# Security Modeling and Simulation to Address the Insider Threat

**F.A. Durán, D. Dominguez, M.J. Parks, and B.B. Cipiti**

SAND2013-5211C

Sandia National Laboratories, P.O. Box 5800 MS-0757, Albuquerque, New Mexico, 87185-0757 USA

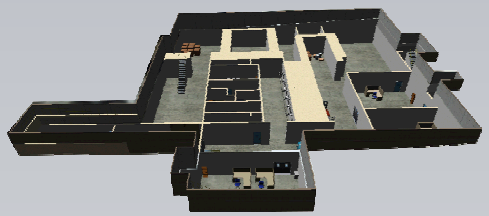
faduran@sandia.gov

## 1, Introduction

Security modeling of adversary attacks has been an evolving science over the years. Sandia National Laboratories (SNL) is applying the STAGE commercial modeling and simulation software to develop scenarios for a demonstration facility that is being used by SNL for a variety of security training activities. To extend the range of simulation capabilities, an insider scenario has been developed based on an insider analysis method that integrates the evaluation of material control and accounting (MC&A) activities and physical protection system (PPS) elements.

## 2, Methods and Approach

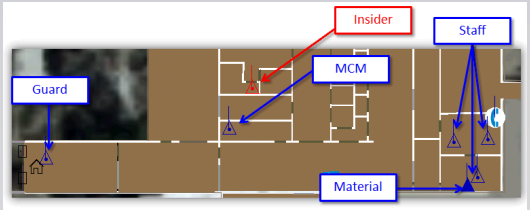
In the insider simulation, a "force-on-force" approach was taken to model two key entities – a malicious insider and an operational staff member who is responsible for performing MC&A activities that would provide a "detection capability" for material that has been taken. Additional entities include staff that provide possible observation of malicious insider activity and a facility response force that performs hypothetical activities when an alert indicates that material is missing. Logic rules were developed for insider and staff behaviors situations in which an insider might attempt theft of material. The initial scenario involves theft of an item that could be hand-carried by the adversary and possible detection of anomalous conditions through staff performance of one MC&A operational activity. This paper describes the insider simulation model and associated scenario. It is anticipated that training activities at the demonstration facility will be developed for scenarios with malicious activities by insiders and to consider how operational activities might be used to mitigate these types of scenarios.



### 2.1 Hypothetical - Processing Facility

The hypothetical processing facility is model as one of the buildings on the demonstration facility. The target and employee characteristics are as follows:

- Two-Room vault - Containing Target
- Six Regular Employees
- Malicious Insider
- Material Control Manager (MCM)
- Three Staff members




The security system features includes the following:

- Single Builidng Guard
- Administrative Controls
- Two-man rule
- Visual inspections as employees leave
- ECP visual check
- MC&A check (daily)

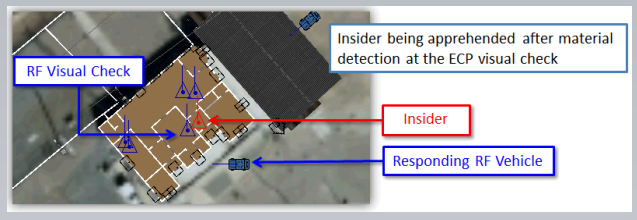
### 2.2 Extended Path Analysis

The insider threat is often addressed within the context of the evaluation of a facility's PPS. The PPS for a facility is evaluated using probabilistic analysis of adversary paths on the basis of detection, delay, and response timelines to determine timely detection. The path analysis methodology focuses on systematic evaluation of the PPS for potential external threats, and calculates the probability that the PPS is effective (PE). Because insiders have facility access, knowledge and authority of facility operations, a facility's PPS provides minimal protection against the insider threat. Probabilistic risk assessment methods have been applied to develop an extended probabilistic path analysis methodology in which MC&A protections can be combined with detection by PPS elements in a calculation for timely MC&A detection. To address the performance of MC&A activities, human reliability analysis (HRA) methods and models for nuclear power plant operations have been applied to characterize detection capabilities.

### 2.3 Scenario Overview

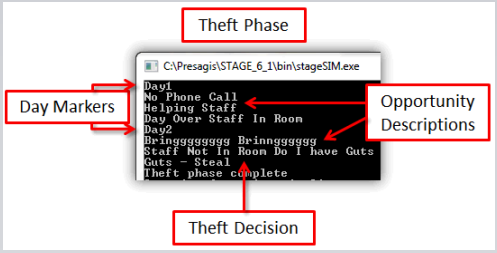
The security system features includes the following:

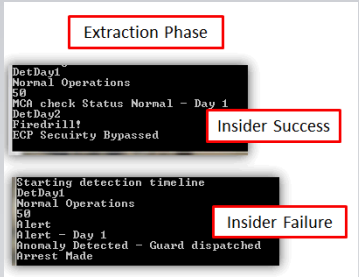
- Adversary bypasses all PPS features through normal facility entry
- A non-violent Insider attempts to remove material from a vault (Phase I)
- Ten-day window of opportunity
- Then transport material offsite (Phase II)
- Ten-day window of opportunity
- Facility staff provide general observation
- Various administrative checks occur throughout to prevent theft

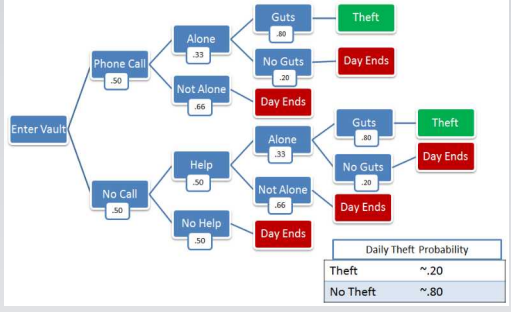


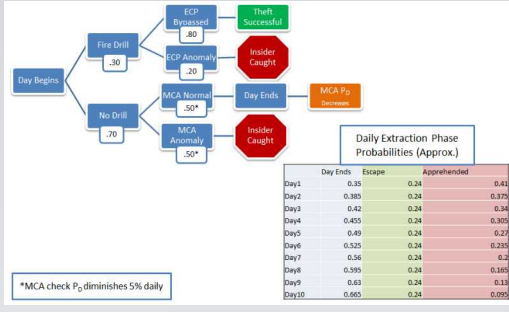

## 3. Results and Conclusions

- The insider simulation model provides a proof of concept for the extended path analysis methodology for insider analysis of a hypothetical process building and extends the simulation modeling for the SNL demonstration facility.
- This simulation model will be used to develop insider training activities at the demonstration facility that will consider how operational activities might be used to mitigate these types of scenarios.
- Several modeling areas have been addressed using the commercial modeling and simulation software, including process modeling, complex behavior, administrative procedures, and random event generation. Additional efforts are being undertaken to develop a more detailed insider simulation models for a nuclear facilities.




Poster Ref. Number: B19

International Conference on Nuclear Security: Enhancing Global Efforts, Vienna, Austria; 1-5 July 2013