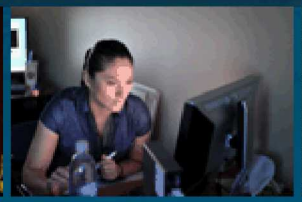
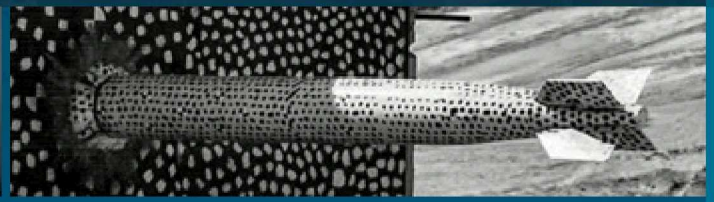
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-4720C

Integrated Safety and Security Dynamic Event Tree Analysis for Nuclear Power Plants





PRESENTED BY

Brian Cohn

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

Vital Area Identification

- Nuclear Power Plants (NPPs) use Vital Area Identification (VAI) to determine plant locations that must be protected from sabotage to protect the reactor core
  - Loss of a vital area results in an unacceptable release of radionuclides from the NPP
- Includes locations where sabotage would directly damage the reactor and secondary locations containing necessary equipment
- Based on Level 1 Probabilistic Risk Analysis
  - Necessitates assuming order of events
  - Otherwise segregated from safety analysis

Nuclear Security Pre-9/11

- Physical security has always been viewed as necessary for nuclear facilities

-VAI began in the 1970s to identify minimum sets of equipment to protect
  - Previously almost all equipment needed protection

- Nuclear plants adopted VAI through the 1980s

- The NRC formally considered implementing VAI in 1999

Post-9/11 Nuclear Security

- 2002 order by NRC for increased security measures
  - Included loss of large area analysis, which required plants to study possible effects of an airplane crash from losing several rooms of equipment
  - General enough to inform effects of fire or explosions
  - Implies value in physically separating trains of safety equipment
- NRC guidance on VAI issued in 2008
  - Acknowledged potential conflicts between safety and physical security
- Evaluated through several methods
  - Timeline Analysis
  - Adversary Sequence Diagrams
  - Force-on-Force tools

Time [s]	Adversary Task	Timely Response Task	Late Response Task
5	Truck crosses PIDAS fence	First detection of adversaries	--
125	Adversary cuts aircraft cable	Notification sent to response forces	--
133	Truck approaches control room wall	--	--
203	Adversaries exit blast radius	Response forces complete preparations	--
204	Bomb detonation	--	First detection of adversaries
274	Adversaries enter auxiliary building	Response forces begin driving to adversary location	Response forces complete preparations
284	Adversaries breach auxiliary control room	Response forces arrive	Response forces begin walking to adversary location
285	Sabotage	--	
300	--	--	Response forces arrive

Methodology

Research Framework

- Dynamic Probabilistic Risk Assessment (DPRA) analyzes the evolution of various scenario paths between initiating events & possible end states
  - A 'bottom-up' technique that statistically evaluates simulation run-based data from deterministic approaches
  - Better accounts for both epistemic (e.g., arising from the model) and aleatory (e.g., stochasticity in the system) uncertainties → higher fidelity analytical conclusions for complex system analysis

