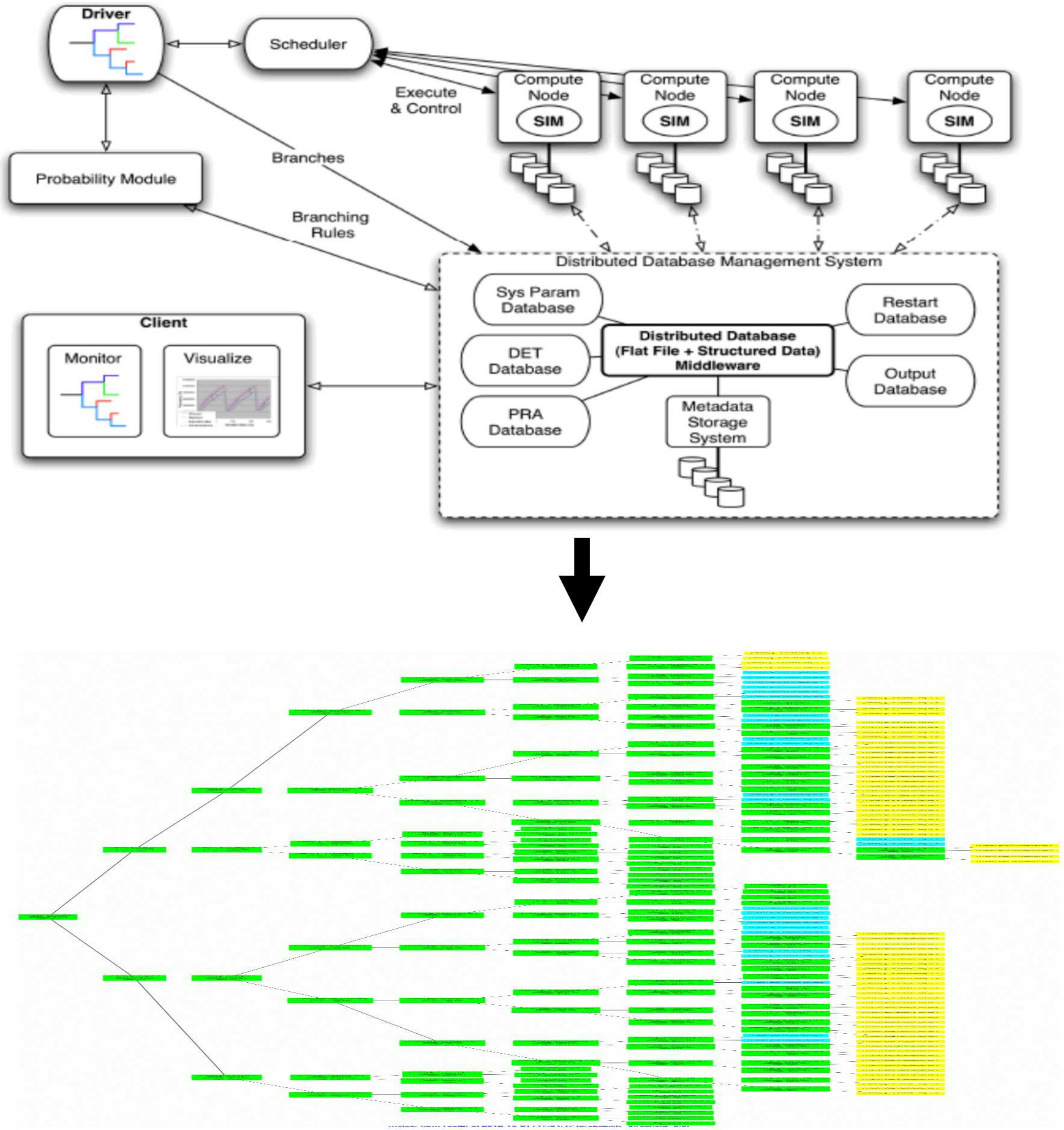
A Sandia-developed dynamic event tree scheduler uses control functions within a nuclear power plant system response simulator to determine when branching criteria are satisfied

Branching criteria could be

- Time
- SCRAM ignition
- Number of valve cycles
- Initiation of cladding oxidation

Branching Visualization

However, branching must be binary, but staged binary branches can create for non-binary branching



