Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials*

Felicia Angelica Durán†
Nuclear and Radiation Engineering Program – The University of Texas at Austin
Risk and Reliability Analysis – Sandia National Laboratories

Gregory D. Wyss
Security Systems – Sandia National Laboratories

ABSTRACT

The work presented here describes a new method to incorporate material control and accountability (MC&A) protection elements within the existing probabilistic vulnerability assessment (VA) methodology to estimate the probability of effectiveness (P_E) for insider threats. MC&A activities, from monitoring to inventory measurements, provide information about target materials and define security elements useful against insider threats. Activities that discourage insiders provide many, often reoccurring opportunities to determine the status of critical items. Considering this, we have developed an object-based state machine paradigm whereby an insider theft scenario races against MC&A activities that can move a facility from a normal state to a heightened alert state having additional detection opportunities. This paradigm has been coupled with nuclear plant probabilistic risk assessment (PRA) methods to incorporate the evaluation of MC&A elements in the existing VA methodology. Along with the P_E for the physical protection system (PPS), the overall result is an integrated effectiveness measure of a protection system that addresses outsider and insider threats.

INTRODUCTION

Nuclear facilities use a system of materials control and accountability (MC&A) to control and protect nuclear materials. MC&A is one of four overlapping components of a site's safeguards and security (S&S) protection system, which also includes physical protection, personnel security and information security. Vulnerability assessments (VA) systematically evaluate the effectiveness of a site's protection systems, and often calculate the probability of physical protection system (PPS) effectiveness (P_E). P_E is a measure of the degree to which the system can protect targets against a range of potential threats. The VA methodology focuses on a systematic quantitative evaluation of the physical protection component of the system against potential outsider threats, whereas other qualitative approaches have been used to evaluate the effectiveness of MC&A, personnel security and information security protection systems.

Some system elements support both the PPS and MC&A protection systems (for example, automated surveillance and personnel access control), and some MC&A protections are already incorporated, although perhaps not explicitly identified as such, in the current VA methodology. Other MC&A elements, however, have been difficult to characterize in ways that are compatible with VAs. One step toward addressing this gap uses deterministic Material Assurance Indicators

* Sandia National Laboratories is a Multiprogram Laboratory Operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.
† Felicia is at PhD candidate in the Mechanical Engineering Department at The University of Texas at Austin.

(MAIs) to estimate a real-time effectiveness for protecting nuclear materials [1]. Initial testing has successfully demonstrated that the MAI algorithm is useful for evaluating characteristics of MC&A system capability, but the MAI algorithm is not truly probabilistic. The work to be presented here describes a new method that focuses on incorporating MC&A protection elements within the existing probabilistic VA methodology to estimate P_E for insider threats.

OBJECT-BASED PARADIGM FOR INSIDER THEFT

To determine the effectiveness of a PPS, path analysis is performed to evaluate adversary paths and the associated detection, delay and response timelines. Path analysis determines a quantitative probabilistic measure of timely detection of an outsider adversary path and can also be used to assess active violent insiders. Similar quantitative and qualitative methods are used for other types of insider threats.

Insiders represent formidable threats because they have knowledge of and access to target materials. They can take advantage of opportunities that arise to circumvent system elements and to interact directly with the target without being detected. The detection and delay timelines are not as relevant because insiders can choose the most opportune times and optimum strategies. One strategy for addressing the insider threat would be to optimize the control and accountability of materials, and to more fully incorporate MC&A elements into the VA of the S&S protection system.

MC&A activities, from monitoring to inventory measurements, provide information about target materials and define security elements useful against insider threats. In the MAI work, Dawson and Hester [1] observed that many MC&A activities provide sensing and detection capabilities, similar to other sensors in a PPS. In a sense, MC&A protection elements are interwoven within each physical protection layer, and provide additional detection and delay opportunities within the S&S system. Activities that discourage insiders provide many, often reoccurring opportunities to determine the status of critical items (for example, *daily* administrative checks).

