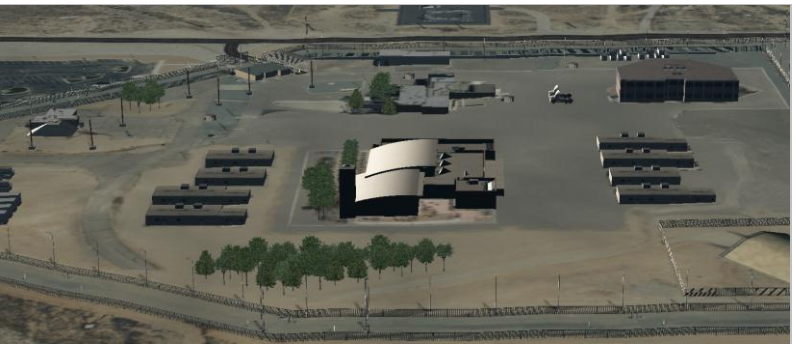
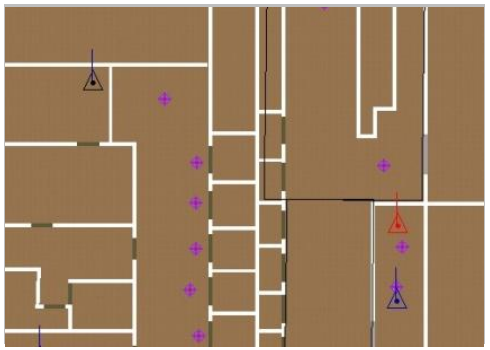
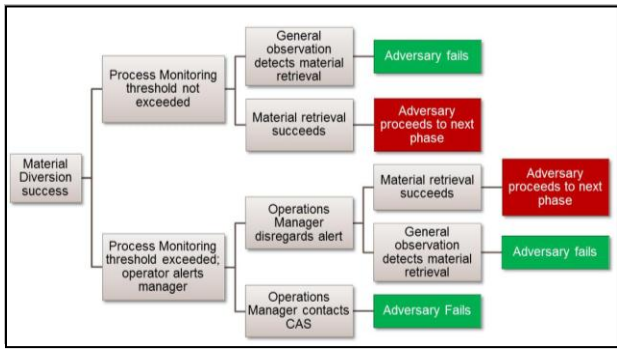
SAND2012-8024C

Exceptional service in the national interest

Sandia National Laboratories







Addressing the Facility Safeguards Interface for the Insider Threat

Felicia A. Durán, Ph.D.

Co-Authors: Dean Dominguez, Jordan Parks, Rebecca Ward, Ivan Lozano, Yaxi Liu, and Ben Cipiti

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Introduction

- Modeling and Simulation for Insider Scenarios
- Overview of Presagis Software
- Insider Simulation Modeling
  - Proof of Concept – Item Theft
  - Process Facility
- Insights for Facility Operation
- Future Efforts

