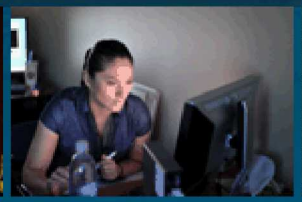
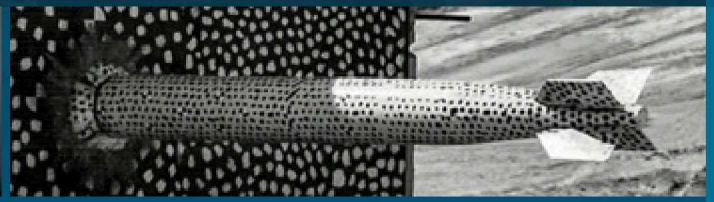
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2020-0444C

Using Reactor Simulations to Improve Security Analysis





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.

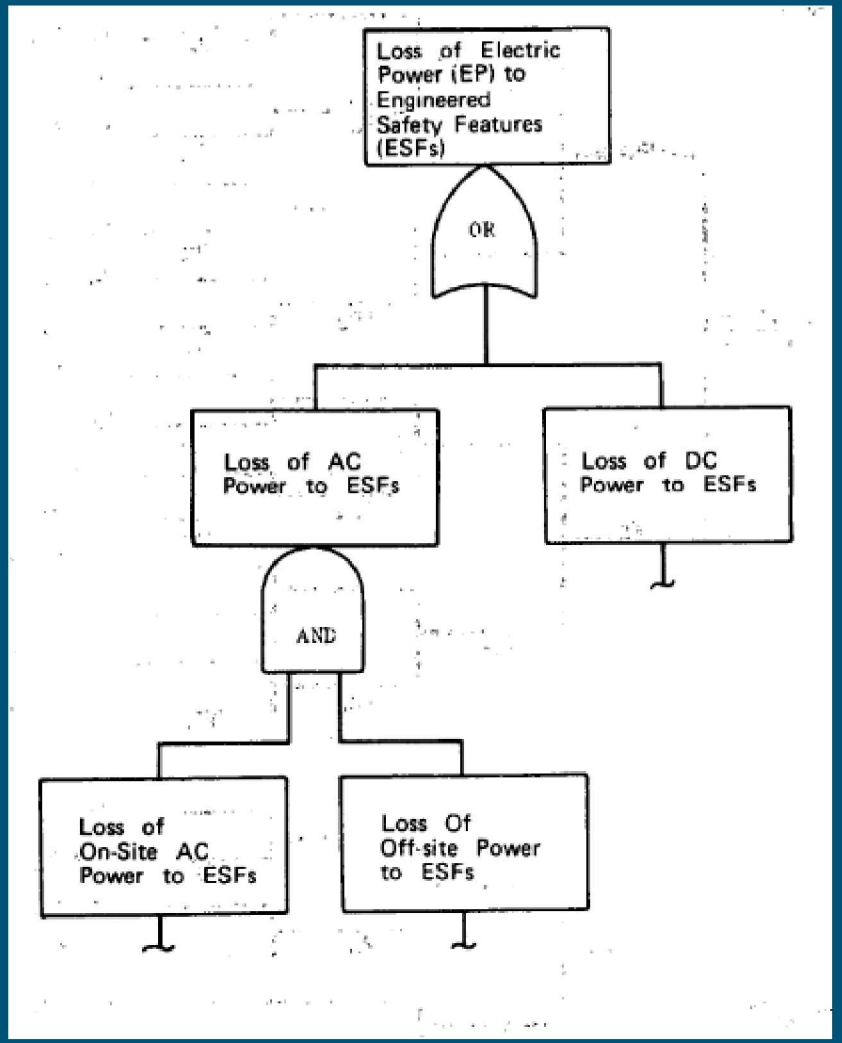
History of Security Analysis

Development of Fault Tree Analysis

Fault trees were first used for nuclear power plants with the Reactor Safety Study, or WASH-1400

