SAND2008-4030C

Probabilistic Basis and Assessment Methodology For Effectiveness of Protecting Nuclear Materials[*]

by

Felicia Angelica Durán[†]
Nuclear and Radiation Engineering Department – The University of Texas at Austin
Security Systems Analysis – Sandia National Laboratories

Gregory D. Wyss
Security Systems Analysis – Sandia National Laboratories

ABSTRACT

For nuclear facilities, a key approach for defeating insider activities includes procedural measures for protecting critical materials, specifically material control and accountability (MC&A) operations. The work presented here describes recent developments for a new method to incorporate 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, including detection of missing materials. Previous developments for elements of the method are reviewed, including the 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, the definition of possible timing distributions, and the use of probabilistic convolution. The latest method development furthers the coupling of the object-based paradigm with nuclear plant probabilistic risk assessment (PRA) methods to incorporate the evaluation of MC&A elements in the existing VA methodology. These include the use of event sequence diagrams (ESDs) and human error probabilities (HEPs) for detection of missing material. The combination of the elements in the method provides a probabilistic basis for applying this method for determining the effectiveness of protecting nuclear materials against insider threats. Information from ongoing analyses to demonstrate the method and determine an effectiveness measure for MC&A activities is also discussed. Along with the P_E for the physical protection system (PPS) determined in existing VA analyses, the overall result is an integrated effectiveness measure of a protection system that addresses outsider and insider threats.

INTRODUCTION

For nuclear facilities, a key approach for defeating insider activities includes procedural measures for protecting critical materials, specifically material control and accountability (MC&A) operations. MC&A activities, from monitoring to inventory measurements, provide critical information about target materials and define security elements that are useful against

[*] 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. SAND2008-XXXX, Unclassified/Unlimited Release.

[†] Felicia is a PhD candidate in the Mechanical Engineering Department at The University of Texas at Austin.

insider threats. However, MC&A elements have been difficult to characterize in ways that are compatible with the vulnerability assessment (VA) methods that are used to systematically evaluate the effectiveness of a site's protection systems. 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. VAs systematically evaluate the effectiveness of a site's protection system, 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 and does not explicitly consider or take credit for MC&A protection elements. We investigate the characterization of MC&A activities as detection elements. The work presented here describes recent work in the development and application of a new method that extends the existing probabilistic VA methodology to incorporate MC&A protection elements to provide an effectiveness measure for insider threats. MC&A activities that discourage insiders provide many, often reoccurring opportunities to determine the status of critical items, and can be considered a type of sensor system with alarm and assessment capabilities necessary for detection. Previous developments [1] for elements of the method are reviewed, including the object-based state machine paradigm (whereby an insider theft scenario races against MC&A "sensor systems" that can move a facility from a normal state to a heightened alert state having additional detection opportunities), the definition of possible timing distributions, and the use of probabilistic convolution. Recent advances in the method use event sequence diagrams (ESDs) and human error probabilities (HEPs) for detection of missing material to evaluate MC&A elements under the existing VA methodology, further coupling the object-based paradigm, MC&A evaluation, and traditional probabilistic risk assessment (PRA) methods. Information from ongoing analyses to demonstrate the method and determine an effectiveness measure for MC&A activities is also discussed.

OBJECT-BASED PARADIGM FOR INSIDER THEFT

To determine the effectiveness of a PPS, path analysis is performed to evaluate adversary paths using detection, delay and response timelines. Path analysis determines a quantitative probabilistic measure of timely detection of an outsider adversary along an attack path, and can also be used to assess active violent insiders.

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, often using protracted or discontinuous attacks. 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 their work developing Material Assurance Indicators (MAIs), Dawson and Hester [2] 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). As an example, Table 1 lists some key administrative MC&A activities that are performed on a reoccurring basis. A year-long detection opportunity timeline can be constructed from the compilation of the reoccurrence of these activities and demonstrates the importance of these activities as protection elements against insider threats.

Table 1. Frequencies of Key Administrative MC&A Activities (Representative)

MC&A ACTIVITY (Examples of Key Administrative Controls)	**ACTIVITY FREQUENCY (days)**
Plan of the Day	1
Daily Administrative Check	1
Forms Reconciliation	3
Process Call	15
Physical Inventory	30
DOE Audit	365

Considering these observations about MC&A protection elements, we previously described [1] the application of an object-oriented modeling approach [3] to develop an object-based state machine paradigm to characterize the insider theft scenario. The object-based state machine for the "system" is shown in Figures 1a and 1b. The system is characterized by two objects – an Insider Theft object and a Facility Status object, the state transition diagrams for which are illustrated. The Insider Theft object describes the steps in a specific insider theft scenario. 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.