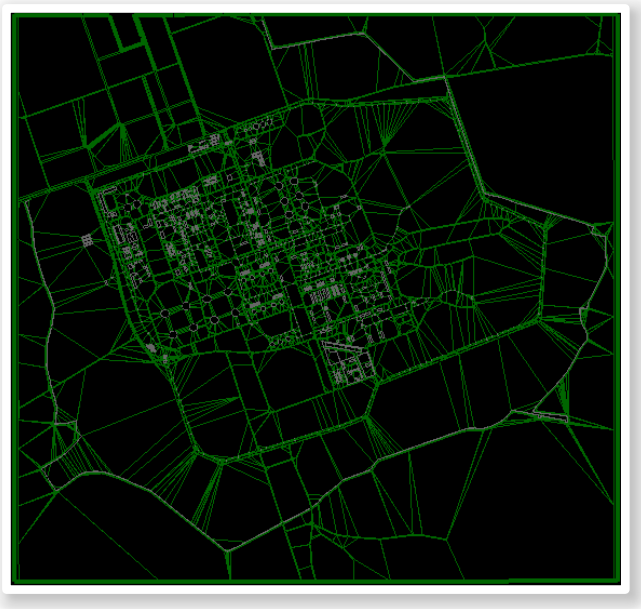
Presagis Software Overview

STAGE

Creator Pro

AI.implant

VAPS XT

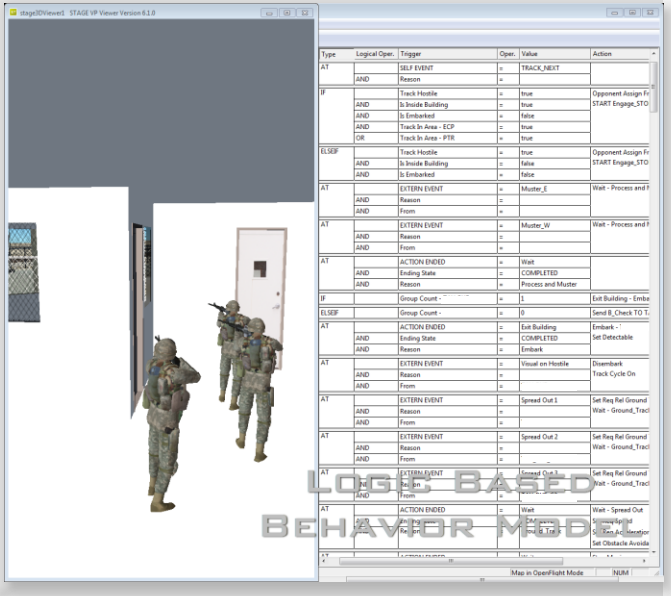


STAGE – Applications

Sandia National Laboratories

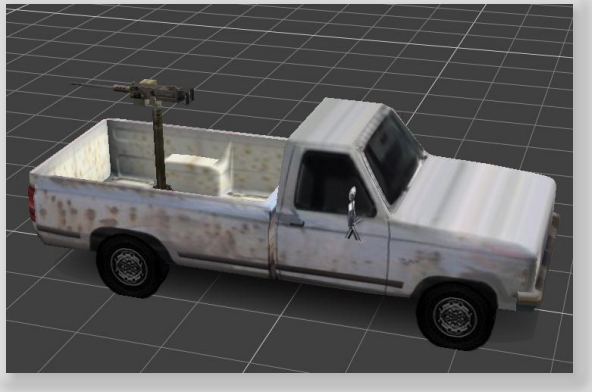
Capabilities

- Logic Based Behavior Model
- Ground Navigation – Dynamic Path Planning
- Probability-based Combat Model
- Performance-based Databases
- Batch Mode
- Road Networks
- Explosives
- 3D Environment
- Federation



Analysis Applications

- Single Analyst Tool
- Physical Protection System (PPS)
- Detection, Delay, & Response
- Command and Control (C2)
- Situational Awareness
- Alarm C&D
- Expert Input
- Design Basis Threat
- Insider
- Probability of Neutralization/ Risk Reduction

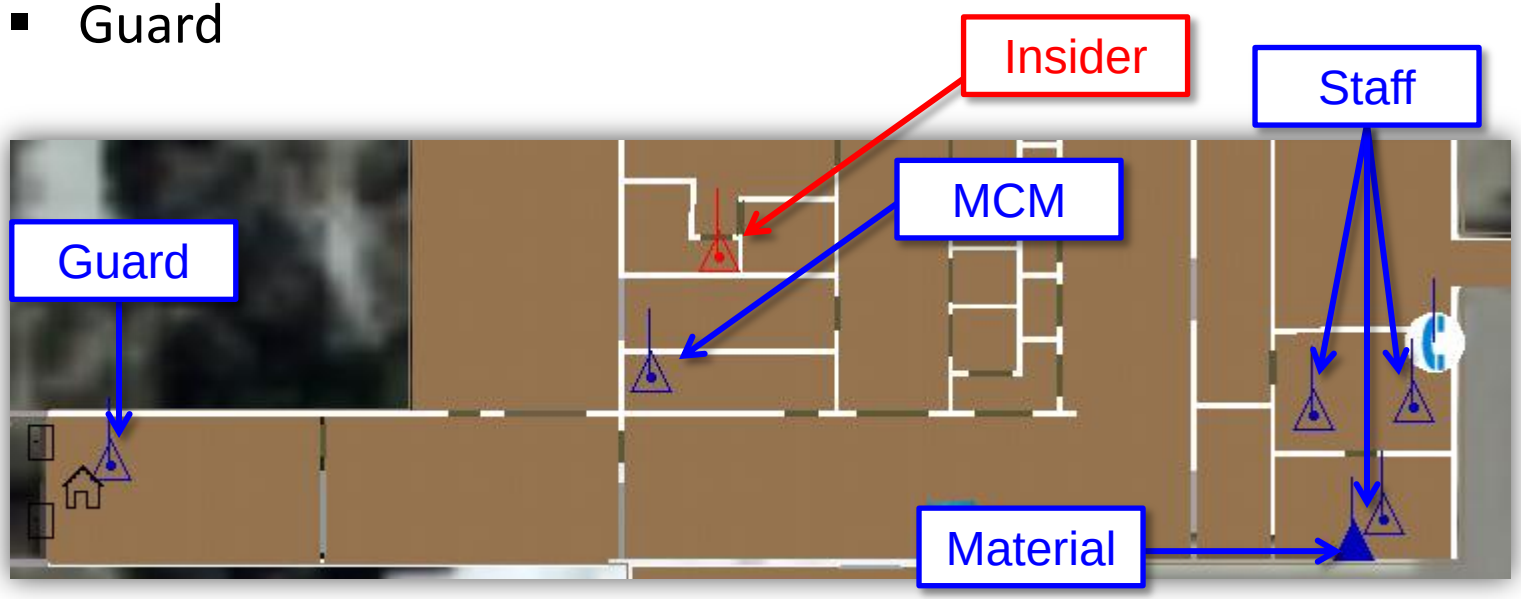


Insider Scenario – Proof-of-Concept

- "Force-on-Force" approach for facility response to insider threats
  - Blue Team – Facility protections (equipment, people, operations)
  - Red Team – Malicious Insider Adversary
- Item Theft
  - A non-violent Insider attempts to remove material from a vault (Phase I)
  - Then transport material offsite (Phase II)
  - Facility staff provide general observation
  - Various administrative checks (material control and accounting MC&A) to prevent theft
- Stage Capabilities Demonstrated
  - Process Modeling
  - Complex behavior
  - Administrative Procedures
  - Random event generation

