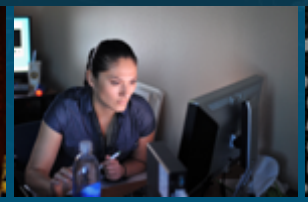
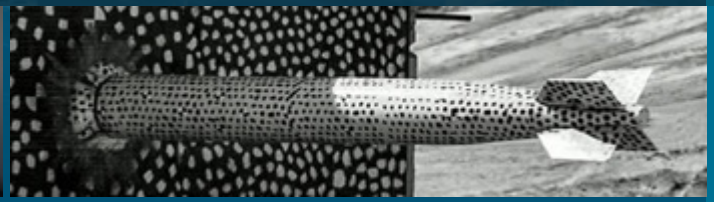
SAND2021-14105C

Sandia National Laboratories

Integrated Safety-Security Analysis using EMRALD





PRESENTED BY

Brian Cohn

U.S. DEPARTMENT OF ENERGY | NNSA

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.

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.

Introduction

Nuclear safety and security are separate concepts with similar goals

- Addressing possible losses of reactor systems
- Protecting public from consequences of nuclear power

Systems at nuclear power plants are complex and highly intertwined

Minimizing systemwide risks requires a combined safety-security (2S) analysis

Risk triplet for safety risks

- Risk = <scenario, likelihood, consequence>

Previous attempts at 2S analysis

ERDA-7

- Applies safety risk triplet to security
  - $R = l \times c \times (1 - P_E)$

Vital Area Identification

- Based on safety fault trees

RIMES

- Semi-quantitative, based on rankings from subject matter experts

Challenges with Integrated 2S Analyses

Adversaries decide to attack facilities

Decision to attack depends on PPS

Passive components can be damaged by adversaries

Safety and security events have different circumstances

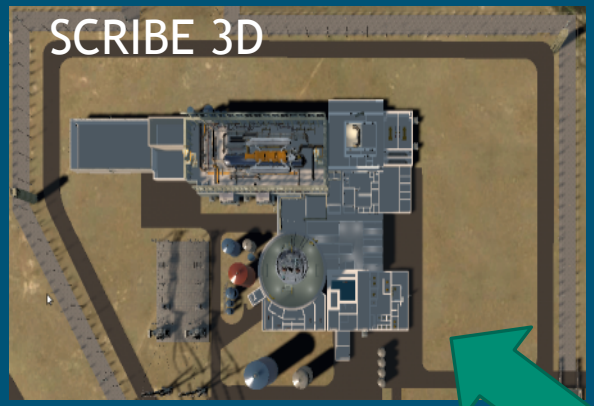
Research Framework

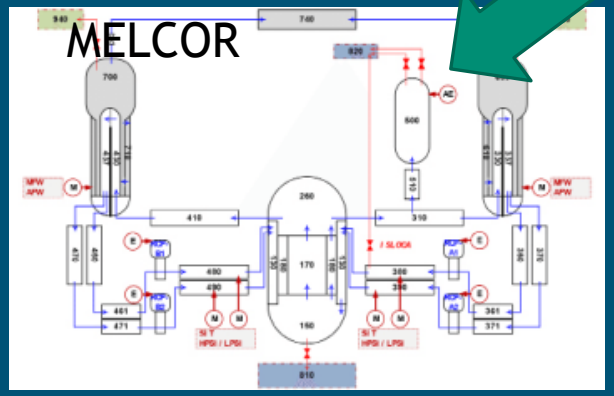
Purpose is to develop an integrated 2S analysis
- Driver code - EMRALD
- Safety code - MELCOR
- Security code – Scribe3D

EMRALD is a Markovian risk modeling tool
- Based on transitions between system states and connected to fault trees
- Uses a three phase event simulation process

MELCOR is a reactor system tool
- Models reactor accident evolution
- Includes all aspects of an accident

Scribe3D is a force-on-force tool
- Serves to support tabletop analysis
- Models damage to and availability of reactor systems