INCORPORATING ASSESSMENT OF MC&A ACTIVITIES

Characterizing the protection system to include MC&A elements interwoven within each physical protection layer provides a basis for extending the traditional event tree representation of insider theft (Figure 2a) to include MC&A activities. The set of possible scenarios to be evaluated can be deduced by analyzing the object model as an ESD. Figure 2b illustrates this extension as an ESD. Having a basis to represent the steps of insider theft and to incorporate MC&A activities within each layer provides a framework for propagating probability values to determine effectiveness for detecting missing material. Figure 2b indicates where MC&A activities trigger a change of facility state from normal to "heightened alert," where the facility is searching for "missing" material. This state change is modeled using different detection probabilities for the normal and heightened alert facility states at each detection opportunity.

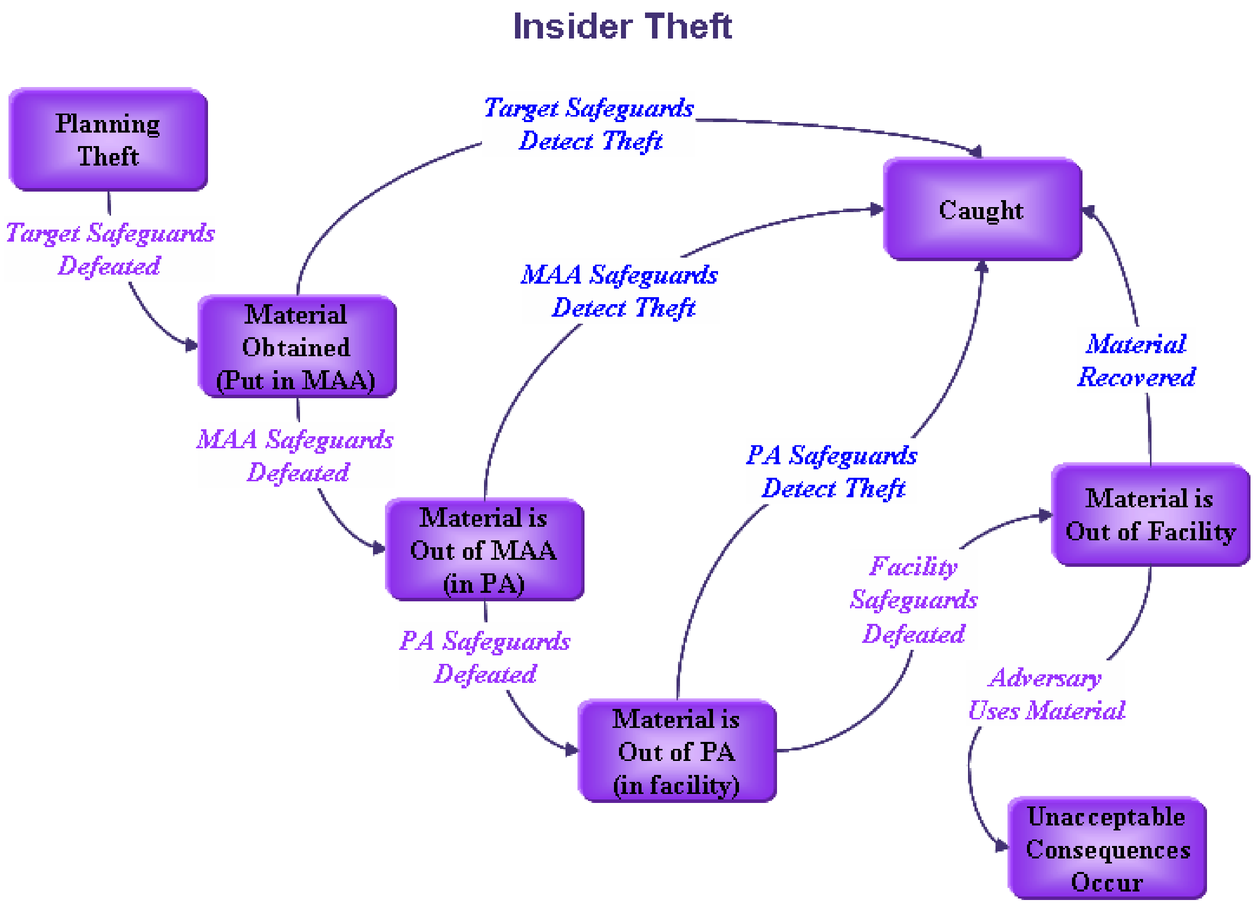
Insider Theft
Planning Theft
Target Safeguards Defeated
Material Obtained (Put in MAA)
Target Safeguards Detect Theft
Caught
MAA Safeguards Defeated
MAA Safeguards Detect Theft
Material is Out of MAA (in PA)
PA Safeguards Defeated
PA Safeguards Detect Theft
Material Recovered
Material is Out of PA (in facility)
Facility Safeguards Defeated
Material is Out of Facility
Adversary Uses Material
Unacceptable Consequences Occur