Facility Overview

- Two-Story Processing Facility
- Two-Room vault Containing Target material
- Six Employees
  - Insider
  - Material Control Manager (MCM)
  - Three Staff members
  - Guard



Blue Team

Blue Team Member	Responsibilities
MCM	General observation in processing facility vault Conducts routine MC&A activity (shift check)
Staff Members	General Observation as they go about daily business
Facility Guard	Conducts inspections as employees process out of the facility
CAS operator	Receives communications from MCM and dispatches response forces
Roving patrol	Responds to anomaly at processing facility as directed by CAS
Backup patrol	Secures ECP as directed by CAS Conducts random inspections on exit

Material Control & Accountability (MC&A)

Sandia National Laboratories

- Operations and administrative procedures which track and account for critical assets, for example
  - Material measurement
  - Inventory audits
- MC&A in our model
  - Based on human reliability modeling for nuclear power plant operations
  - Recurring procedures and actions done by staff are incorporated into theft prevention and detection schemes
  - Many recurring opportunities to observe and detect any anomalies in the operational environment

Human Reliability Analysis (HRA) and Dependence of Recurring MC&A Activities

Sandia National Laboratories

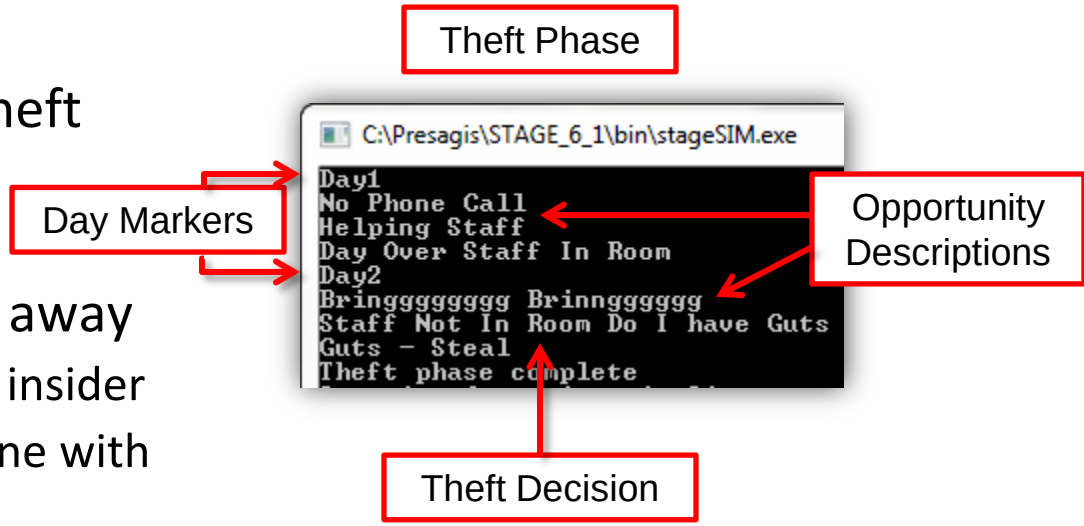
- MC&A activities depend significantly on human performance
- HRA models estimate the probability of human error in performing operations
  - Recurring operations can cause a degradation in performance
  - Considers how previous task failures or successes affect future task performance
- Dependence model is used to model performance of MC&A activities for the process operator

Red Team

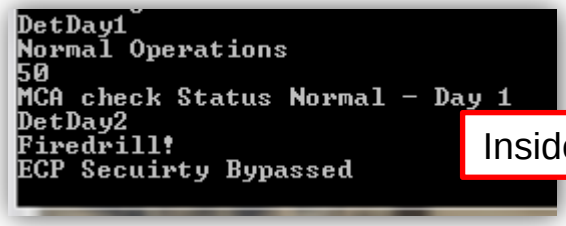
- Adversary acts alone
- Has access to target material and facility knowledge
  - PPS measures
  - MC&A Adminstrative Checks
  - Emergency Drill Schedule
- Non-Violent (will surrender if confronted)
  - Will attempt to remove material undetected

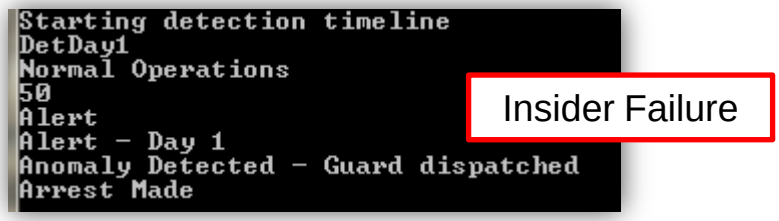
Insider Timeline

- Ten day theft period
  - Each day represents a theft opportunity
  - Phone call or staff consultation pulls MCM away
    - Theft decision point for insider
    - Will only steal if left alone with material