Results

Lone Pine Nuclear Power Plant

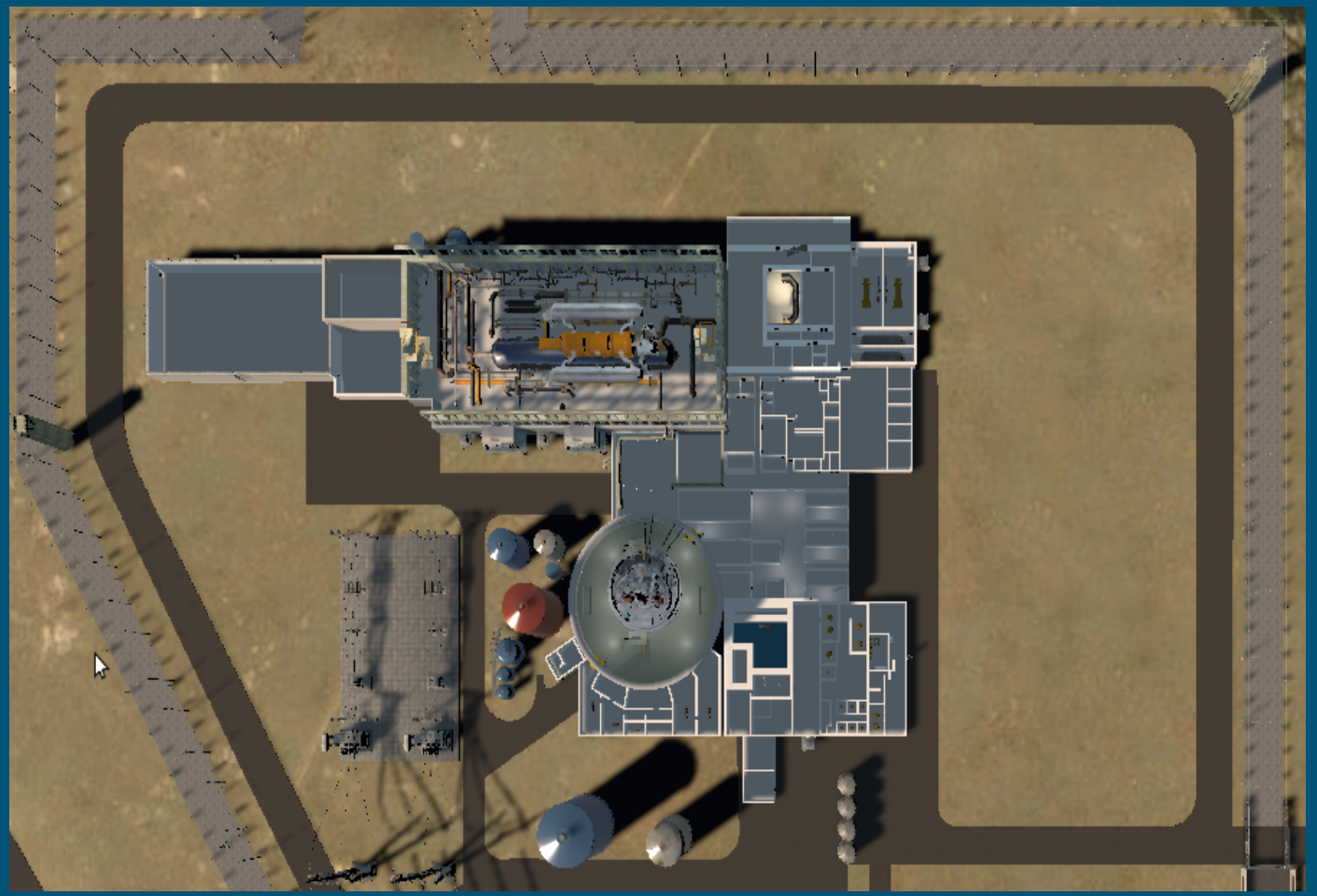
Security postures are restricted information

- Methods are public, but cannot risk revealing vulnerabilities of existing plants

