ICFO-SI 9 – The 9th International Conference on Facility Operations- Safeguards Interface
Savannah, Georgia, USA, September 23-28, 2012, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2012)
SAND2012-8391C

ADDRESSING THE FACILITY OPERATIONS SAFEGUARDS INTERFACE FOR THE INSIDER THREAT*

Felicia A. Durán, Dean Dominguez, Jordan Parks, Ivan Lozano, Yaxi Liu, and Ben Cipiti
Sandia National Laboratories
P.O. Box 5800, MS 0757, Albuquerque NM 87185-0757
faduran@sandia.gov; ddoming@sandia.gov;mjparks@sandia.gov;bbcipit@sandia.gov

Rebecca M. Ward
Nuclear and Radiation Engineering
The University of Texas at Austin
rebecca.m.ward@gmail.com

ABSTRACT

The insider threat is most often addressed within the context of the evaluation of a facility's physical protection system (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, quantitative evaluation of the PPS and often calculates the probability that the PPS is effective (P_E) in defeating an adversary who uses that attack path. Modeling and simulation are also applied for a variety of security applications, particularly for force-on-force combat engagements. These evaluation and analyses approaches have been most extensively used for evaluating PPS effectiveness against outside adversaries. Because insider adversaries have facility access as well as knowledge about and a range of authority for facility operations, a facility's PPS actually provides minimal protection against the insider threat. Other facility operations and interfaces must be considered to evaluate protection effectiveness against inside adversaries. This paper describes the development of insider scenario simulation models that takes a "force-on-force" approach and implements methods to integrate material control and accounting and other operational procedures that provide protection against inside adversaries by monitoring and tracking critical materials.

Key Words: insider threat, insider analysis, insider modeling and simulation.

1. INTRODUCTION

Modeling outsider adversary attacks for the U.S. Department of Energy (DOE) has been an evolving science over the years. Traditionally, live exercises, and map exercises have been considered the most effective means of analysis for the outsider threat. These methodologies are widely practiced and accepted. As technology has evolved, methodologies for integrating modeling and simulation (mod/sim) into the analyst toolkit has become more accepted and operationally preferred. Sandia National Laboratories (SNL), a leader in physical security analysis, has adopted numerous modeling tools to fill the outsider threat definition. As part of an

* Sandia National Laboratories is a multi program laboratory operated by Sandia Corporation, a wholly-owned subsidiary of Lockheed Martin Company, for the U.S. Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000. Approved for unclassified/unlimited release.

overall training and demonstration initiative, SNL has refreshed and updated a retired DOE facility. This facility is a former DOE Category I site that has now been adapted to show the capabilities of an operational physical protection system (PPS). Commercial mod/sim software is being used to develop scenarios for a variety of security applications, particularly for force-on-force engagements for outside adversary attacks.

The insider threat is most often addressed within the context of the evaluation of a facility's physical protection system (PPS). Because insider adversaries by definition have facility access as well as knowledge about and a range of authority for facility operations, a facility's PPS actually provides minimal protection against the insider threat. Other facility operations and interfaces must be considered to evaluate protection effectiveness against inside adversaries. To extend the range of simulation activities, a "force-on-force" approach was taken to develop insider simulation models based on an insider analysis method that integrates the evaluation of material control and accounting (MC&A) activities and PPS elements [1] and integrated safeguards and security modeling for advanced nuclear reprocessing facilities [2]. An initial proof-of-concept insider scenario simulation model for item theft was developed. Subsequently, a second insider scenario simulation model was developed for material diversion in an electrochemical processing plant. These mod/sim efforts provide a variety of capabilities to explore facility operations and important interfaces for safeguards and security.

2. BACKGROUND

The background for this work includes an overview of the modeling and simulation software and model development for the SNL demonstration facility and a summary of the extended path analysis methodology.

2.1 Overview of STAGE Software

The STAGE commercial mod/sim software is being applied for a variety of security applications, particularly for force-on-force combat engagements for outside adversary attacks [14]. STAGE stands for "Scenario Toolkit And Generation Environment." STAGE is often used for designing complex and intelligent strategic simulation applications. It provides a framework to create end-to-end scalable Red Team/Blue Team force-on-force combat simulations.

STAGE was used to take a "force-on-force" approach to analyze how a facility might respond to insider threats. STAGE provides the following capabilities:

- Logic based behavior: Human entities model the ability to "make a decision" based on the current situations and partially controlled by probability analysis.
- Ground navigation: Humans and mobile equipment can dynamically find paths both inside and outside the facility. Sensing abilities possessed by the human entities enables visual detection of other humans and objects.
- Event-based entity missions: These help define the main thread and strategies of the scenarios.
- Scripting support: Provides the ability to model "Process Monitoring" including the random function that is required for generating dynamic scenarios.

- 2D/3D environment: Provides visual representation of the scenarios.

2.2 Simulation Model Development for Demonstration Facility

The simulation modeling for the SNL demonstration facility has focused on traditional principles for modeling force-on-force activities via outsider attacks. Simulation modeling for several types of outsider attacks has been developed, including single path, multiple path and diversion scenarios. The demonstration facility includes a perimeter intrusion detection and assessment system (PIDAS) for a protected area (PA) that is separated into seven perimeter sectors. A perimeter alarm is sent to the Central Alarm Station (CAS), and the CAS then assumes Command and Control to direct the response force (RF). A generic RF can include a Quick Response Team (QRT), a Patrol Team, and a Backup Force (BUF). Following a specific Security Incident Response Plan (SIRP), the RF employs a generic protection strategy. Table I summarizes the security features for the demonstration facility PPS. Figure 1 provides the model for the demonstration facility, which also includes a demonstration processing building.