Extraction Phase

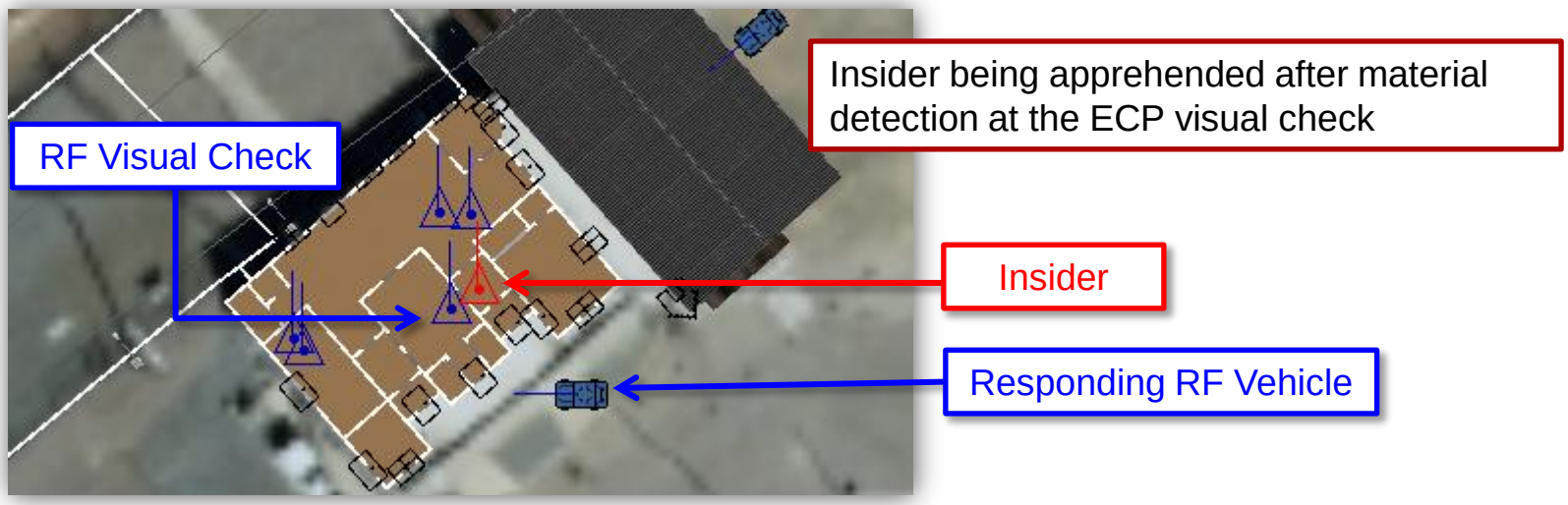




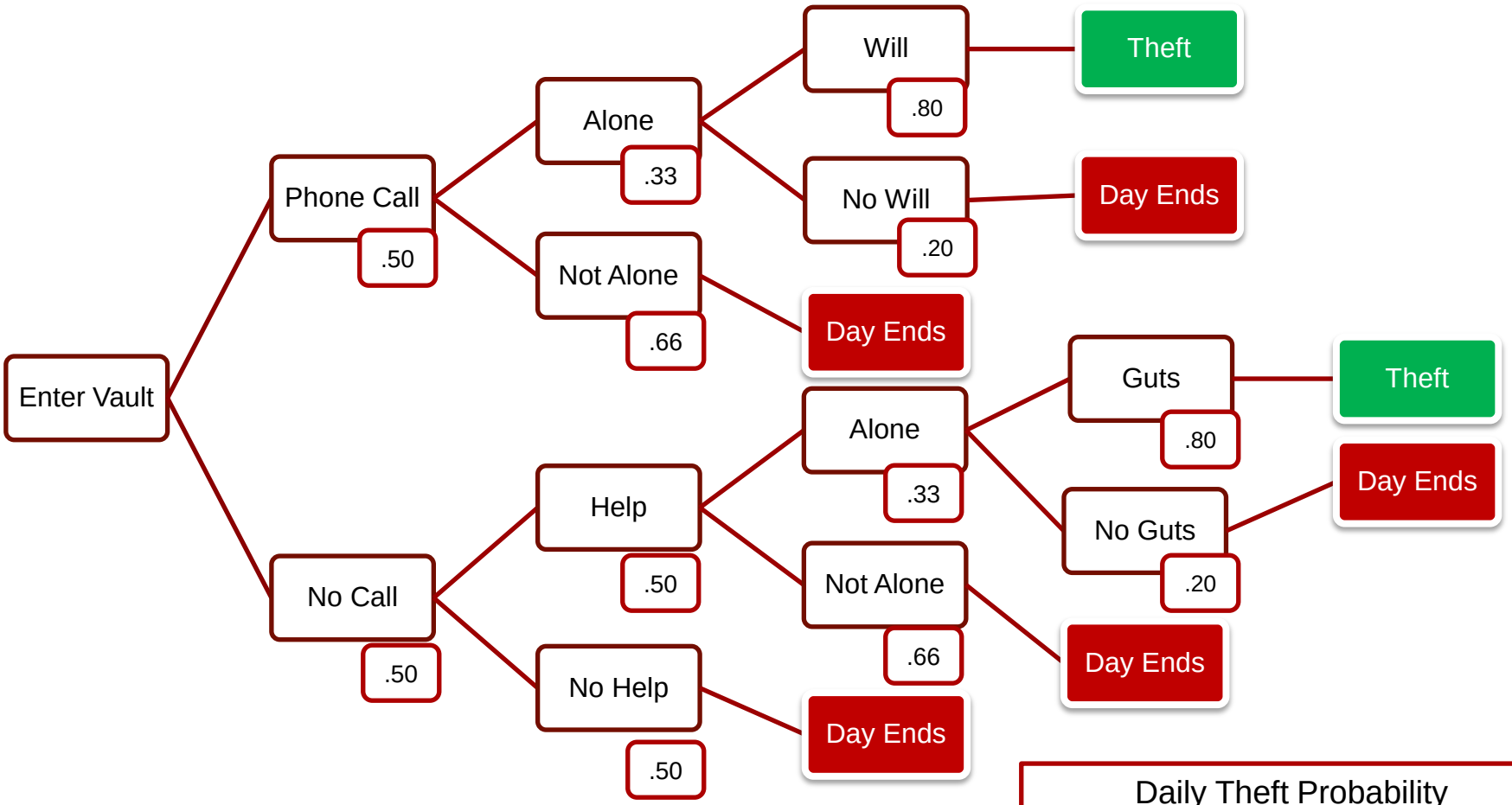
- Ten day escape period
  - Each day represents an opportunity to remove material
  - Fire drill allows insider to bypass one visual check and attempt to remove material