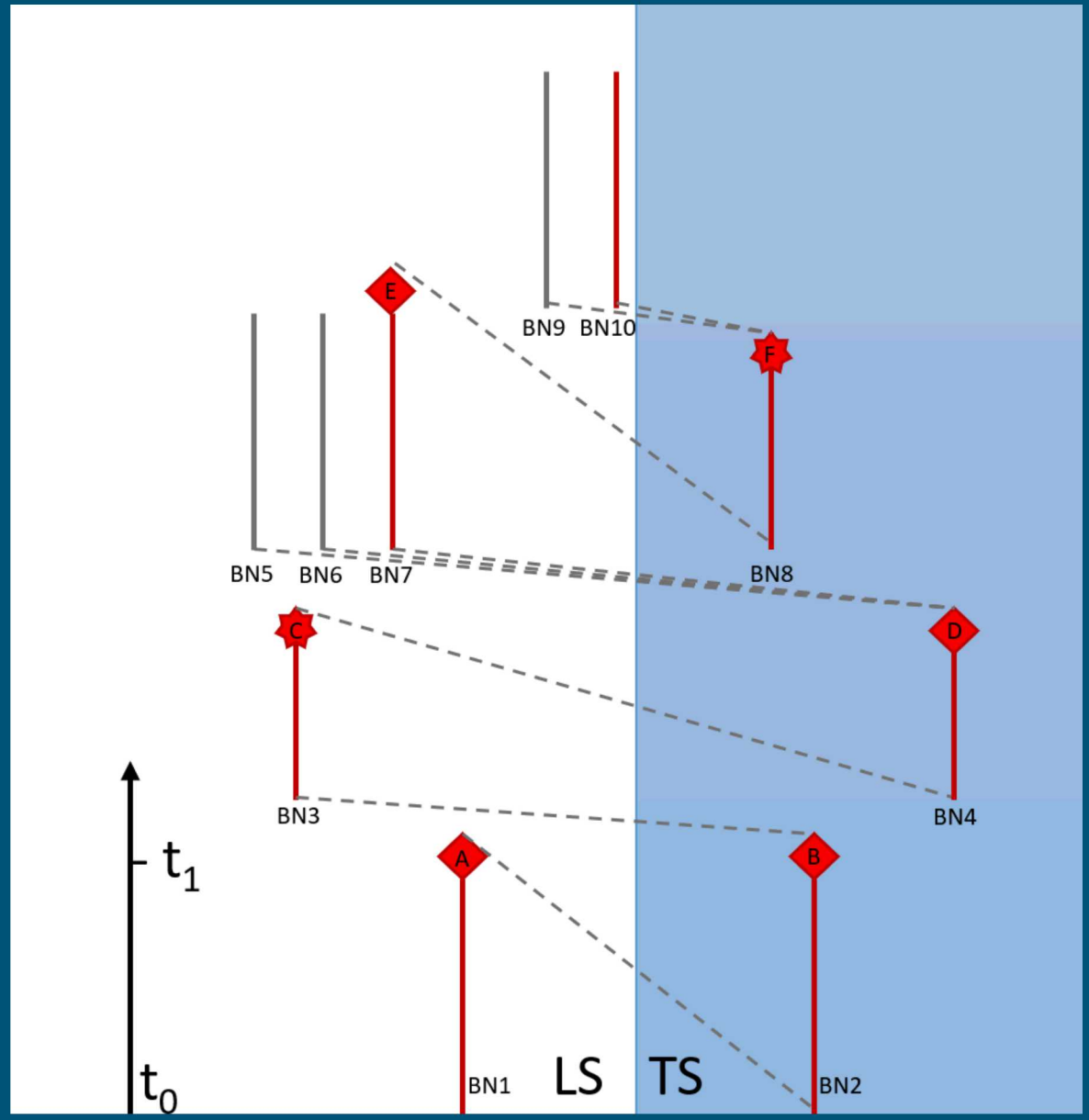
- ADAPT serves as the scenario coordinator and scheduler for the system codes
  - Security Force-on-Force simulation to model damage to and availability of plant safety systems
  - Safety model to determine accident progression and recovery options given sabotage of safety systems

ADAPT

- ADAPT performs Dynamic Event Tree (DET) analysis
- Code agnostic
  - Requires connected system models to:
    - Stop on a preset condition
    - Report stopping condition
    - Save the current system state in a text file
    - Restart on loading a modified save file
- Analysis begins with one instance and splits into daughter branches at points of uncertainty
- Branches based on analyst selected condition
  - Can explicitly include time element
- Recently modified to allow for multiple simulators
  - Cannot currently accommodate two simulators branching at unknown times

Leading Simulator/Trailing Simulator Approach

- Will use a hybrid approach inspired by ADS-IDAC
  - Construct time blocks of approximately 10 minutes
  - Leading Simulator (LS) executes for one time block
    - Include occasional saves during time block
  - Trailing Simulator (TS) executes for the same time block
- If LS identifies a branching point, TS executes until branching time
- If TS identifies branching point, branching occurs immediately
- Create new time block and begin execution with LS