Table I. Security features for the Demonstration Facility PPS

PPS Features and Functions	
Feature	**Capability**
Entry Control Point (ECP)	Access Control; Vehicle Sally Port
Central Alarm Station (CAS)	Command & Control; Alarm Assessment
Perimeter Intrusion Detection and Assessment System (PIDAS)	Perimeter Detection; Assessment; Delay
Local Zone	Layered Delay; Detection
Response Facility	Protected Response Facilities
Protection-in-depth	Perimeter Delay; Local Zone Delay; Target Delay
Interruption and Neutralization	Response SIRP; QRT; BUF

2.1.1 Opposition force red team capabilities

Red Team capabilities for outside scenarios in the simulation software allow for complex mission execution utilizing the full breadth of a design basis. This mission execution can include a single primary or multi-target acquisition, secondary or tertiary mission requirements. Mission execution will be dependent on a pre-defined Red Team timeline. This timeline will outline which barriers are to be defeated, which sensors (detection zones) must be accounted for, reaction to RF interdiction, command and control of respective units, small team assignments, contingencies, and other pertinent scenario information. As the team continues along its timeline, the software accounts for changes in the environment and makes dynamic decisions based on the logic the analyst programs for the team.

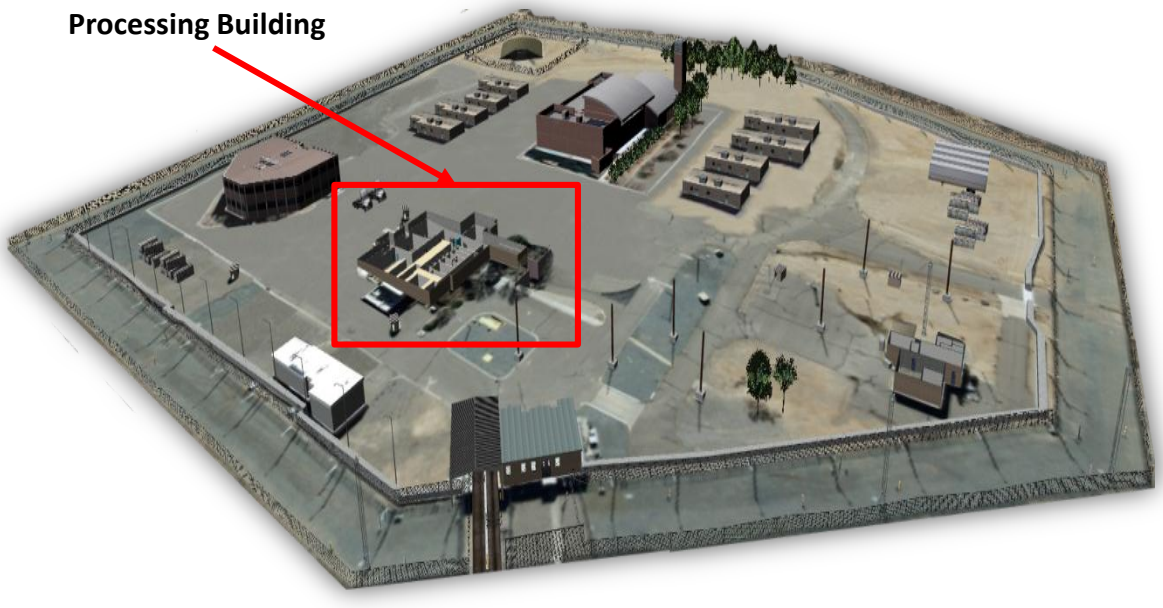

Figure 1. Demonstration facility with processing building and operational PPS.

2.1.2 Response force blue team capabilities

Blue Team capabilities for outside scenarios within the simulation software allow for complex reactive mission execution utilizing the full range of response strategy. This includes the ability to model a command and control element that communicates from a CAS to entities (responders) in the simulation. This allows for information to be disseminated to the responders as it becomes available. For example, breach in perimeter, target location compromised, unauthorized intruder, etc. Once this communication is received, the responding elements can then act autonomously within the simulation to execute a predetermined set of rules. These reactive measures continue as the Red Team continues along their timeline. At which point there is interdiction, an engagement, and adjudication of the engagement.

2.3 Extended Path Analysis Methodology for Insider Analysis

The insider threat is most 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, quantitative evaluation of the physical protection component for potential external threats, and often calculates the probability that the PPS is effective (P_E) in defeating an adversary who uses that attack path. Because insider adversaries by definition have facility access as well as knowledge about and a range of authority for facility operations, a facility's PPS actually provides minimal protection against the insider threat. Other facility operations and interfaces must be considered to evaluate protection effectiveness against inside adversaries. By monitoring and tracking critical materials, MC&A operational activities provide additional protection against inside adversaries. Timely detection for MC&A activities,

however, has been difficult to determine so that for the most part, the effectiveness of these activities has not been explicitly incorporated in the insider threat evaluation of a PPS.

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. The application of this methodology is intended to provide an assessment of the effectiveness of a site's protection systems against insider theft [1]. 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 [3]. An object-based state machine paradigm models insider theft as a race against detection by facility MC&A activities. This paradigm is coupled with the HRA techniques to characterize detection timelines for MC&A protection elements and provides the framework for applying convolution mathematics to calculate timely MC&A detection. Event sequence diagrams are applied to incorporate MC&A activities as path elements and to develop evaluation scenarios for insider paths through layers of the PPS. These insider analysis methods and previous analyses were adapted as the basis for the insider simulation scenario development.