Force-on-Force Simulator – 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

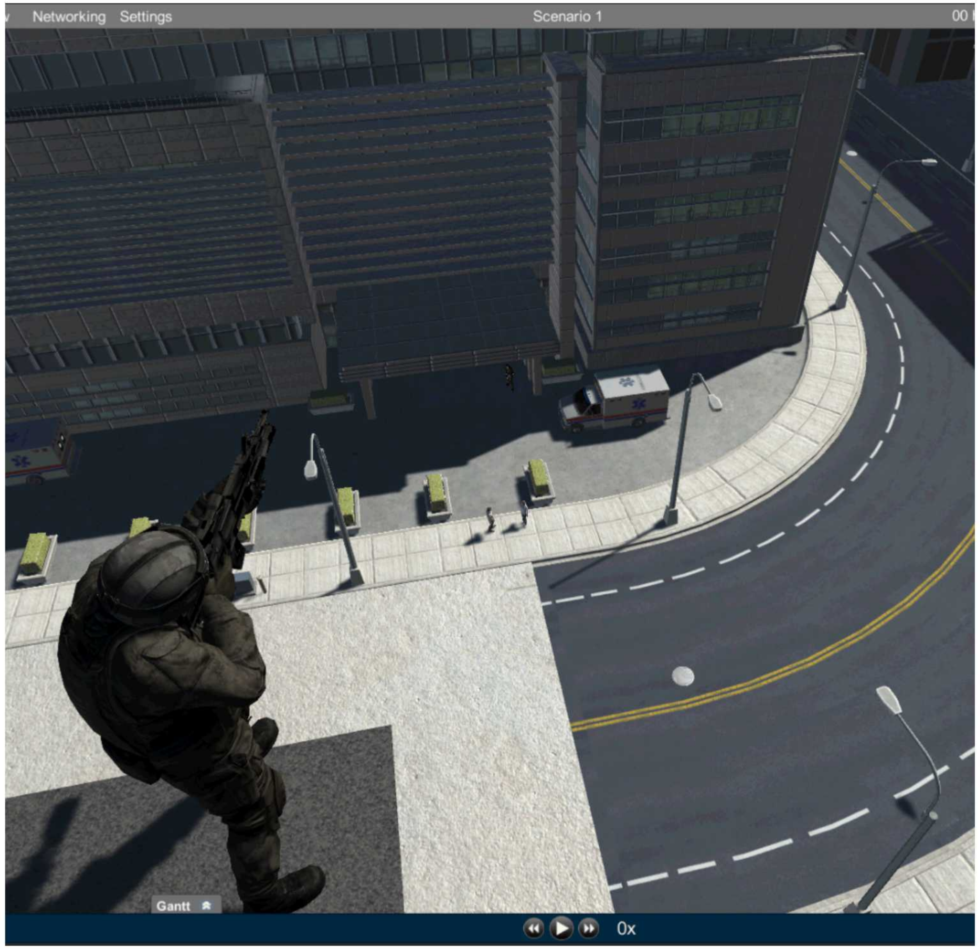
Does timeline automatically
- One person is usually completely dedicated to doing the tabletop's timeline

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 Response Simulator – MELCOR

NRC sponsored simulation code for analysis of accidents in nuclear power plants

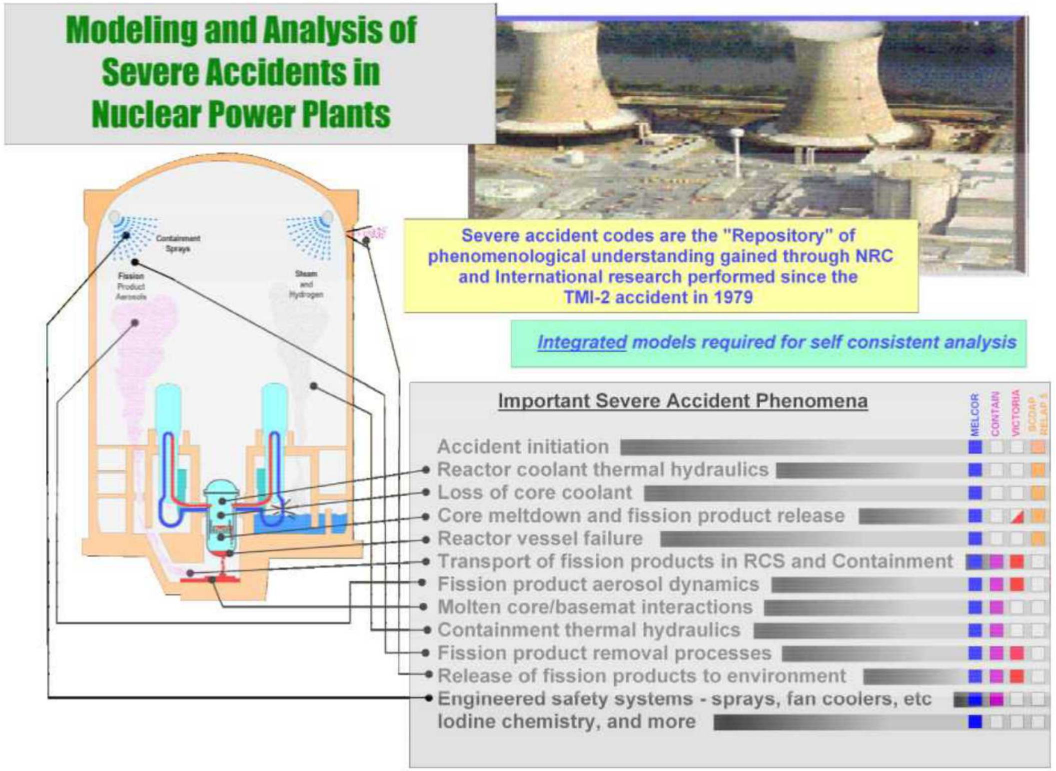
- Applied to containment design basis accident simulation too
- Reactor types: PWR, BWR, HTGR, PWR-SFP, BWR-SFP, HTGR, SFR