Hypothetical Lone Pine Nuclear Power Plant developed for teaching best practices

- Includes artificial vulnerabilities

Adapted in this analysis to represent a BWR plant



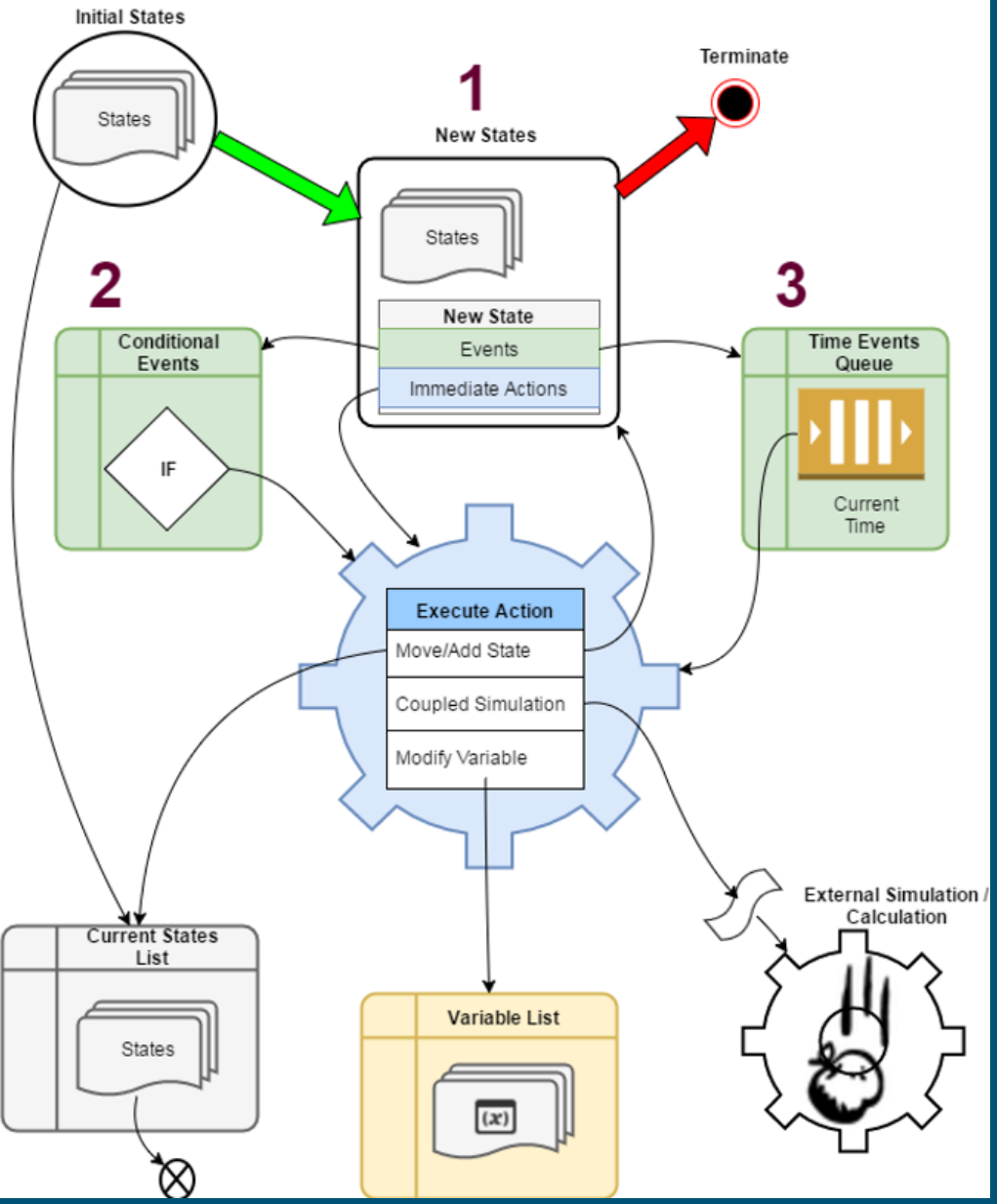
Three-Phase Event Simulation Process

Upon loading, initial start states are added to the “Current” and “New States” list.