3. PROOF-OF-CONCEPT – INSIDER SCENARIO FOR ITEM THEFT

The initial proof-of-concept insider simulation explored a "force-on-force" approach for item theft by an insider adversary. Two key entities were modeled – a malicious insider (Red Team) and an operational staff member (the Blue Team material control manager (MCM)) who is responsible for performing MC&A activities that would provide a "detection capability" for material that has been taken. Additional Blue Team 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 for hypothetical 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.

3.1 Target Material in Processing Building

The target material is in a hypothetical two-story processing building within the demonstration facility with the bottom floor below ground. Target material is stored in a two-room vault on level one of the processing building. Each target piece is man-portable and has a mass of approximately 1 kg. The building has one main entrance point accessible by foot via normal entry control process, as well as four stairwells leading to second floor emergency exits that are alarmed during normal operations. The main access point is staffed by an armed guard.

3.2 PPS Measures

Inside the processing building, the adversary is able to circumvent all PPS measures in the baseline scenario due to his operational knowledge. The only active PPS measures include a two-man rule in the vault and general observation by facility staff. The MCM always enters the

vault with the insider adversary and provides general observation of the adversary's actions. A posted guard conducts visual inspections as employees badge out of the building.

The ECP is equipped with physical protection measures on exit from the facility. Exiting personnel must enter a pin to gain access to the mantrap. Once in the mantrap, a security police office (SPO) conducts visual inspections and then permits personnel to exit the ECP. During a fire drill, random inspections of exiting employees are conducted at the processing facility exit and the ECP. Additionally, fire drills present a site condition that ignores emergency exit alarms.

3.3 Insider Blue Team

The insider Blue Team is comprised of the MCM, three staff members and the response force. The responsibilities of each member of the Blue Team are listed in Table II.

Table II. Insider Blue Team Members and Responsibilities

Blue Team Member	Responsibilities
Material Control Manager	General observation in processing facility vault Conducts routine MC&A activity (shift check)
Staff Members	General observation as they conduct daily operations
Posted Guard	Conduct inspections as employees exit the building.
CAS Operator	Receives communications from MCM and dispatches response forces
Rover Team	Responds to anomaly at processing facility as directed by CAS
Backup Force	Secures ECP as directed by CAS Conducts random inspections on exit

3.4 Insider Red Team

The adversary is a facility insider acting alone. He has access to the target material and knowledge of facility operations. In the base scenario, it is assumed that the insider has full knowledge of any PPS measures located within the facility and is able to circumvent those measures. He also knows the ten-day period over which a fire drill will occur, during which time he will attempt to remove material from the facility. The adversary is non-violent and will surrender without struggle if interdicted. His goal is to steal one piece of target material from the vault and store the material in his office until a fire drill occurs, at which time he can move the material off-site without undergoing visual inspection at the exit of the processing building. Figure 2 illustrates a portion of the processing building layout, the location of the material, and positions of the Blue Team members and Red Team.

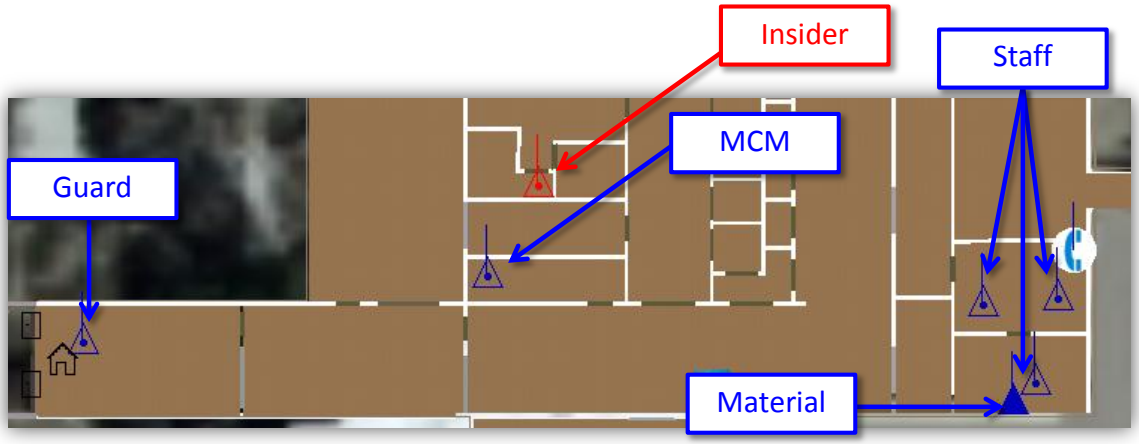

Figure 2. Portion of processing building layout, location of the material, and positions of the Blue Team members and Red Team.

3.5 Scenario Timelines

For the scenario, several timelines need to be considered for the Blue Team and Red Team. The Blue Team timelines include the MC&A detection timeline and the RF timeline. The Red Team timelines include the theft timeline (Phase I) and the extraction timeline (Phase II).

For MC&A detection, a shift check is conducted at the end of every shift. This administrative procedure has the MCM review and reconcile records for activities conducted during the shift. The ability of this procedure to detect an anomaly changes with time. HRA models for nuclear power plant checking operations indicate that human performance for detecting anomalies generally degrades over time as the operator(s) performs a task multiple times [3]. These methods were applied as the basis for determining a probability of detection for an MC&A activity [4, 5] and adapted for MC&A detection included in this insider scenario.

If the shift check detects an anomaly, that is MC&A detection occurs, the facility moves into a heightened state of alert and the RF timeline begins. A roving SPO patrol is dispatched to the facility, and a SPO enters the facility and arrests the insider. If a theft is detected by a visual inspection in the ECP, the roving team dispatches to the ECP and arrests the insider. Figure 3 illustrates possible RF actions.