Considering these observations about MC&A protection elements, we have applied an object-oriented modeling approach [2] to develop an object-based state machine paradigm to characterize the insider theft scenario. The object-based state machine is shown in Figures 1a and 1b. The "system" is characterized by two objects – an Insider Theft object and a Facility Status object. The Insider Theft object describes the possible steps in a specific insider theft scenario. The figures below illustrate the state transition diagrams for each object – the Insider Theft object (1a) and the Facility Status object (1b) and their interrelation. Each box in the diagrams is a "state" in which the object can be at a point in time. The arcs between each state are events that can occur to move the object from one state to another. This approach characterizes insider theft as a "race" between insider theft stages from internal to external physical protection layers and the MC&A system elements that detect material is not where it should be. The Facility object indicates how MC&A protection elements act as a "switch" that change the state of the facility from normal to heightened alert where the facility is searching for material that is discovered "missing." This characterization of the insider theft is similar to the characterization of the outsider attack for the PPS as a race between the adversary and facility response team after detection has occurred.

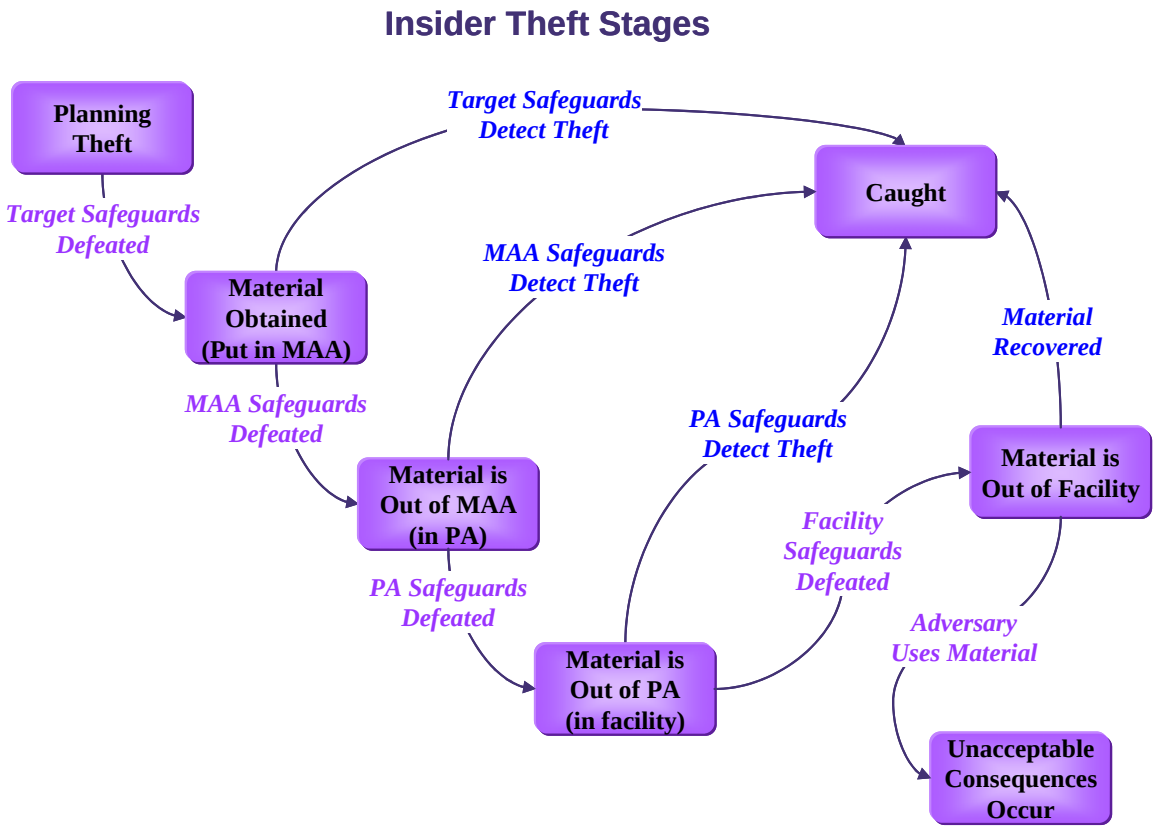

Figure 1a. State transition diagram for Insider Theft Object.