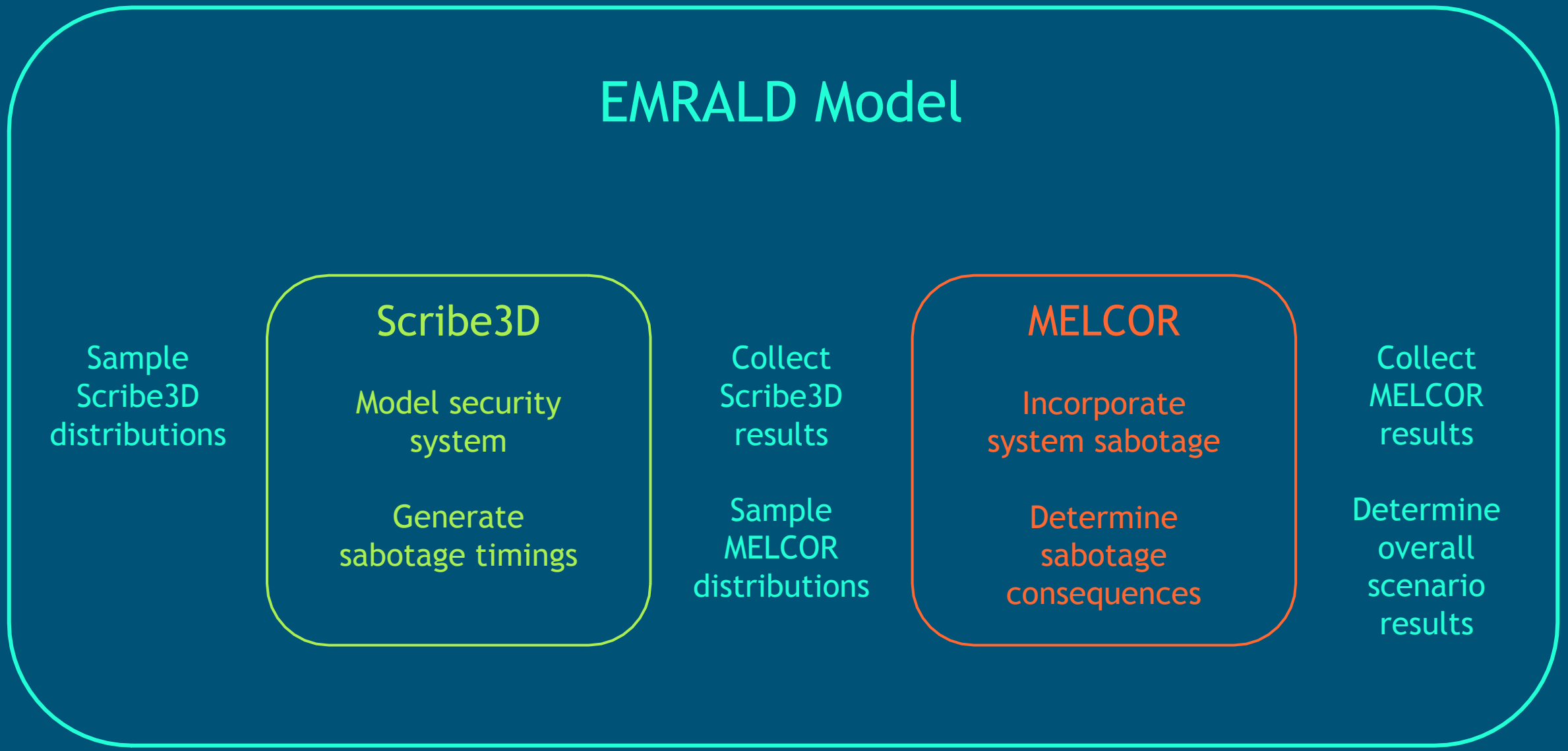
1. While there are states in the “New States” list, For each state:
   - Add the events to the “Time Events Queue” or “Conditional Events” list.
   - Execute any Immediate Actions