For the Red Team theft timeline, the adversary has one sequence of chances to remove material from the vault each day. This chance occurs if the MCM is called away from the workbench by a phone call or another staff member needing assistance. If the MCM is called away, the insider adversary is likely to steal the material, though he may decide he is not ready or he will not take action if he is not alone (other staff members are still around). For the theft timeline (Phase I), the insider adversary has ten days over which he may steal the material from the vault and move it to his office. Once the material is in his office, the extraction timeline (Phase II) begins and the insider has ten days to move the material off site. He will move the material during a fire drill, which may occur anytime during the ten day period, so that he can circumvent the posted

guard at the building exit. Figures 4 and 5 provide the insider decision processes for the theft and extraction timelines, respectively. The numbers associated with each event indicate a notional probability of occurrence. Once the material has been removed from the process building, the adversary hides the material on his person, and proceeds to exit the ECP on foot according to normal procedure. If he successfully gets through the ECP, he then drives the material off-site in his personal vehicle.

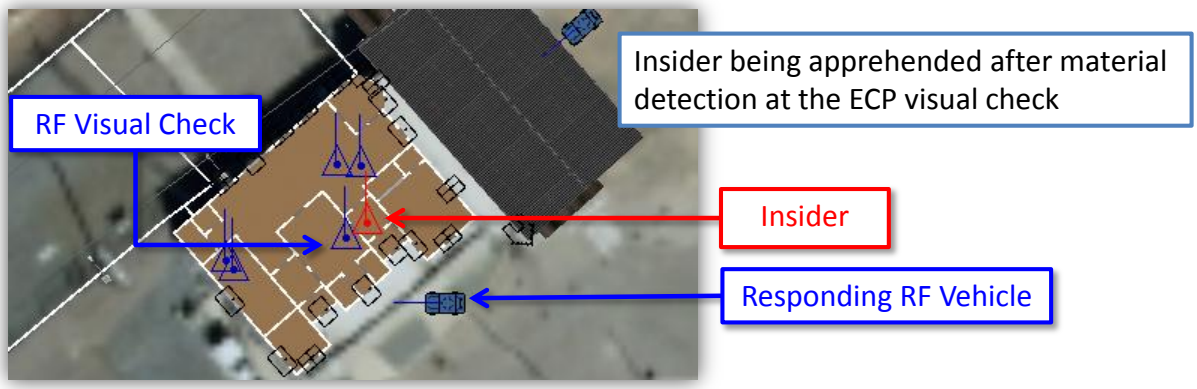

Figure 3. Response Force actions at the ECP.

Table III summarizes the Blue Team and Red Team timelines for detection and adversary action, respectively.

Table III. Scenario timeline for adversary action and detection

Time	Adversary Action	Detection
0	Circumvent 2-man rule and grab material	2-man rule
[1-10 days]	Take to office	General observation
[1-10 days]	Hide in office until fire drill	MC&A – shift check
E – traversal time	Remove during drill	General observation
Δ – traversal time	Walk out ECP	Man trap, SPO visual check

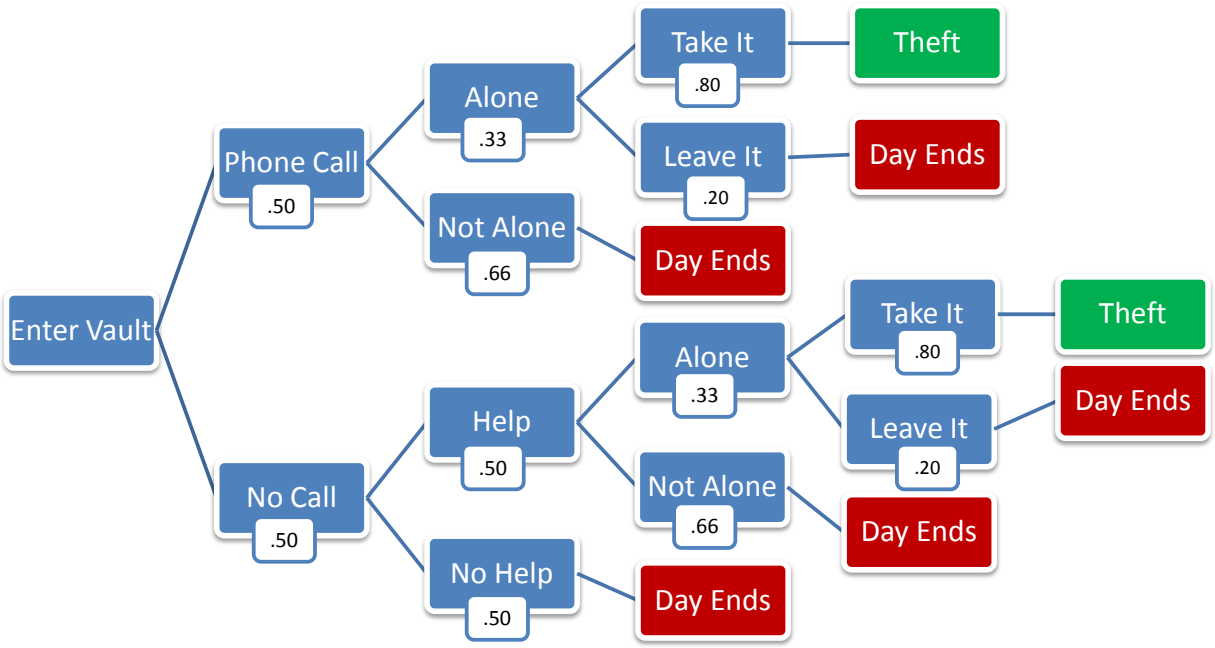

Figure 4. Decision tree for Red Team theft timeline (Phase I).