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

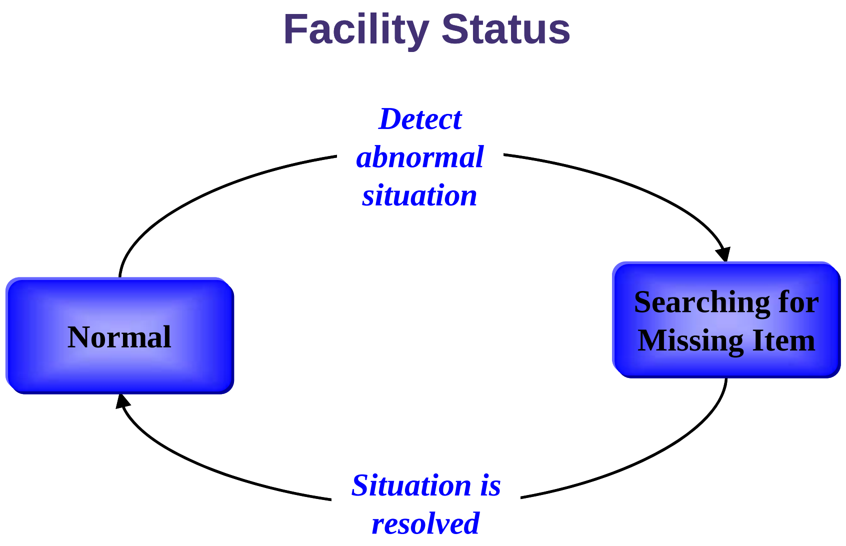

Figure 1b. State transition diagram for Facility Status Object.

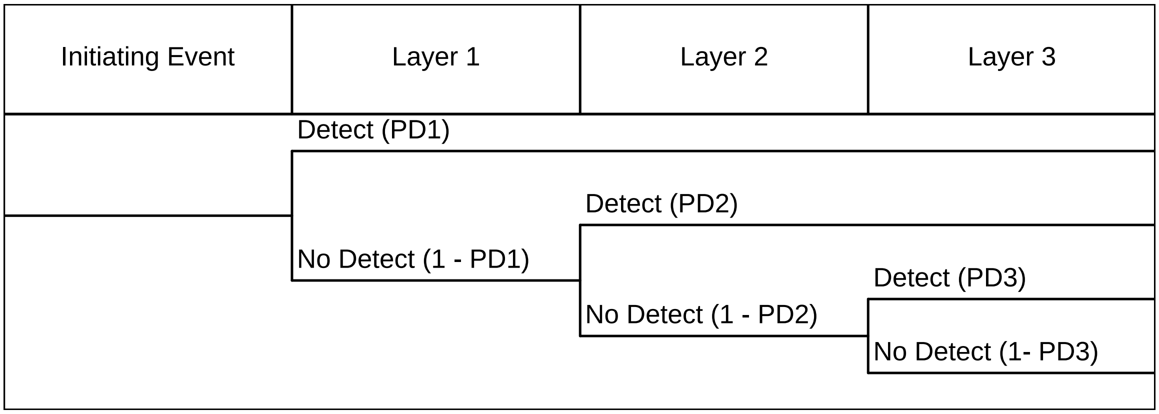

Figure 2a. Traditional event tree model of insider theft through PPS layers.