Response Force (RF) Timeline

- Two opportunities to detect theft
  - MC&A check at the Processing Facility
  - Visual Inspection at the ECP
- If anomalies are detached a guard is dispatched to apprehend the insider



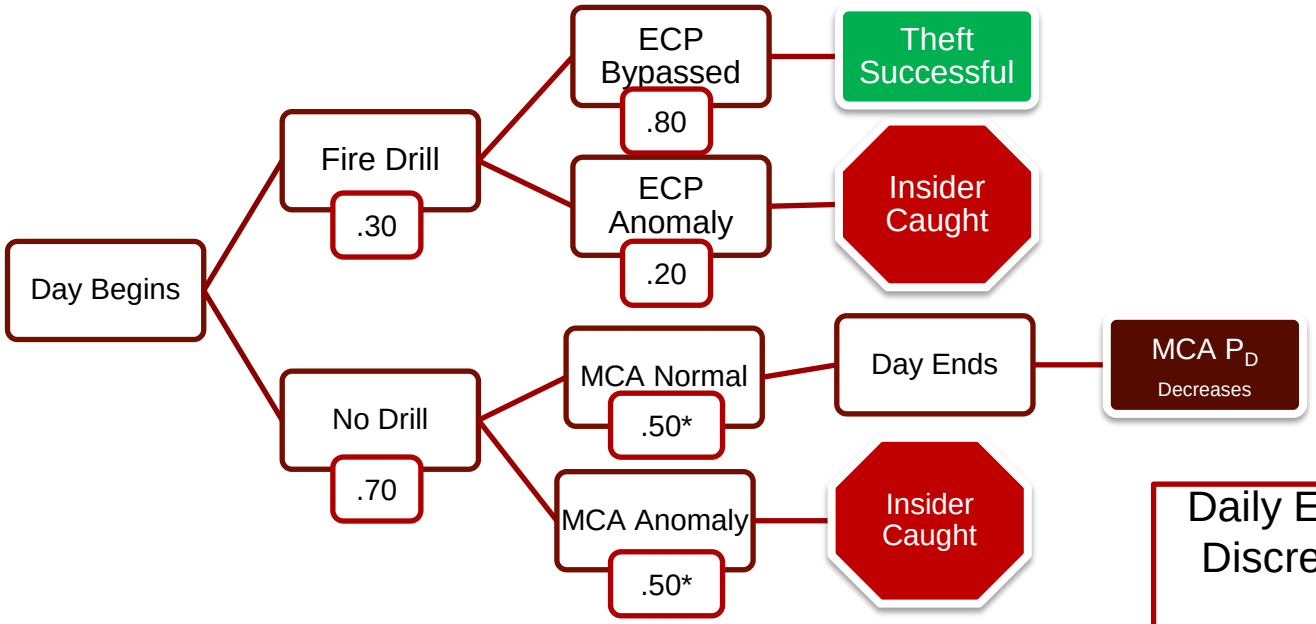
Theft Phase Decision Tree



Daily Theft Probability

Theft	~0.20
No Theft	~0.80

Extraction Phase Decision Tree



*MCA check P_D diminishes 5% daily

Daily Extraction Phase Discrete Probabilities (Approx.)

	Day Ends	Escape	Apprehended
Day1	0.35	0.24	0.41
Day2	0.385	0.24	0.375
Day3	0.42	0.24	0.34
Day4	0.455	0.24	0.305
Day5	0.49	0.24	0.27
Day6	0.525	0.24	0.235
Day7	0.56	0.24	0.2
Day8	0.595	0.24	0.165
Day9	0.63	0.24	0.13
Day10	0.665	0.24	0.095

Insider Scenario – Process Facility

Sandia National Laboratories

- Electrochemical processing plant – a technology for recycling metal or oxide spent nuclear fuels
  - Key operations in the process include:
    - Spent fuel Chopping
    - Electrolytic Reduction
    - Electrorefining
    - Uranium and Uranium/Transuranic Mixture Processing
- Integrated monitoring system
  - Physical Protection System (PPS)
  - Process Monitoring
  - Material Control & Accountability (MC&A)
  - Human Reliability Analysis (HRA)