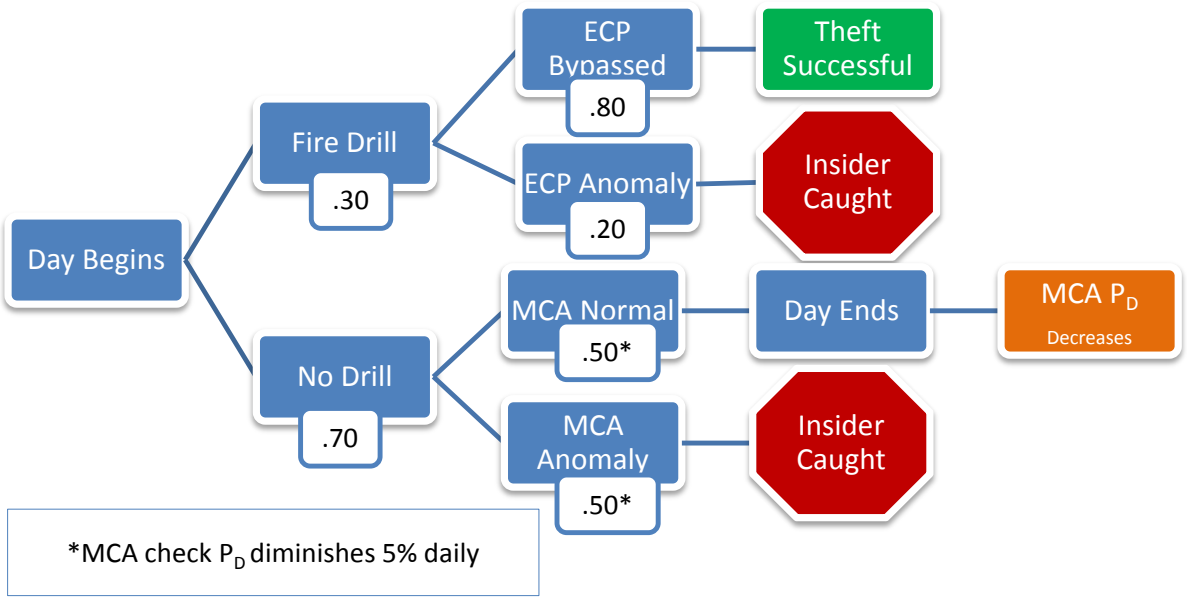

Figure 5. Decision tree for Red Team extraction timeline (Phase II).

4. INSIDER MATERIAL DIVERSION FROM AN ELECTROCHEMICAL PROCESS

Following the development of the initial proof-of-concept scenario a second effort proceeded to incorporate additional process modeling along with adversary and operational staff entities to model material diversion by an insider adversary. A high-level version of the electrochemical process was incorporated in the model along with adversary and operational staff entities. This model incorporated the electrochemical process in the processing building and included several elements of the demonstration facility's PPS (Figure 6). The two rooms on the east side of the building are used as the hot cell (northern room) and process cell (southern room) which would be found in a typical electrochemical processing plant. Fuel assemblies are received via daily shipments from a rail car in the process cell, which houses the shredder (the first unit operation). All other unit operations in the scenario occur in the hot cell. The remainder of the building is a general work area with some rooms serving as offices (such as for the operations manager). The southwest corner of the building contains the only entrance/exit for the facility. The PPS elements that are included in the model are the inner and outer perimeter fence around the facility with microwave sensors to detect movement in the area between the two, the ECP that includes a radiation sensor that scans anyone leaving the facility, guard patrols around the facility, and the CAS.

Figure 6. Process building for demonstration facility.

4.1 Electrochemical Processing Model and Operations

The model of the electrochemical process includes three unit operations, the shredder, electrolytic reduction, and the electrorefiner. Process material is model as some amount of

unspecified mass. Each unit operation, modeled as an entity in STAGE, takes in a certain amount of mass as input. Processing is simulated by the unit operation holding on to the mass for a configurable amount of time for each unit operation. Mathematical formulas can be applied to the input mass during this time to produce an output mass that would be representative of the input. Baskets are modeled as entities as well whose sole purpose is to transfer material from one unit operation to the next. Baskets are always on hand to shuttle material to the next operation.

The mass at any stage of the process is represented internally within each entity as a variable. A communication protocol handles mass transfer between entities. Mass can be in three states within a unit operation: newly arrived mass, mass being processed, or mass ready for output. It is important to note for electrochemical processing that mass flows are not treated individually. This generalized process framework can be extended to accommodate other material flows as needed by adding additional baskets and logic to split and send different masses down separate paths.

With the process flow model, an entity which conducts process monitoring and material measurement was also developed. This entity monitors the input to each unit operation and basket, then calculates the expected output and waits for a measured output to be reported. The measured output contains some small configurable random error, and the entity compares the measured output with the expected output. The differences for each unit operation and basket is tracked and compared to the expected value. If the total difference crosses a defined mathematical threshold, then the process monitoring system can trigger an alarm in the facility. When an alarm is raised by this entity, an event is sent to the operations manager, who can decide to contact the CAS to put the facility in a state of alert.

Around the facility, several entities go about their daily tasks (the Blue Team). Each entity has its own set of logic and through their actions they comprise the MC&A portion of our integrated system. The HRA methods have also been implemented into the actions of our entities, where previous failures or successes in a task have an impact on future task performance [3]. The Blue Team entities and their responsibilities are listed in Table IV. The process and entities are shown in Figure 7.