Safety assessment of nuclear plants which formulated link between individual component failures and loss of major systems

Protection of a plant is accomplished by maintaining enough equipment to prevent any complete failure pathway to reactor damage



Example fault tree from WASH-1400

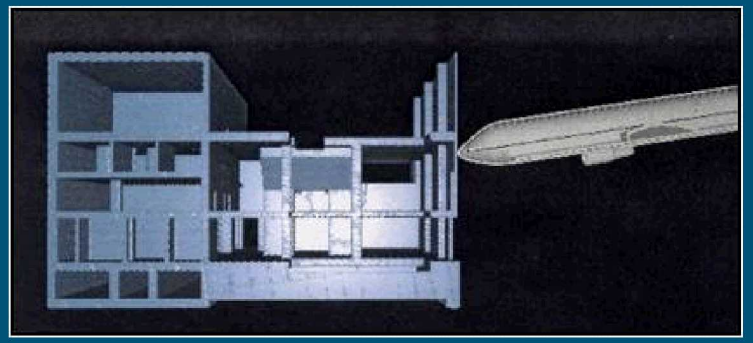
Application to Security Analysis

Regulations charged nuclear plants to protect all vital equipment from sabotage

- *[A]ny equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation.*

Fault trees provide a way for nuclear plants to distinguish vital equipment and vital areas from other safety equipment

Goal is to protect one minimal set of equipment for the plant in event of adversary attack



Vital Area Identification

1. Determine inventories of nuclear material with sabotage concern;
2. Evaluate direct dispersal as a potential risk;
3. Identify initiating events which can lead to radiological release and systems required for mitigation of events;
4. Construct adversary logic model to determine combinations of events which could lead to core damage;
5. Eliminate events that the design basis threat adversaries are unable to perform;
6. Identify locations within the plant that the remaining events can be performed in and replace the events with their corresponding areas;
7. Solve the tree to identify minimum target sets of areas that could lead to successful radiological sabotage;
8. Find the Boolean complement of the target areas to produce candidate vital area sets;
9. Select the vital area set that is most advantageous to protect.

Limitations of Vital Area Identification

Vital areas identify areas to protect, not the effects of losing those areas
- Assumes all areas not protected are lost

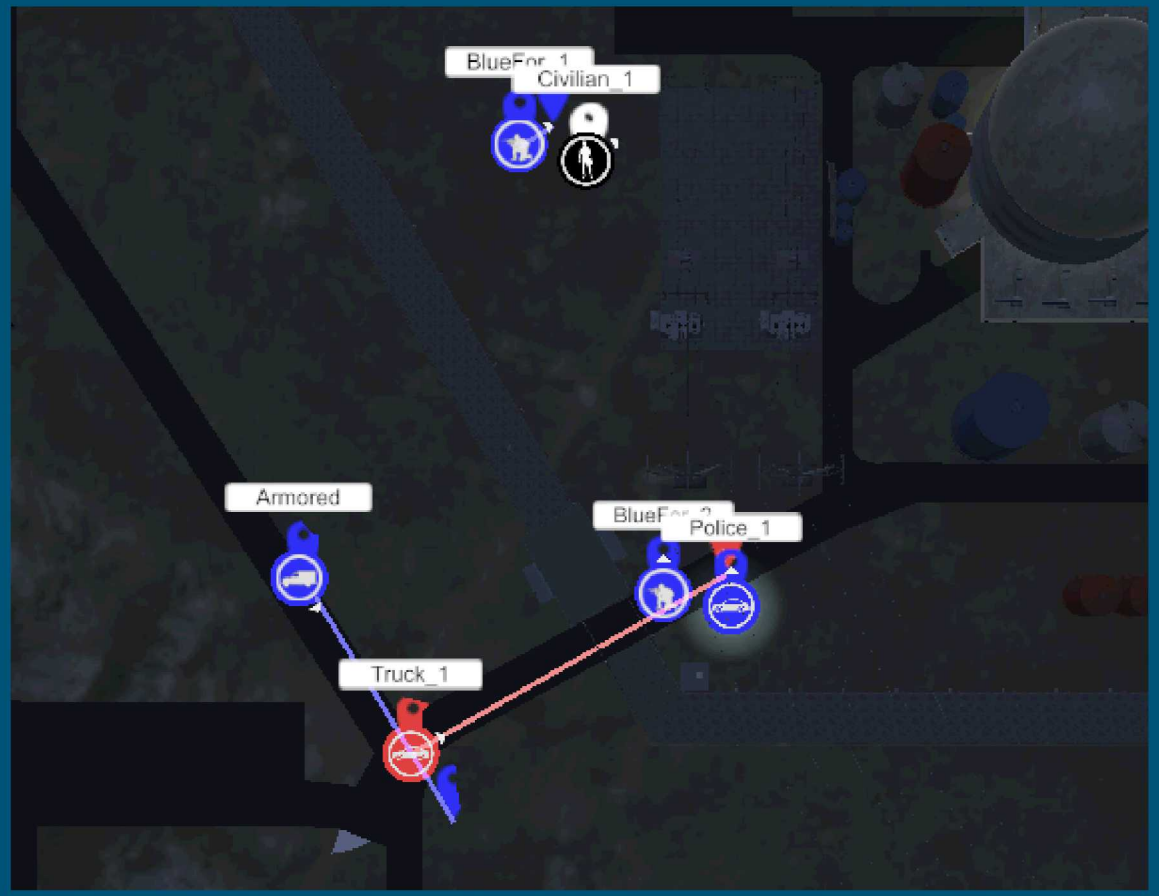
The fault trees are built for a full power state and preclude actions taken by operators
- Reducing power can change the systems needed by the plant