Our Model Environment

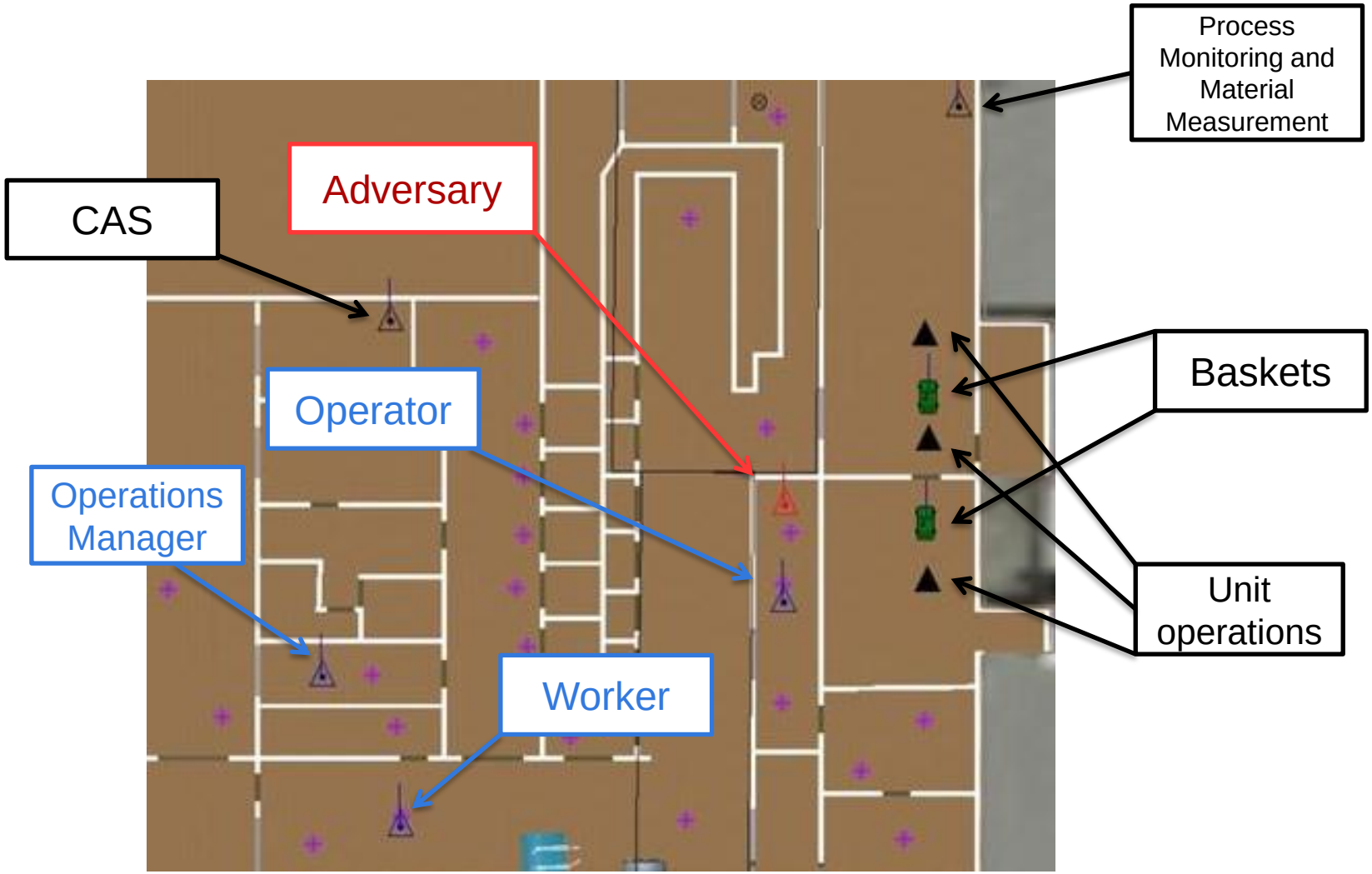
Sandia National Laboratories

Integrated Protection System

Sandia National Laboratories

- Physical Protection Elements
  - Inner and outer perimeter fence
  - Microwave sensors along the perimeter
  - Guard patrols around the facility
  - Personnel Entry Control staffed with guards
  - Radiation sensors at facility entrance and exit
- Process Monitoring
  - Mass flow tracking at each operation in the processing cycle
  - Cumulative mass accounting to detect both abrupt and protracted material diversion
  - Built in thresholds prevents false alarms due to random measurement error
  - Automatic reporting when abnormality is found