4.2 Scenario Description

The scenario envisioned for this facility is one where the insider adversary has setup a mechanism to divert material from the electrorefiner unit operation after material has been scraped off the cathode. This mechanism would divert the material into a man-portable container elsewhere in the facility for the adversary to recover. The adversary will be aware of coworker movements and when an opportunity presents itself, he will trigger the automated material diversion process. The current implementation involves a single, large diversion, although a protracted diversion is also possible in the framework. Once the container is ready, the adversary will attempt to move it to an interim location. He will then attempt once a day to leave the facility with the material and deposit it on a departing rail car. The phases of the adversary's actions follow with more detail.

Table IV. Blue Team entities and responsibilities

Blue Team Entities	Responsibilities
Guards (x4)	Two man the Personnel Entry Control point. Two patrol the outside of the facility looking for suspicious activity
Worker	Works around the facility conducting various tasks while providing visual observation of activities and operations nearby
Operator	General monitoring of processing operations. After a theft has occurred, attempts to detect the theft each day with diminishing success after each detection failure.
Operations Manager	Checks process monitoring and material measurement alerts and decides if a particular alert is a cause for concern or a false positive. If the former, the CAS is notified.
Central Alarm Station	Coordinates guards and receives alerts from other entities.
Process Monitoring and Material Measurement	Monitors mass flows in the processing operation. Anomalies are reported to the operations manager when a threshold is broken.

4.2.1 Material diversion phase

Diversion of the material will involve removing material which has just been recovered from the cathode in the electrorefiner. The material diversion phase event tree is shown in Figure 8. It is assumed that the adversary has setup an automated process that, once started, will either continuously steal material over time or take a large amount of material at once. The consequence of this is that the adversary only needs to be alone for a short period of time to start the diversion process. Once started, he can return to his work area and simply wait for the diversion process to alert him that it has been successful.

The insider adversary is a process operator, one of two such operators. He is aware of other co-workers movements around him. If he sees them moving away from the automated process trigger, he will make his move to begin the process. Starting the process takes some arbitrary small amount of time. If he is spotted by another worker in the process, the worker will recognize the malicious activity and alert CAS. At this point, the scenario would end with the adversary failing as security is alerted. If the adversary is successful, he will no longer leave his post daily and will instead wait for the diversion to complete.

4.2.3 Material retrieval phase

The material retrieval phase event tree is shown in Figure 9. The process monitoring/material management system constantly keeps track of the mass flows in the electrochemical process.

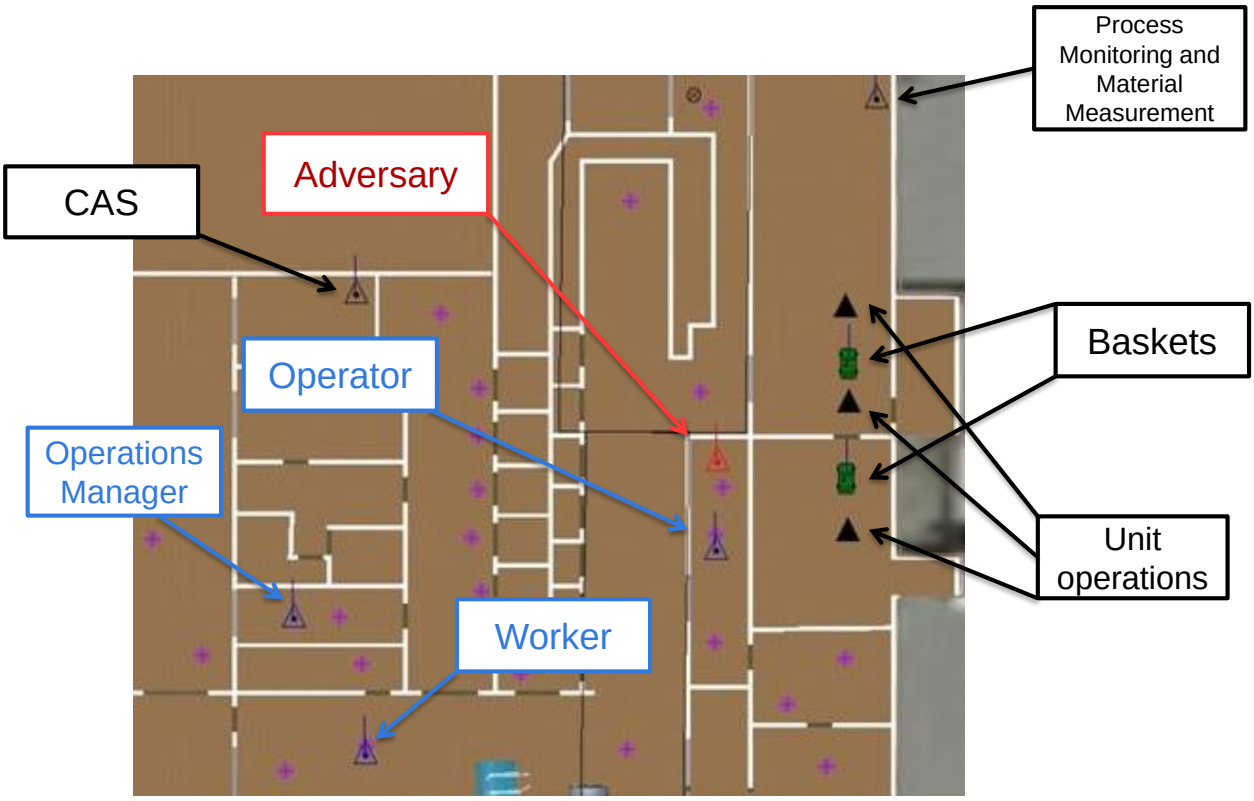

Figure 7. Entities and electrochemical process operations.