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



Progress to date

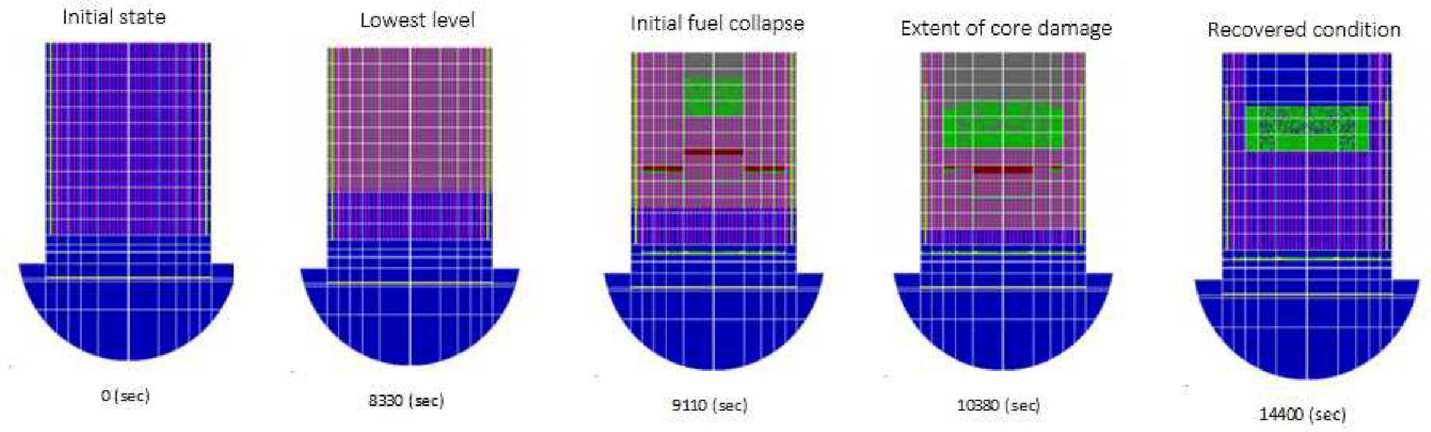
Update the TMI-2 MELCOR model for use with ADAPT in the Lone Pine scenario

- 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

Risk-Informed Nuclear Security – Direct Translation

Traditional Nuclear Safety 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,…,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

Direct Translation Security Risk Equation:

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

NOT appropriate

The equation is incomplete

Where:

i = The i^th scenario category (i = 1,…,l)

j = The j^th target set (j = 1,….,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

Past Risk Informed Security Models

Risk-Informed Management of Enterprise Security (RIMES) Risk Equation:

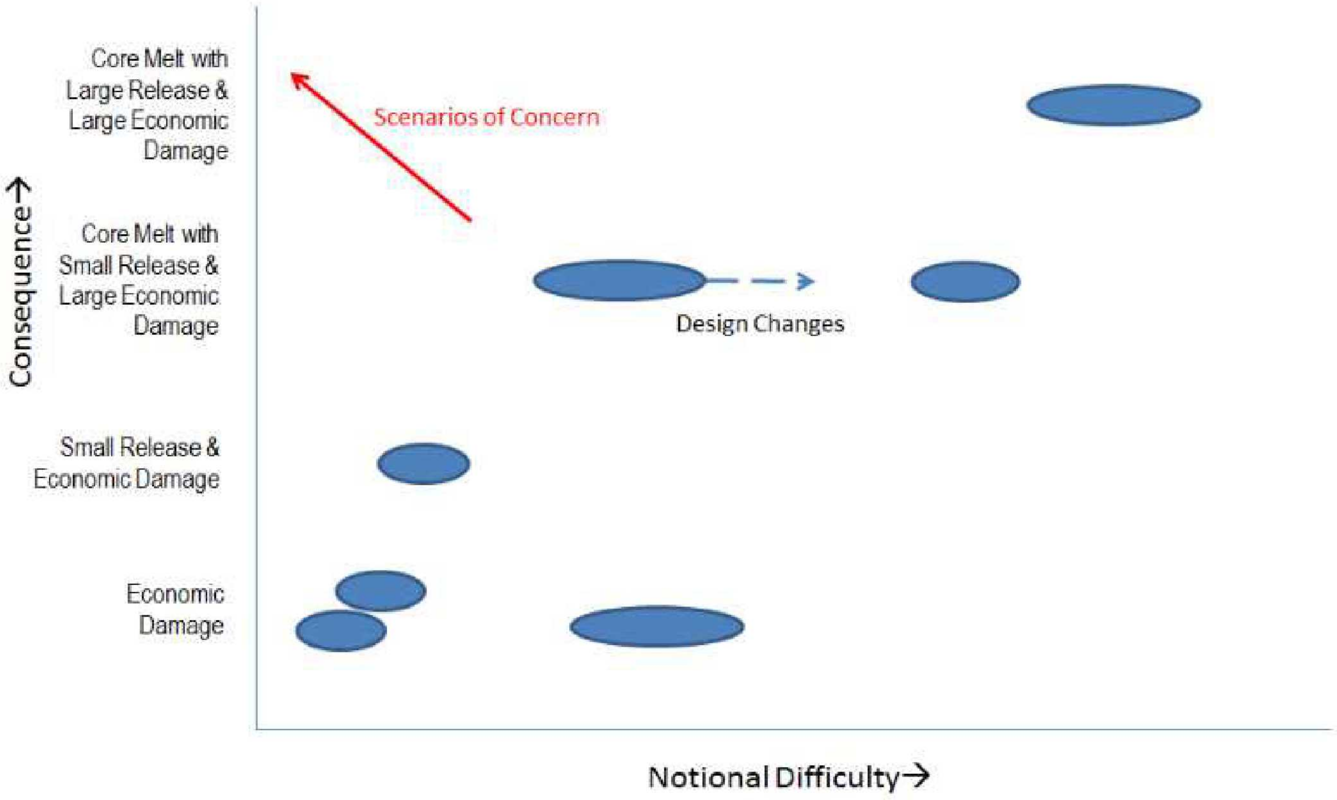
$$\text{Risk} = \bigcup_{i=1}^{i=I}\{\langle d_i, x_i\rangle\}$$

Where:

i = The i^{th} scenario $i = 1,\ldots,I$

d_i = The degree of difficulty for an adversary to successfully accomplish i^{th} scenario causing consequence x_i

x_i = The consequence or evaluation measure of the i^{th} scenario



Note: In this RIMES representation, as well as the next model, the target index will be included under the scenario index, *i*, to simplify the notation

Past Risk Informed Security Models *(continued)*

More General Security Risk Equation:

$$\text{Risk} = \bigcup_{j=1}^{j=J}\left(\bigcup_{i=1}^{i=I}\{\langle tp_{ij}, x_i, \rangle\}\right)$$

Note: A more precise form of this model would consider adversary utility based on the range of possible outcomes from the scenario

Where:

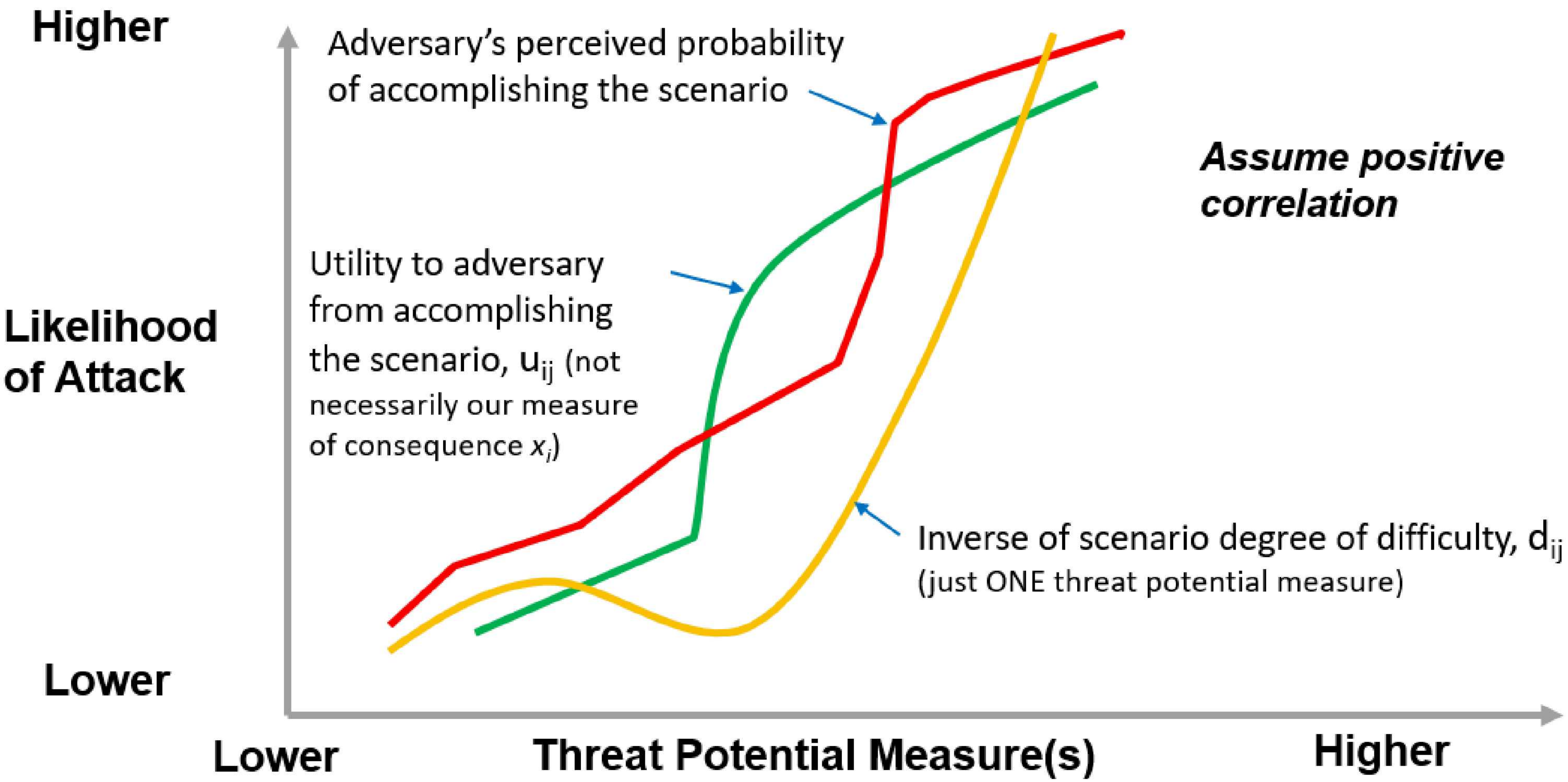
j = The j^{th} adversary (from a threat assessment) $j = 1,\ldots,J$
i = The i^{th} scenario $i = 1,\ldots,I$
tp_{ij} = Threat potential for an j to want to accomplish i^{th} scenario causing consequence x_i
x_i = The consequence or evaluation measure of the i^{th} scenario
pe_{ij} = The effectiveness of the physical protection system in preventing the adversary j from successfully accomplishing i^{th} scenario causing consequence x_i

Where *threat potential* is assumed to be some combination of the following factors that is correlated with the (unknown) probability of attack:

d_{ij} = The degree of difficulty for adversary j to successfully accomplish i^{th} scenario causing consequence x_i
pas_{ij} = Adversary j's perceived probability of success in accomplishing the i^{th} scenario.
u_{ij} = The utility for adversary j from successfully accomplishing i^{th} scenario causing consequence x_i

Threat Potential rather than Probability of Attack

Threat Potential is defined as a set of measures that are treated *as if* they are positively correlated with the "True" Likelihood of Attack



Questions