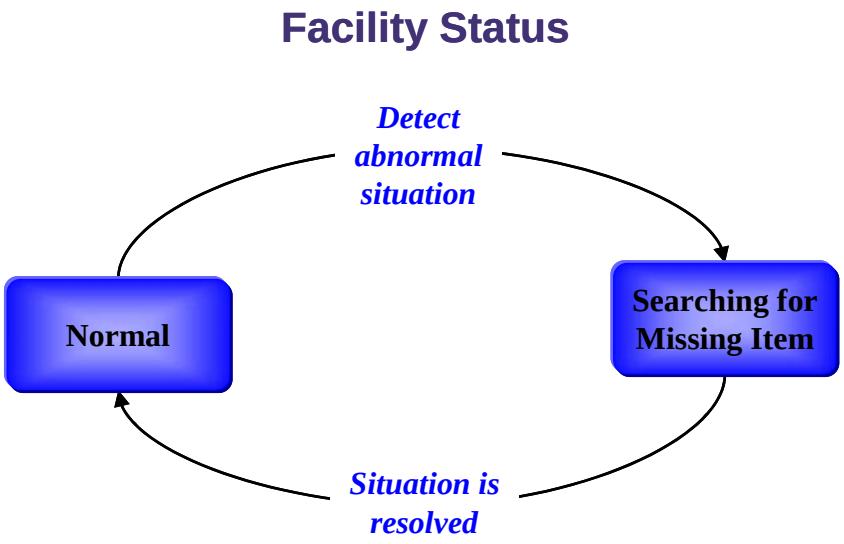

Figure 1b. State transition diagram for Facility Status Object.

TIMING FOR INSIDER THEFT

One of the challenges for evaluating the effectiveness of an S&S protection system against an insider adversary is that the detection and delay timelines determined for the outside adversary and the PPS are not as relevant because an insider adversary can choose the most opportune time to take advantage of system vulnerabilities. Indeed, the various theft events may be separated by large gaps in time. Characterizing the MC&A protection elements in a facility in terms of an object-based state machine provides a framework for defining timing distributions for insider theft stages and facility alerts triggered by MC&A activities that can be convolved to determine the probability of theft or detection happening first. Probabilistic convolution is a method that has been used in nuclear power plant PRA [3] and security timeline analyses [4].

As an insider theft is initiated and proceeds through the physical security layers of a facility, we can define the following time variables:

- T_{R1} - Time for adversary to successfully remove target material from Physical Security Layer 1. Time interval begins when the adversary obtains the material and ends when adversary removes target from Physical Security Layer 1.
- T_{R2} - Time for adversary to successfully remove target material from Physical Security Layer 2. Time interval begins when T_{R1} ends and ends when adversary removes target from Physical Security Layer 2.
- T_{R3} - Time for adversary to successfully remove target material from Physical Security Layer 3. Time interval begins when T_{R2} ends and ends when adversary removes target from Physical Security Layer 3.
- $T_{MC\&AAlert}$ - Time when MC&A activities may indicate that target material is missing. Time interval begins when theft occurs and ends when MC&A alert occurs.

Each of these times is represented as a probability distribution in order to represent the variation in *both* the time before a removal opportunity presents itself and the time to accomplish the removal task. Time and associated probabilities [$P(T_{R1})$, $P(T_{R4})$, $P(T_{R3})$] depend on the defeat methods used in scenario (e.g., removal through SNM monitor after disabling monitor). These data are often available in the existing VA methodology data base. Distributions for a "Normal" facility state can be degraded if MC&A alert has occurred and the facility state is "Searching for Missing Material." Logically, if an MC&A alert has occurred, the facility has a higher probability of detecting and finding the material, and the adversary has a lower probability of successfully removing the material from a Physical Security Layer.

For the last time variable, $T_{MC\&AAlert}$, this is the time when the Facility state transitions from "Normal" state to "Searching for Missing Material" state (Alert). Times and associated probabilities [$P(T_{Alert})$] are dependent on specific MC&A activities included in scenarios. Distributions can be developed considering specific MC&A activities and associated operational considerations. Human reliability analysis (HRA) methods for evaluating operator attention to unannuciated alarm signals during nuclear power plant operations [5] provide insights for developing these distributions. These methods also show how the effectiveness of repeated inspections decreases over time if an anomalous condition is not recognized the first time it occurs.

MC&A activities contribute to the effectiveness of the facility protection system by providing alerts that material may be missing. The effectiveness of MC&A activities can be determined by comparing the probability distributions for the time for MC&A alerts [$T_{MC\&AAlert}$] with the probability distributions for the time for removal of material by the adversary [T_{R1}, T_{R2}, and T_{R3}] using probabilistic convolution to determine the probability that detection occurs before theft. The set of possible scenarios to be evaluated can be deduced by analyzing the object model as an event tree.

CONVOLUTION INTEGRAL

As a general example considering removal of material, let T_M and T_R be random variables over time. Let t_M and t_R be specific values of these random variables. The range of T_M and T_R is $[0, \infty]$.