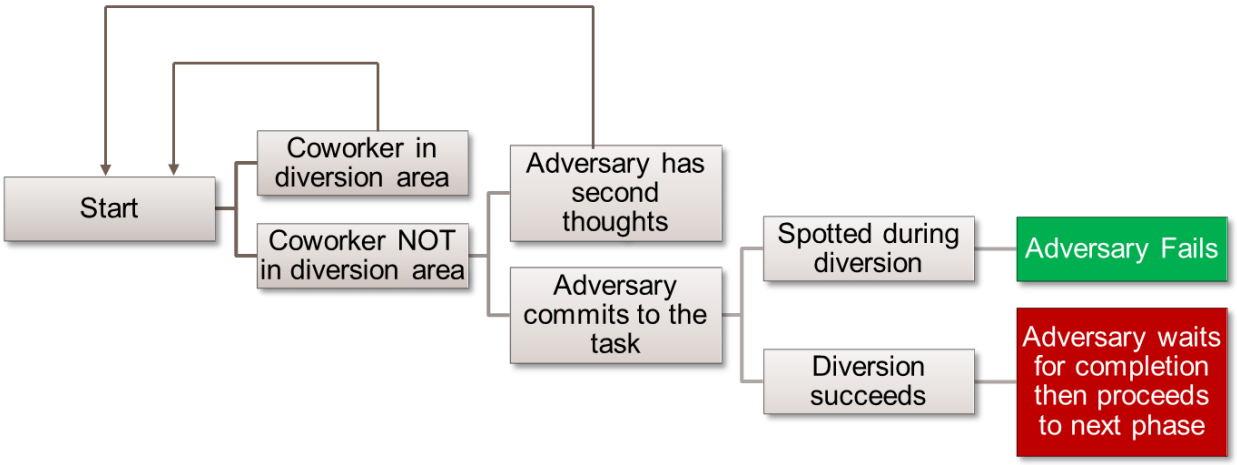

Figure 8. Material diversion phase event tree.

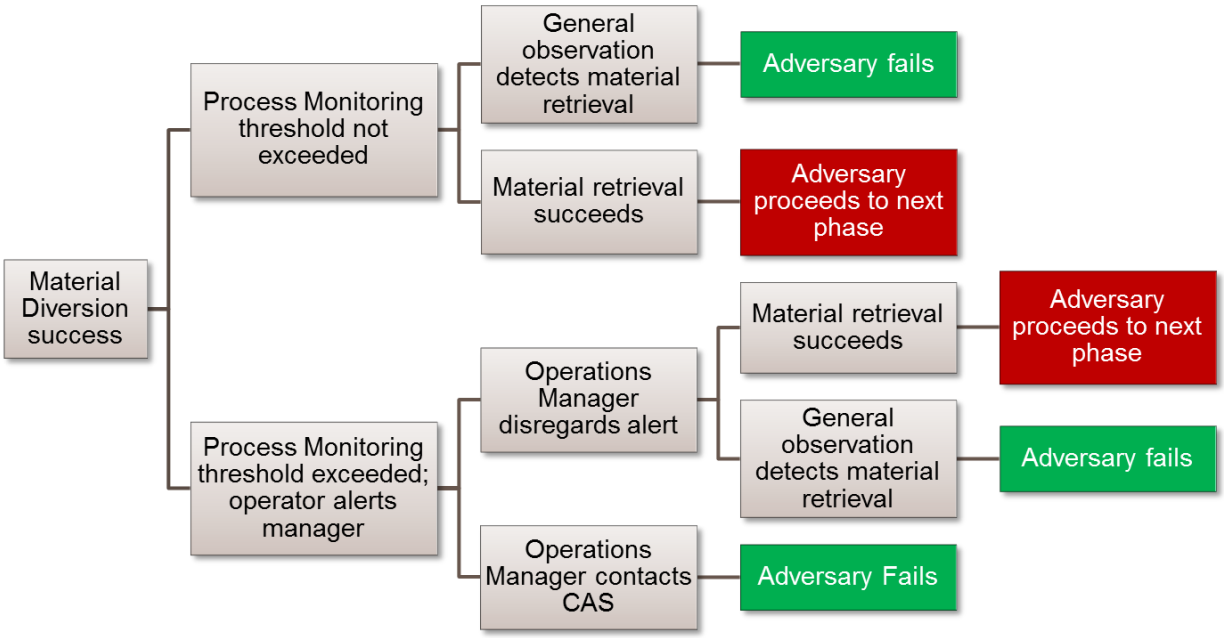

Figure 9. Material retrieval phase event tree.

Any difference between the expected value and the measured value of the mass flow is recorded. As with any measurement, mass flow measurements contain a small amount of random error. To account for this, the system keeps track of the total difference of previous measurements. If the total difference crosses some mathematical threshold, then an alert is sent to the operations manager. Depending on the amount of material the adversary is attempting to steal, the alert may be triggered. The operations manager will then make a probabilistic decision about the alert. If he decides that it is not a concern, then the facility will not be sent into a state of alert. Should the operations manager suspect something is wrong, the CAS is alerted, and response force guards are sent to investigate. This results in the scenario ending and an adversary failure.

When the container is filled, the adversary will attempt to retrieve the material for later extraction from the facility. He will attempt to move to the location of the diverted material container, however if another worker is present he will abort and return to his desk for a short period. Should he make it to the location of the container, he will spend a short amount of time retrieving it. During this time, if a coworker observes his unauthorized activity, the CAS is alerted and guards are deployed. This results in the scenario ending and an adversary failure. Should the adversary successfully collect the container, he will store it in an interim location and wait for the next day to begin the material extraction phase.