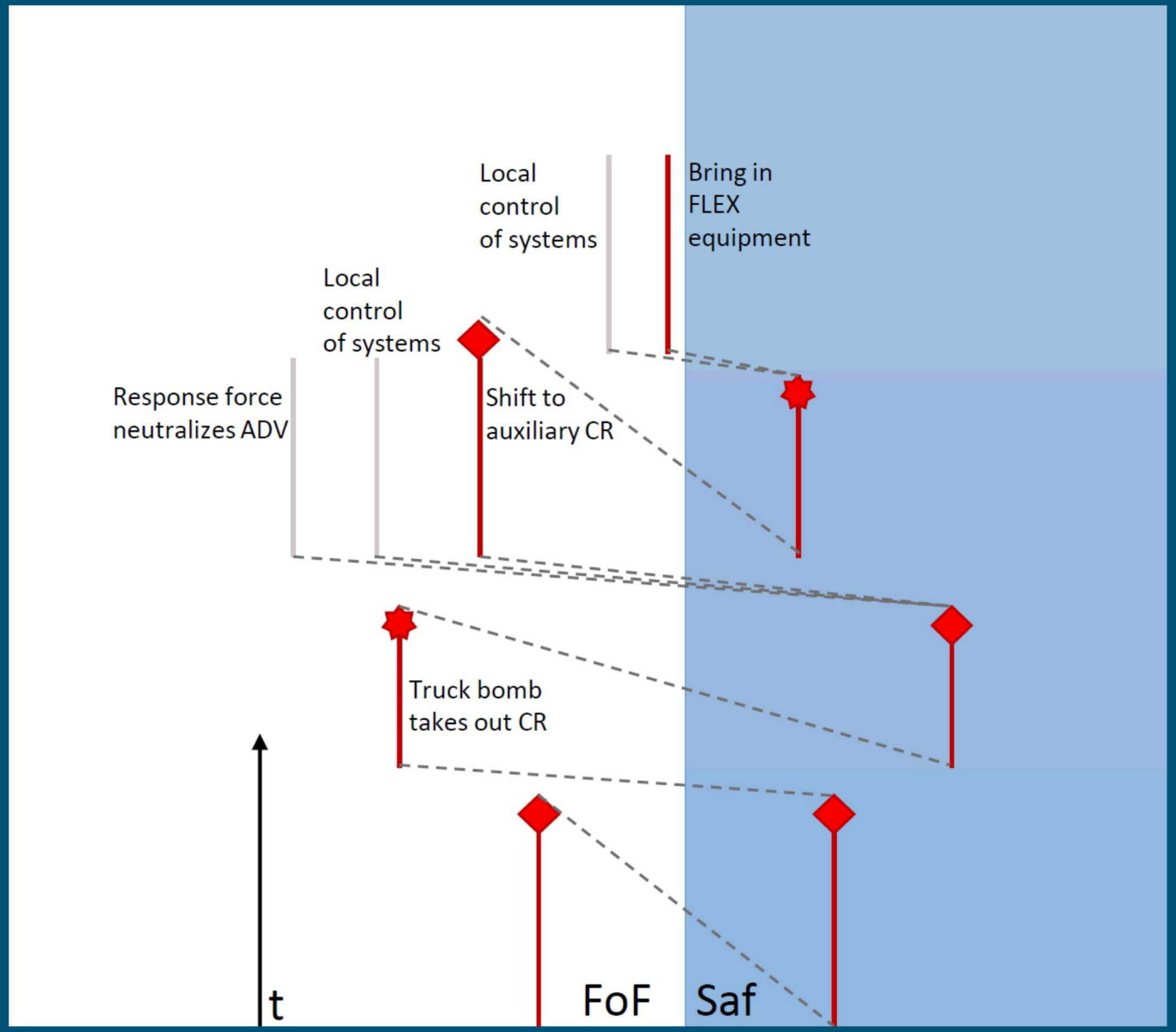
Hypothetical Lone Pine Plant for Case Study

Step	Time [s]	Adversary Task	Timely Response Task
1	5	Truck crosses PIDAS fence	First detection of adversaries
2	125	Adversary cuts aircraft cable	Notification sent to response forces
3	133	Truck approaches control room wall	--
4	203	Adversaries exit blast radius	Response forces complete preparations
5	204	Bomb detonation	--
6	274	Adversaries enter auxiliary building	Response forces begin driving to adversary location
7	284	Adversaries breach auxiliary control room	Response forces arrive
8	285	Sabotage	--

Preliminary Results

Preliminary Results

- Scenarios are encoded in the DET structure
- On uncertainties in either model, branch and return to the LS
- Representation shifts to best estimate plus uncertainties
  - Minimization of conservative assumptions



Conclusions

- Safety assessments challenge the current assumption that loss of vital areas results in unacceptable releases of radionuclides
  - Safety procedures and equipment used to mitigate severe accidents at NPPs (e.g. FLEX) can mitigate sabotage

- The inability of security assessment to fully capture safety strategies represents a gap in capabilities
  - Tying level 2 probabilistic risk assessment to security supports the IAEA objective of mitigating the effects of successful sabotage

- Integrating safety and security assessments allows for changes to both safety and security procedures to drive down systemwide risk, capturing effects based on safety/security interactions while reducing assumptions

Questions?

bcohn@sandia.gov