Scenario Entities



Scenario Entities

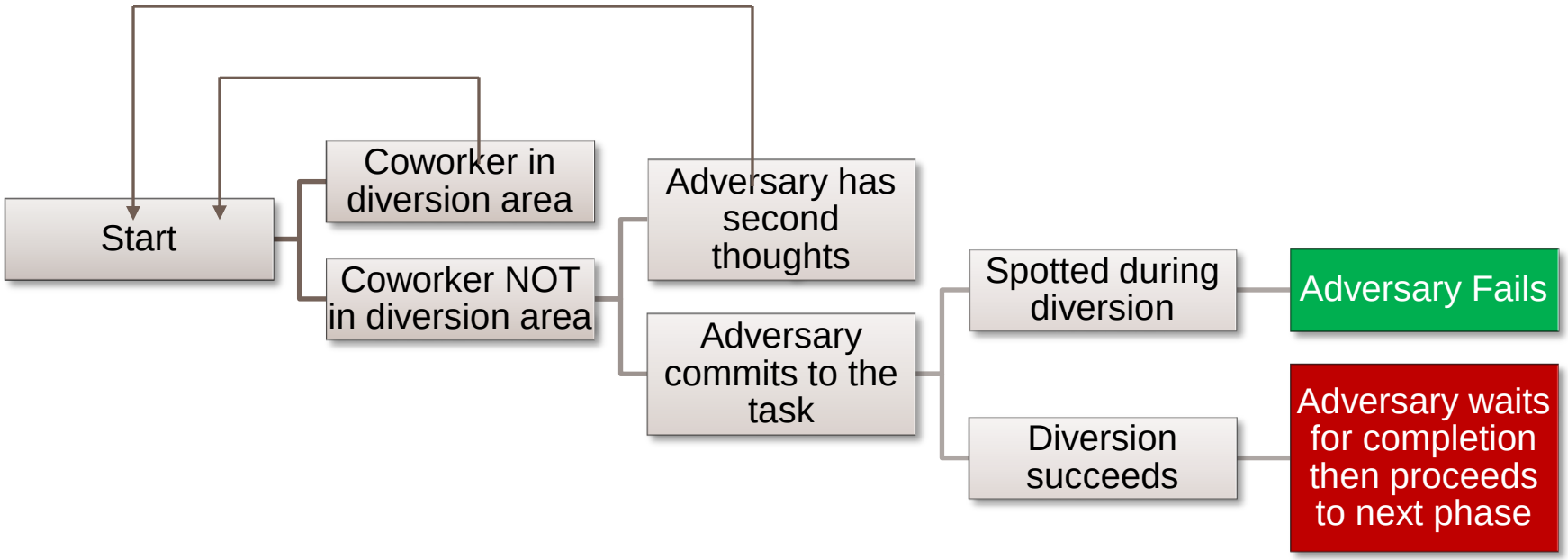
Blue Team Entities	Responsibilities
Guards (x4)	Patrol the outside of the facility looking for suspicious activity
Worker	Works around the facility, can provide visual observation of activities and operations
Operator	Manages and monitors processing operations
Operations Manager	Checks process monitoring and material measurement alarms
Central Alarm Station	Coordinates the guards and handles alarms
Process Monitoring and Material Measurement	Keeps track of mass flows for material in the processing operation

Material Diversion Scenario

Sandia National Laboratories

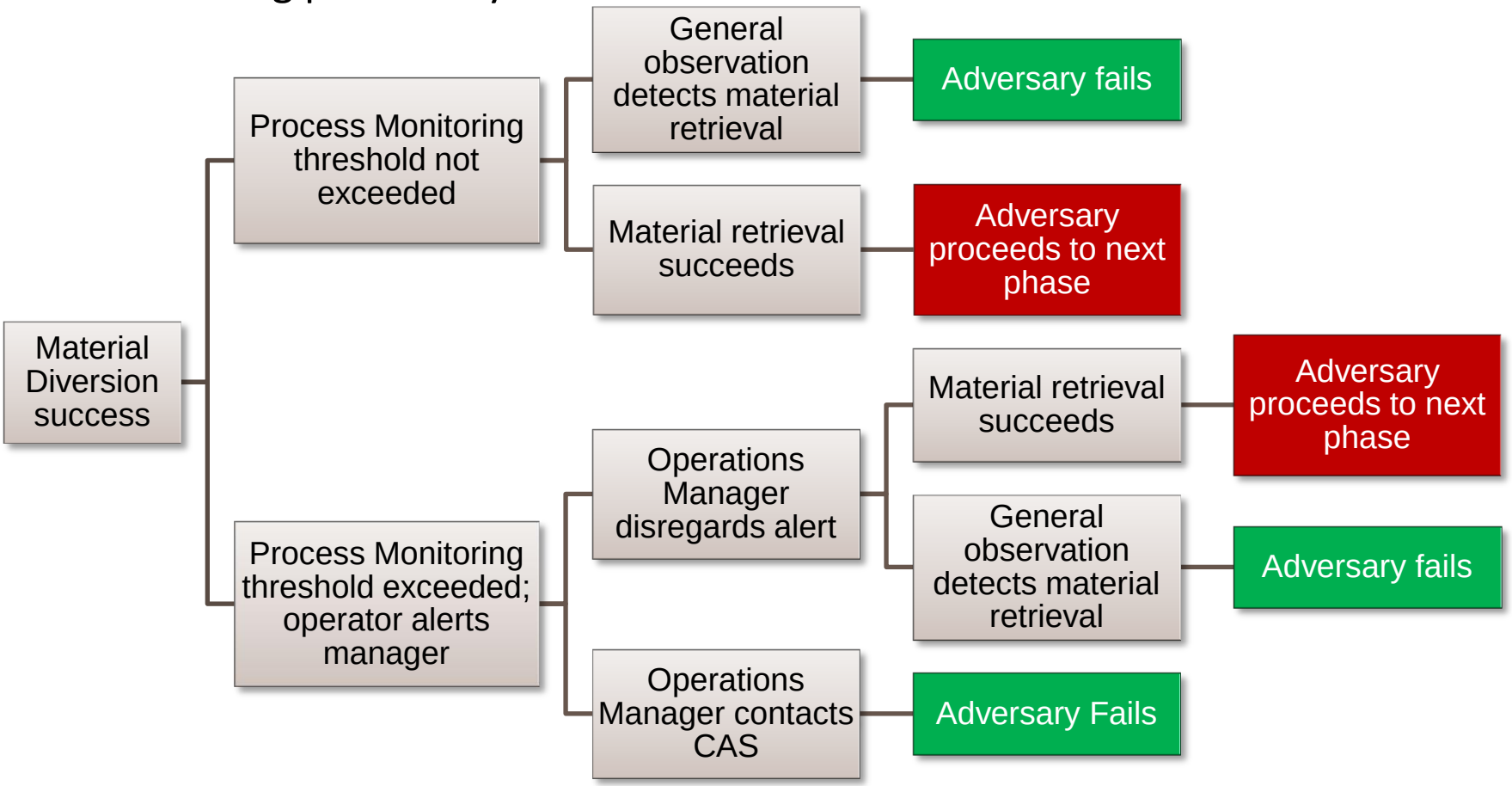
- Each day, a rail car delivers spent fuel assemblies to
- Process is modeled as unit operations which take input and output at some efficiency after set period of time
- Material Diversion Phase
  - Adversary begins by attempting to start a previously installed diversion mechanism
- Material Retrieval Phase
  - When container is filled, the adversary moves to retrieve it and bring it to an interim location
- Material Extraction Phase
  - Each day the adversary then attempts to leave container on a rail car and exiting the facility undetected