Let $P(t_M)$ denote the probability density function for T_M and let $P(t_R)$ denote the probability density function for T_R. Let $P(t_M, t_R)$ denote the joint probability density function for T_M and T_R.

A random variable for time of possible "detection" is defined as $T_D = T_M - T_R$ and t_D is a specific value of this random variable. The probability density function for T_D is:

$$P(t_D) = \int_0^\infty \{P(t_M, t_R) \mid t_R = t_M - t_D\} dt_M \tag{1}$$

If T_M and T_R are independent, then $P(t_M, t_R) = P(t_M) \cdot P(t_R)$, and

$$P(t_D) = \int_0^\infty P(t_M) \cdot P(t_M - t_D) dt_M \tag{2}$$

The range of T_D is $[-\infty, \infty]$. The probability that T_D is less than zero is:

$$P(t_D < 0) = \int_0^\infty P(t_D) dt_D \tag{3}$$

This is the probability that an MC&A alert occurs and the Facility transitions from the "Normal" state to the "Searching for Missing Material" before the insider is successful in moving the material past that physical protection layer.

MODEL DEVELOPMENT AND ANALYSIS

A hypothetical facility description has been developed to use as a basis for exercising these new techniques for evaluating the effectiveness of MC&A protection elements. The ATLAS and ASSESS software programs [6, 7], VA tools which comprise a systematic approach for evaluating safeguards and security effectiveness against theft or sabotage of nuclear material by different adversaries, have been used to develop the facility model based on the description, and

to do a preliminary insider analysis. In terms of these two VA tools, a transition from ASSESS to ATLAS is currently underway. Although ASSESS provides the capability for developing facility models and doing outsider and insider analyses, ATLAS was used to develop the facility model for this analysis because it is the VA tool with the most current facility and outsider modules available, and provides up-to-date graphics, computational algorithm, and documentation capabilities. The current version of ATLAS, however, does not as of yet include a complete insider module, so ASSESS continues to be used for the insider analysis in this work.

The adversary sequence diagram for the facility model is shown in Figure 2, and represents the facility security layers (of which there are 7) around a billet target in a storage vault, and the respective safeguards elements on each layer. This facility model was exported from ATLAS and loaded into ASSESS, where insider personnel and their access and authorities were defined. The resulting set of insider scenarios includes both continuous and discontinuous pathways, with respect to timing, which will provide an interesting basis for exercising the probabilistic timing and HRA methods.