2. If any “Conditional Events” criteria is met.
   - Execute that events action/s.
   - Go to Step 1.

3. Jump to the next chronological event.
   - Process that event’s actions.
   - Go to Step 1.



Modeling Structure



Scenario Development

Simple scenario created to test methodology
- Shows dynamics of 2S system

Adversary attacks LPNPP to create short term station blackout

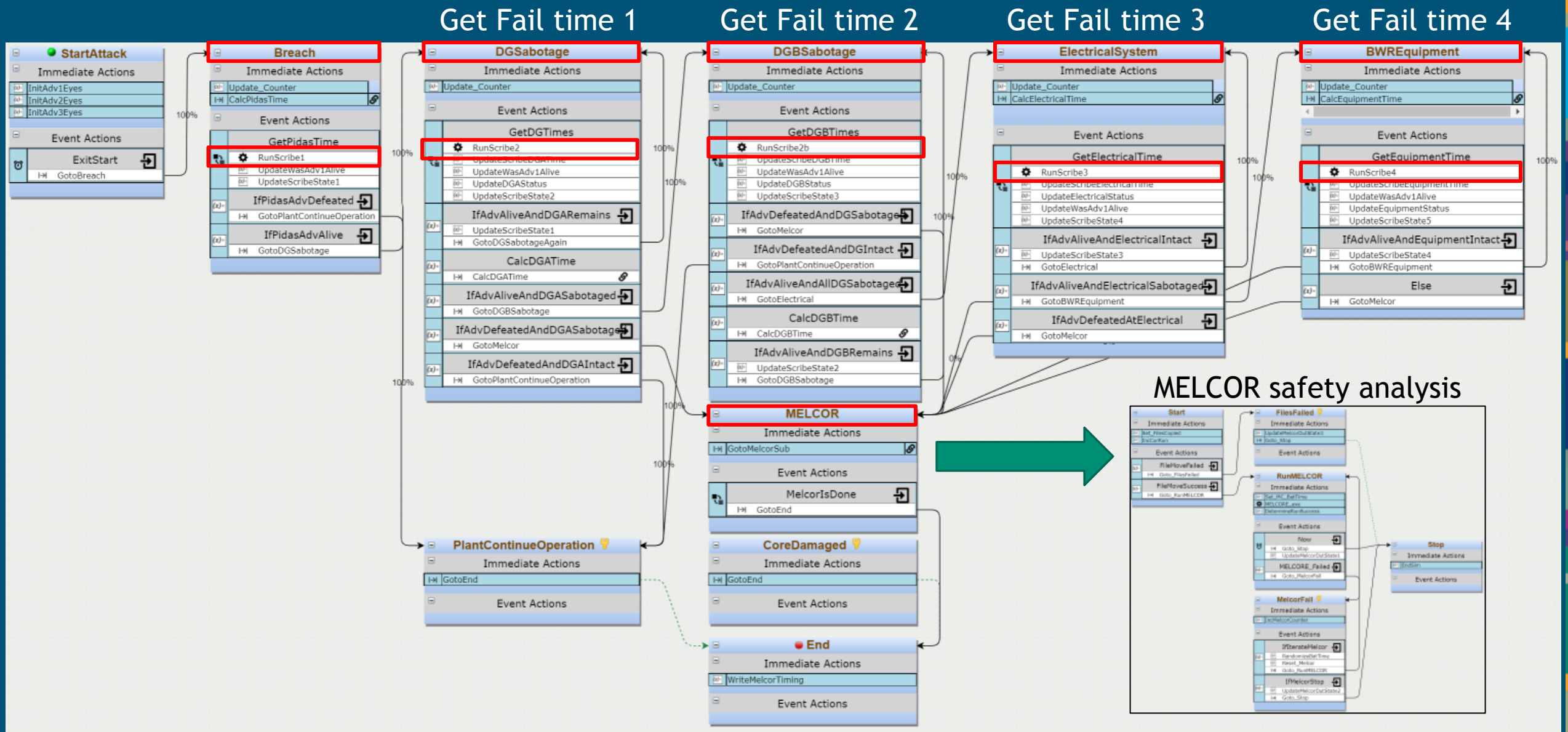
Begins at time t_0 with loss of offsite power

Adversaries disable onsite electrical equipment
- Disable diesel generators
- Disable battery systems

Security system and operator actions not modeled
- Security code used purely to determine adversary timelines

Consequences of attack modeled until core damage

Modeling Structure (EMRALD – SCRIBE 3D)