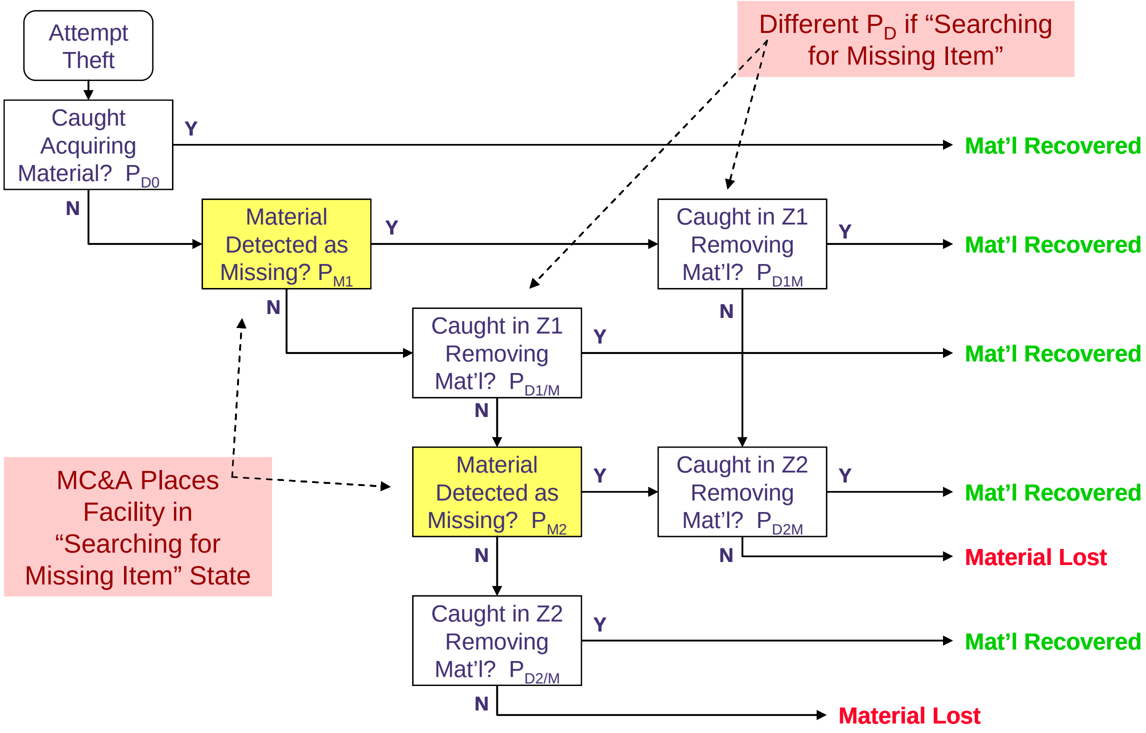
Attempt Theft
Caught Acquiring Material? P_{D0}
Y
N
Mat'l Recovered
Different P_D if "Searching for Missing Item"
Material Detected as Missing? P_{M1}
Y
N
Caught in Z1 Removing Mat'l? P_{D1M}
Y
N
Mat'l Recovered
Caught in Z1 Removing Mat'l? $P_{D1/M}$
Y
N
Mat'l Recovered
MC&A Places Facility in "Searching for Missing Item" State
Material Detected as Missing? P_{M2}
Y
N
Caught in Z2 Removing Mat'l? P_{D2M}
Y
N
Mat'l Recovered
Material Lost
Caught in Z2 Removing Mat'l? $P_{D2/M}$
Y
N
Mat'l Recovered
Material Lost

Figure 2. Insider theft modeled as an Event Sequence Diagram incorporating MC&A.

TIMING AND MC&A DECTECTION FOR INSIDER THEFT

One of the challenges for evaluating the effectiveness of an S&S protection system against an insider adversary is that 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. Thus, the detection and delay timelines determined for the outside adversary and the PPS are not as relevant. Characterizing the MC&A protection elements in a facility in terms of an object-based state machine provides a framework for defining timing and detection distributions for insider theft stages and facility alerts triggered by MC&A activities; these distributions 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 [4] and security timeline analyses [5].

As an insider initiates a theft 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 and emergency exit during an occasional evaualtion drill). These data are often available in the existing VA methodology data base. Distributions for a "Normal" facility state can be modified to reflect performance changes if an 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 material, and the adversary has a lower probability of successfully removing the material from a Physical Security Layer. The development of and sampling approaches for these timing distributions would also consider frequency of reoccurring administrative controls, for example, those listed in Table 1.

The last time variable, $T_{MC\&AAlert}$ represents the time when the Facility state transitions from "Normal" state to "Searching for Missing Material" state (Alert). Times and associated probability distributions [$P(T_{Alert})$] 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 (NPP) operations [6] 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. Additionally, detection probabilities for MC&A activities can be estimated from the human error probabilities that have been developed for similar types of activities at NPPs such as following procedures, administrative controls, and walk-around inspections.