Event Tree – Material Diversion Phase



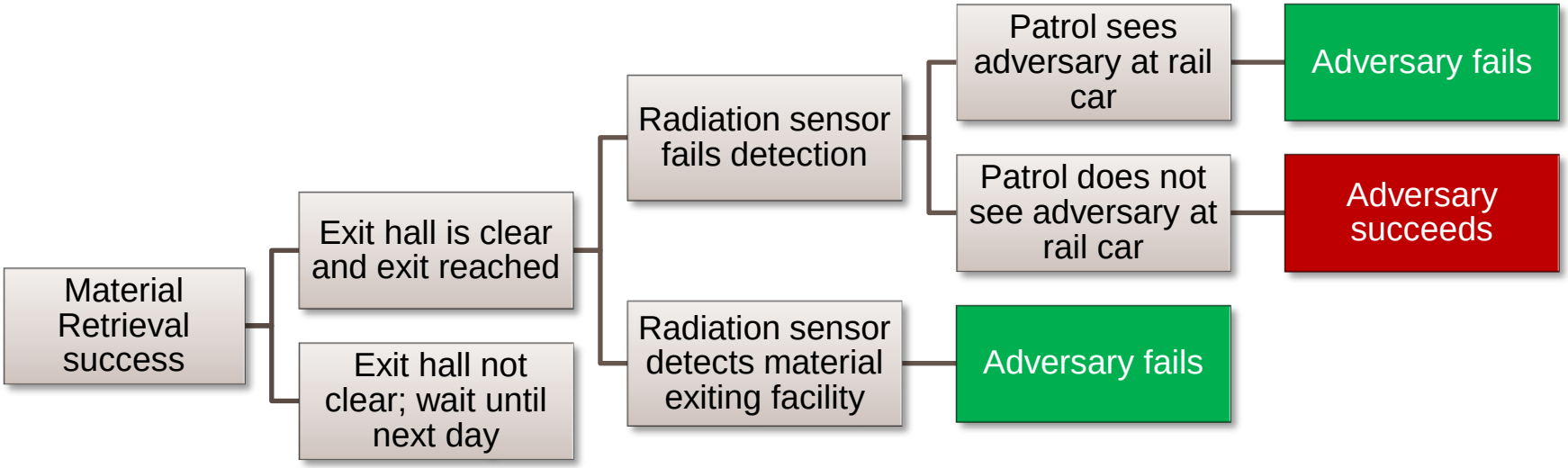
Event Tree – Material Retrieval Phase

- The blue operator can possibly detect the diversion once a day with diminishing probability



Event Tree – Material Extraction Phase

- The blue operator can possibly detect the diversion once a day with diminishing probability



Insights for Facility Operations

Sandia National Laboratories

- Insider simulation modeling for insider adversary using “force-on-force” approach
- Modeling/simulation of facility operations including integrated process monitoring, material measurement, MC&A procedures and physical security
- Flexible framework for additional efforts
  - Continue development of additional scenarios and use of additional STAGE capabilities
    - Issues with process modeling
  - Explore different operational approaches
    - Characteristics of integrated protection systems
    - Visualization of adversary behavior and facility operations
  - Deepen understanding of facility operations, systems integration and interfaces

Future Efforts

Sandia National Laboratories

- Increase levels of process fidelity and complexity in behavior of entities (both Insider and Response)
- Expand number of MC&A procedures and integration of procedures with process monitoring and PPS
- Combine modeling and simulation with other training activities at the demonstration facility

3D Scenario View