Uncertainties

Small number of modeled uncertainties

Modeled as distributions in EMRALD

- Breach times
- Sabotage times

Success and failure of breaches were also uncertain

No uncertainties in reactor response

Results

Ran 50 Monte Carlo samples

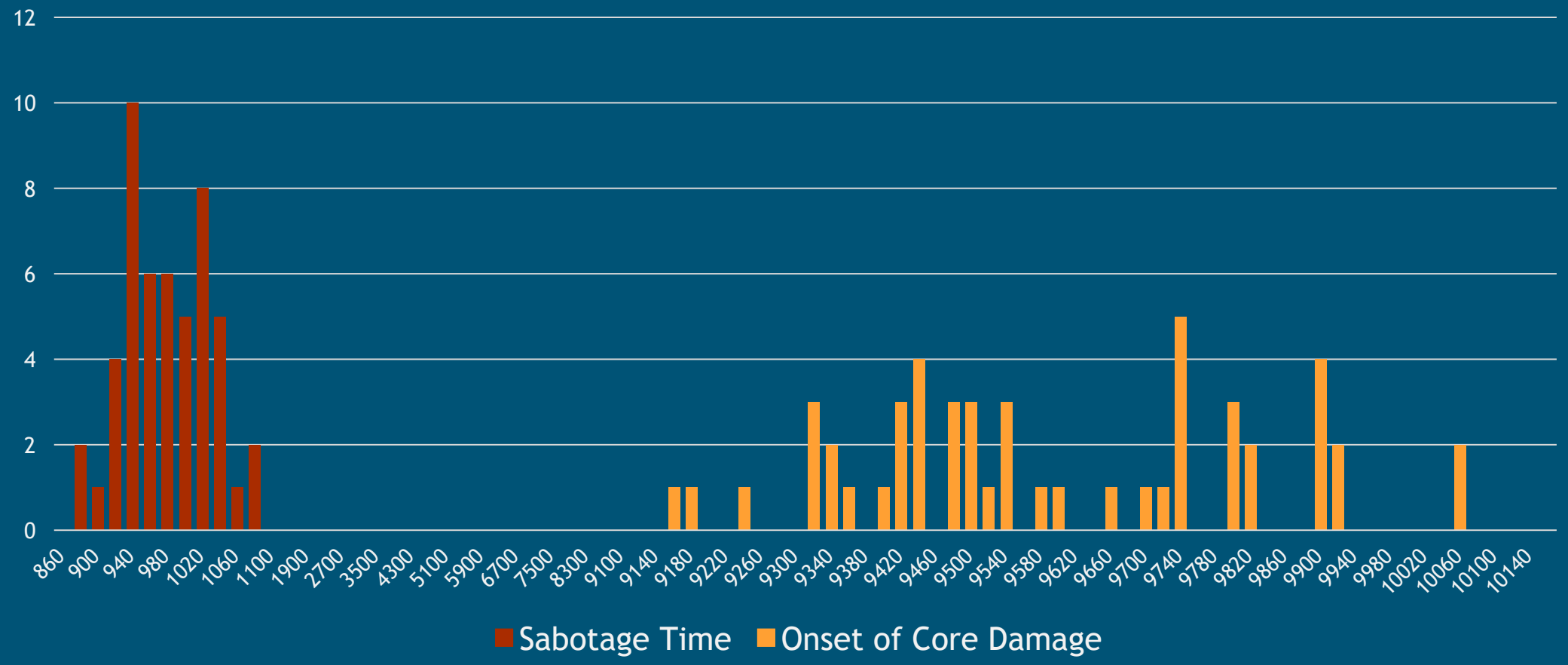
Applied EMRALD safety-security analysis

- Sampled uncertain adversary task times
- Obtained sabotage timing information from Scribe3D
- Applied timing information to MELCOR BWR model
- Collected core damage information in EMRALD

Results are not intended to be representative of existing plants

- Base case of MELCOR model resulted in core damage
- Figure of merit was core damage timing

Results (cont)



EMRALD Modeling/Coupling Evaluation

Benefits

- Drag-n-Drop modeling & visualization
- Can easily model looping vs other dynamic methods
- Could model complex adversary actions/procedures
- Document variables to modify MELCOR model
- Short learning curve

Challenges

- Complex modeling needed to generate a more dynamic behavior in SCRIBE 3D
- Modifying the many SCRIBE 3D variables still needed user scripting
- Needed custom Python script to run MELCOR on servers

QUESTIONS?