MC&A activities contribute to the effectiveness of the facility protection system by providing alerts that material may be missing. For example, Table 1 lists examples of key administrative controls that provide reoccurring detection opportunities, with representative frequencies. 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 mathematics for probabilistic convolution were previously presented [1] and provide a basis to determine the probability that an MC&A alert (detection) causes the Facility to transition to the "Searching for Missing Material" state before the insider moves 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 [7] and ASSESS software programs [8] have been used to develop the facility model based on the description, and to do a preliminary insider analysis. These VA tools provide a systematic approach for evaluating safeguards and security effectiveness against theft or sabotage of nuclear material by different adversaries. ATLAS has superseded ASSESS as the key VA analysis tool with the most current facility and outsider assessment modules, up-to-date graphics, computational algorithms, and documentation capabilities. However, ATLAS does not yet include a complete analysis capability for nonviolent insider attacks, so ASSESS is used for the insider-specific analysis in this work.

The facility model was exported from ATLAS to ASSESS, where facility personnel and their access and authorities are selected to define the insider threats (examples provided in Table 2). The resulting insider scenarios include both continuous and discontinuous pathways, with respect to timing, and provide a basis for exercising the probabilistic timing and HRA methods. These scenarios, when finalized, will be modeled as ESDs with MC&A elements characterized by probabilistic timing and HEPs. The resulting ESDs will be quantified to determine an effectiveness of the system in thwarting each insider threat scenario.

Table 2. Insider Threats

Relative Ranking	Personnel Type	Facility Access	Target Access	Key Access	Important Authorities
1	Security Police	All	Frequent	All	Access to alarms Staffs security post Assesses security alarms
2	MBA Custodian	All	Frequent	Vault and Billet Cages	SNM transfers Sample transfers Performs inventories Access to container TIDs Access to MC&A records
3	Security Police Supervisor	All	Infrequent	All	Supervisory Access to alarms Access to badges

This work is ongoing. We continue to make progress in implementing the method. Initial modeling results using the ATLAS and ASSESS software indicate promising insider theft scenarios on which to exercise these new techniques. Additional work is focusing on selecting final insider theft scenarios, identifying applicable MC&A activities and developing applicable probability distributions for the timing and detection.

CONCLUSIONS

This paper has reviewed previous and presented the latest developments for a new method to incorporate MC&A protection elements within the existing probabilistic VA methodology to estimate the P_E for insider threats. Previous developments for elements of the method include the 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, the definition of possible timing distributions, and the use of probabilistic convolution. Recent advances further the coupling of the object-based paradigm with traditional PRA methods to incorporate the evaluation of MC&A elements in the existing VA methodology. These include the use of ESDs and HEPs for detection of missing material.

The combination of the elements in the method, as discussed in this paper, provides a probabilistic basis for applying this method for determining the effectiveness of the security system to protect nuclear materials against insider threats. In evaluating the initial modeling and analysis, we have observed that this method is likely to be beneficial for discontinuous timeline and protracted theft scenarios, but that current methods are likely adequate for abrupt insider theft scenarios. Also, the approaches we are using to characterize and evaluate MC&A activities demonstrate their importance as protection elements against these discontinuous or protracted scenarios.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the support of Dr. Sheldon Landsberger, Felicia's PhD Co-Advisor at The University of Texas at Austin.

REFERENCES

1. F.A. Durán and G.D. Wyss, "Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials," in *Proceedings of the 48th Annual Meeting of the Institute of Nuclear Materials Management,* Tucson AZ, July 16-20, Institute of Nuclear Materials Management, Deerfield IL, 2007.
2. P. G. Dawson and P. Hester, "Real-Time Effectiveness Approach to Protecting Nuclear Materials," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management*, Nashville TN, July 17-21, Institute of Nuclear Materials Management, Deerfield IL, 2006.
3. G. D. Wyss and F. A. Durán, "OBEST: The Object-Based Event Scenario Tree Methodology," SAND2001-0828, Sandia National Laboratories, March 2001.
4. "South Texas Project Probabilistic Safety Assessment," PLG-0675, Houston Lighting and Power Company, Houston TX, May 1989.
5. H. A. Bennett, "The EASI Approach to Physical Security Evaluation," SAND76-0500, Sandia National Laboratories, 1977.
6. 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.
7. ATLAS (Adversary Time-Line Analysis System) software, Version 4.2. Build 171, Developed at Sandia National Laboratories for the U.S. Department of Energy.
8. ASSESS Insider Module, Version 2.56, Copyright 1989-2003, Lawrence Livermore National Laboratory.