Current PRAs are static
- Unable to include repair actions or implementation of FLEX
- A temporary loss of vital equipment may be recoverable

Performance testing of security is limited to preventing access to limited areas
- Sabotage of one vital area is assumed to cause the immediate loss of the reactor

Simulation Tools

Security Simulations



Simulations model the effectiveness of security postures at nuclear plants

Includes adversary scenarios, timelines and probability of success

Simulations generally end after defeat of adversaries or successful sabotage

Simulation tools

- Avert
- Simajin
- Scribe3D

Safety Simulations

High fidelity modeling captures the effects of losing combinations of systems

Dynamic analysis – timing and order are captured

Can be headless or human-in-the-loop

- Headless can run many times to capture uncertainties
- Human-in-the-loop integrates operator actions with the system response

Common codes:

- MELCOR
- MAAP

Fukushima Daiichi Unit 1-4
Courtesy of TEPCO

Integrating Security with Safety

Security and safety models each model part of the problem

- Security models determine which systems are lost and when
- Safety models predict the effects of those system losses

Integrated safety-security analysis may capture events from initial intrusion through radionuclide release

Requires combining safety analysis with security analysis

- Helps promote communication between otherwise separate departments

Development of Hypothetical Reactor – Lone Pine Nuclear Power Plant

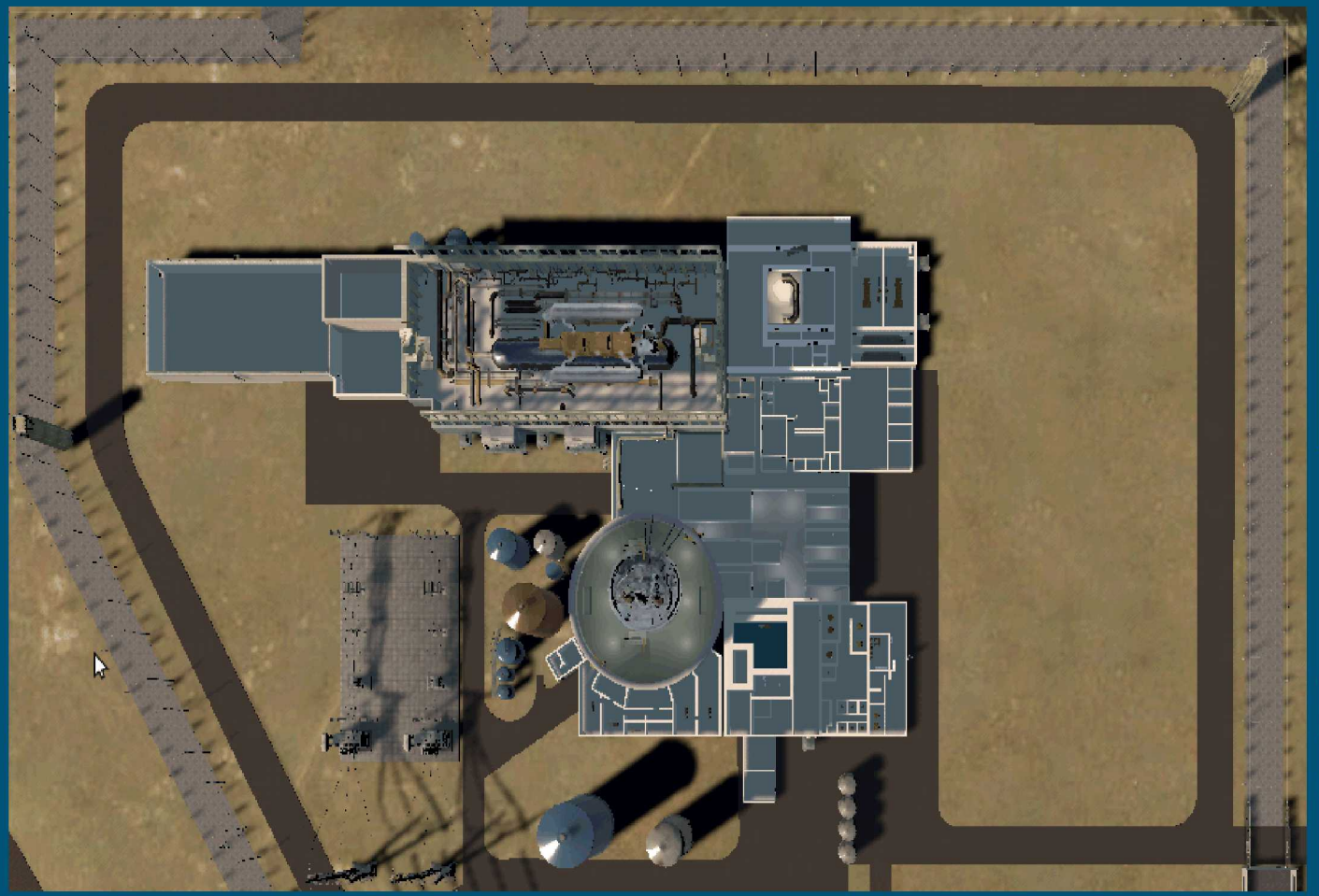
The security posture of nuclear plants is restricted information

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

For many years, Sandia has trained international audiences on nuclear security best practices

Sandia has developed a hybrid PWR for security training purposes

- Includes artificial vulnerabilities
- Created from multiple separate PWR designs
- Includes all major systems and rooms, including FLEX equipment



Scenario Overview

Scenario development remains based on current practice

- Security experts know how to create adversarial attacks
- Safety experts know how to propagate damage through plants

Combining analyses in dynamic models allows uncertainties to be included in analysis

- Single point estimates can be replaced by statistically-defensible distributions

Currently creating demonstration case study involving attack on auxiliary feedwater systems

- Timing of detection
- Timing of sabotage
- Mitigating operator actions
- Application of FLEX

Expected Results

Combining safety and security allows results to extend beyond initial sabotage

- Existing safety systems are able to compensate for many forms of sabotage

Attack scenarios can be systematically investigated

- Models determine the presence of uncertainties or decision points in a scenario
- Identification of scenarios for security and reactor operator training

Connection method is code-agnostic

- Can be used with industry-preferred security and reactor models
- Same methodology can be used with NRC models to provide independent assessment