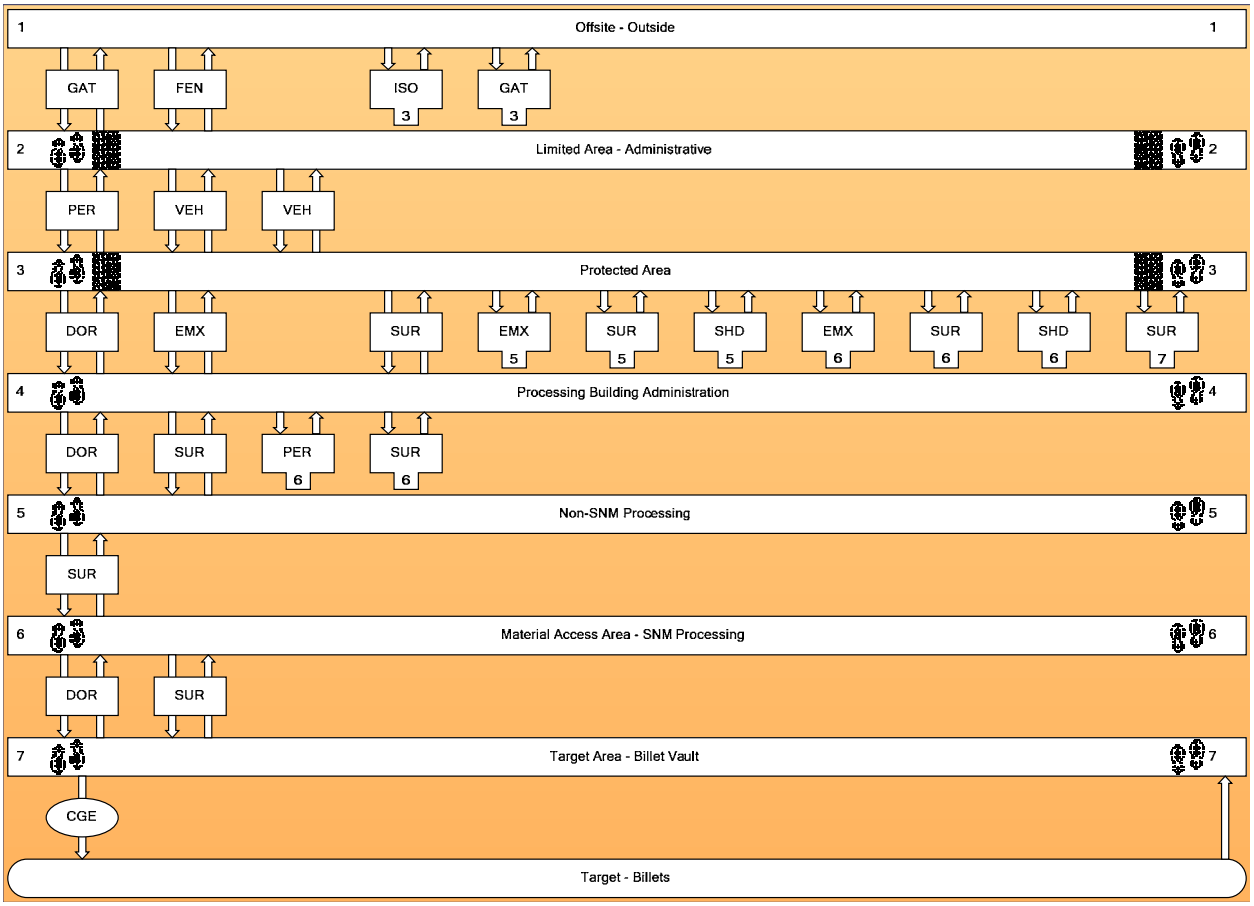

Figure 2. Adversary Sequence Diagram for hypothetical facility.

This work will continue with defining a final set of insider scenarios and developing event sequence diagrams to describe insider paths through the PPS and also incorporate MC&A activities as path elements. The MC&A elements will be characterized by the probabilistic timing and HRA methods, and the resulting event trees will be quantified to determine an effectiveness of the system against the insider threat.

CONCLUSIONS

This work has presented a new method to incorporate MC&A protection elements within the existing probabilistic VA methodology to estimate the P_E for insider threats. We have made significant progress in developing a probabilistic basis and applicable assessment techniques to implement this method. An object-based paradigm of insider theft stages has provided the framework within which to apply nuclear plant PRA techniques for timing, HRA, and event sequence diagrams.

This work is still ongoing. Initial modeling results using the ATLAS and ASSESS software indicate promising insider theft scenarios on which to exercise these new techniques. Additional updated analysis results will be discussed. The P_E for insider threats that is expected to result from this analysis, along with the PPS P_E, will provide an overall result is an integrated effectiveness measure of a protection system that addresses both external and insider threats.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the support of Dr. Sheldon Landsberger, Felicia's PhD Co-Advisor at The University of Texas at Austin. At Sandia, Manuel Trujillo, Michael Benson, and Jose Rodriguez in International Security Programs have provided technical expertise and collaboration in the areas of MC&A, VA, and insider analysis. John Darby provided much needed instruction on probabilistic convolution, and Brad Key (Apogen Technologies) has provided ATLAS and ASSESS software support.

REFERENCES

1. P. G. Dawson and P. Hester, "Real-Time Effectiveness Approach to Protecting Nuclear Materials," Proceedings of the Institute for Nuclear Materials Management 2006 Annual Meeting, July 16-20, Nashville, TN, 2006.
2. G. D. Wyss and F. A. Durán, "OBEST: The Object-Based Event Scenario Tree Methodology," SAND2001-0828, Sandia National Laboratories, March 2001.
3. "South Texas Project Probabilistic Safety Assessment," PLG-0675, Houston Lighting and Power Company, Houston, TX, May 1989.
4. H. A. Bennett, "The EASI Approach to Physical Security Evaluation," SAND76-0500, Sandia National Laboratories, 1977.
5. A.D. Swain III and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants," SAND80-0200, Sandia National Laboratories, 1983.
6. ATLAS (Adversary Time-Line Analysis System) software, Version 4.2,
7. ASSESS Insider Module, Version 2.56, Copyright 1989-2003, Lawrence Livermore National Laboratory.