Once the diversion has completed, there is a chance that the other operator (blue-team) may notice something is wrong and alert his superiors. If this occurs, it ends with the adversary failing. Every day that passes with the operator not seeing the theft, his detection probability for the next day falls. This is part of our HRA dependence modeling. The operator will continue to attempt detection until the end of the scenario, including into the next phase.

4.2.2 Material extraction phase

The material extraction phase event tree is shown in Figure 10. Once the adversary has retrieved the container and stored it in an interim location, they will attempt to leave the facility at the start of each day. The adversary will only attempt to do this once a day as the rail car is only at the facility for a short period of time, and if the chance is missed, extraction will not be possible. They begin by attempting to leave through the entrance of the facility; however if a coworker is present in the area, the adversary will abort and attempt to leave the next day. Should the adversary arrive at the entrance without being seen, he will be required to be tested by a radiation sensor. If the sensor detects the material, the adversary will fail as the CAS will be alerted and the facility will be sent into a state of alert.

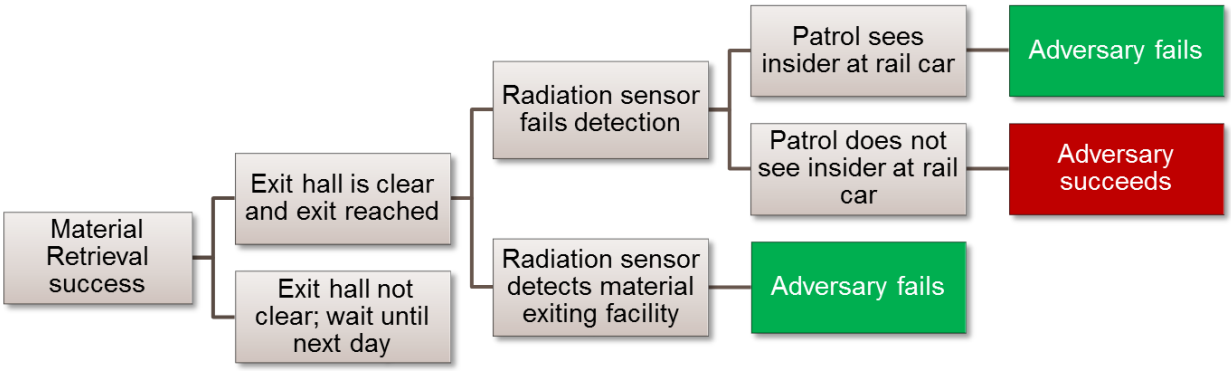

Figure 10. Material extraction phase event tree.

Should the sensor fail detection, the adversary will be allowed to proceed to the exterior of the processing facility. From here, they will make their way to the rail car to attempt deposit of the material. If they are spotted by patrols by the rail car, the adversary will fail as the guards will investigate the suspicious activity. Otherwise, the adversary will succeed overall in extracting material out of the facility.

5. INSIGHTS AND CONCLUSIONS

Beyond evaluation of PPS effectiveness, other facility operations and interfaces must be considered to evaluate protection effectiveness against inside adversaries. This mod/sim effort has demonstrated the STAGE software capabilities for taking a force-on-force approach to develop insider simulation models based on an insider analysis method that integrates the evaluation of MC&A operation and PPS elements on and integrated safeguards and security modeling for advanced nuclear reprocessing facilities. These mod/sim efforts provide a variety of capabilities to explore facility operations and important interfaces for safeguards and security.

Several modeling areas have been addressed including process modeling, complex behavior, administrative procedures, and random event generation. The models provide a framework for

exploring the characteristics of an integrated protections system, allowing the user to change the logic and probabilities for the behaviors of the different entities, perhaps to explore different operational approaches or different threshold values. One of the best outcomes of this work was a framework for visualizing possible insider adversary behavior within facilities operations. These simulation models would be very useful for developing deeper insights and understanding of facility operations and improved safeguards and security designs and operations.

This work extends the simulation modeling for the SNL demonstration facility to include insider scenarios. It is anticipated that these simulation models will be used to develop insider threat training activities at the demonstration facility that will consider how operational activities might be used to mitigate these types of scenarios.

ACKNOWLEDGMENTS

The authors acknowledge the support and encouragement of Dominic Martinez and Carla Ulibarrí for their support of the collaborative teaming of the Sandia staff. This work was funded, in part, by the U.S. Department of Energy, Office of Nuclear Energy Fuel Cycle Technologies Program, Materials Protection Accounting and Control Technologies (MPACT).

REFERENCES

1. F.A. Durán, *Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials*, PhD Dissertation, The University of Texas at Austin, Austin TX (2010).
2. B.B. Cipiti, F.A. Durán, B.R. Key, Y. Liu, I. Lozano, and R.M. Ward, "Modeling and Design of Integrated Safeguards and Security for an Electrochemical Reprocessing Facility," Sandia National Laboratories, Albuquerque NM (2012).
3. A.D. Swain III and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants," SAND90-0200, Sandia National Laboratories, Albuquerque NM (1983).
4. F.A. Durán and G.D. Wyss, "Human Reliability-Based MC&A Models for Detecting Insider Theft," in *Proceedings of the 51st Annual Meeting of the Institute of Nuclear Materials Management*, Baltimore MD, July 14-18, 2010 (2010a).
5. F.A. Durán and G.D. Wyss, "Applying Human Reliability Analysis Models as a Probabilistic Basis for an Integrated Evaluation of Safeguards and Security Systems," *Proceedings of the 10th International Probabilistic Safety Assessment and Management Conference*, Seattle WA, June 7-11, 2010 (2010b).