Proceedings of the ASME 2011 14th International Conference on Environmental Remediation and Radioactive Waste Management
ICEM2011
September 25-29, 2011, Reims, France

ICEM2011-59379

HUMAN RELIABILITY-BASED MC&A METHODS FOR EVALUATING THE EFFECTIVENESS OF PROTECTING NUCLEAR MATERIAL

Felicia A. Durán, Ph.D.*
Sandia National Laboratories
Albuquerque, NM, United States

Gregory D. Wyss, Ph.D.
Sandia National Laboratories
Albuquerque, NM, United States

ABSTRACT

Material control and accountability (MC&A) operations that track and account for critical assets at nuclear facilities provide a key protection approach for defeating insider adversaries. MC&A activities, from monitoring to inventory measurements, provide critical information about target materials and define security elements that are useful against insider threats. However, these activities have been difficult to characterize in ways that are compatible with the path analysis methods that are used to systematically evaluate the effectiveness of a site's protection system. The path analysis methodology focuses on a systematic, quantitative evaluation of the physical protection component of the system for potential external threats, and often calculates the probability that the physical protection system (PPS) is effective (P_E) in defeating an adversary who uses that attack pathway. In previous work, Dawson and Hester observed that many MC&A activities can be considered a type of sensor system with alarm and assessment capabilities that provide reccurring opportunities for "detecting" the status of critical items. This work has extended that characterization of MC&A activities as probabilistic sensors that are interwoven within each protection layer of the PPS. In addition, MC&A activities have similar characteristics to operator tasks performed in a nuclear power plant (NPP) in that the reliability of these activities depends significantly on human performance. Many of the procedures involve human performance in checking for anomalous conditions. Further characterization of MC&A activities as operational procedures that check the status of critical assets provides a basis for applying human reliability analysis (HRA) models and methods to determine probabilities of detection for MC&A protection elements. This paper will discuss the application of HRA methods used in nuclear power plant probabilistic risk assessments to define detection probabilities and to formulate "timely detection" for MC&A operations. This work has enabled the development of an integrated path analysis methodology in which MC&A operations can be combined with traditional sensor data in the calculation of PPS effectiveness. Explicitly incorporating MC&A operations into the existing evaluation methodology provides the basis for an effectiveness measure for insider threats, and the resulting P_E calculations will provide an integrated effectiveness measure that addresses both external and insider threats. The extended path analysis methodology is being further investigated as the basis for including the PPS and MC&A activities in an integrated safeguards and security system for advanced fuel cycle facilities.

INTRODUCTION AND BACKGROUND

The safeguards and security (S&S) protection system for a nuclear facility includes both a physical protection system (PPS) and material control and accounting (MC&A). The performance of a PPS 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 a systematic, quantitative evaluation of the physical protection component of the system for potential external threats, and often calculates the probability (P_E) that the PPS is effective in defeating an adversary who uses that attack pathway. MC&A elements, however, have been difficult to characterize in ways that are compatible with the path analysis methods. Explicitly incorporating MC&A protections into the existing S&S system evaluation provides the basis for an effectiveness measure for insider threats, and the resulting

[*] This work is based on Felicia's doctoral research, which was completed in December 2010 at The University of Texas at Austin.

insider and outsider P_E calculations together provide an integrated effectiveness measure that addresses both types of threats.

MC&A operations that track critical assets at nuclear facilities provide a key protection approach for defeating insider adversaries. Insiders represent the most capable of potential security threats to any organization. An insider is defined as anyone with knowledge of, access to, and authority at a facility. This definition implies that every employee in an organization is an insider, and any employee may pose an insider threat. Contractors, suppliers, vendors, and even visitors may also pose an insider threat. Of concern is a malicious insider who might attempt theft of critical assets, sabotage of equipment or operations, or other criminal activities. For theft or diversion of material, malicious insiders represent formidable threats because they have knowledge of and access to target materials and can interact directly with the target without being detected as well as take advantage of system vulnerabilities and opportunities to circumvent system elements. 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 evaluation of the S&S protection system.

MC&A activities, from monitoring to inventory measurements, provide critical information about target materials and define security elements that are useful against insider threats. 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 approach to evaluating a PPS (for example, material transfers from one PPS layer to another). Other MC&A elements, however, have been difficult to characterize in ways that are compatible with the path analysis methods that are used to systematically evaluate the effectiveness of a site's protection system.

In previous work, Dawson and Hester [1] observed that many MC&A activities have "sensing" characteristics that provide alarm and assessment capabilities of a detector. They developed a deterministic Material Assurance Indicator (MAI) algorithm to estimate a real-time effectiveness for protecting nuclear materials. Before this, neither measures nor standards for comparison were defined to determine whether a protection system provided effective control of nuclear materials, that is, the effectiveness of an MC&A system. Their initial testing for scenarios at hypothetical facilities demonstrated the MAI algorithm is applicable for evaluating MC&A system capability to provide detection of an active non-violent insider attempting theft or diversion of nuclear material. While the MAI provided a quantitative measure of MC&A effectiveness, it is nonprobabilistic and therefore not directly compatible with the probabilistic path analysis methodology.

The characterization of MC&A activities as having detection capabilities was a first step to incorporating MC&A activities as additional sensors in a site's protection system. In addition, a probabilistic basis is needed, specifically to determine an appropriate probability of detection (P_D) for MC&A protection elements. This work describes the application of human reliability analysis (HRA) methods and models for human performance of nuclear power plant (NPP) operations to develop detection probabilities for MC&A activities. In addition, an extended probabilistic path analysis methodology is summarized in which MC&A protections can be combined with traditional sensor data in the calculation of PPS effectiveness.

HUMAN RELIABILITY METHODS FOR MC&A ACTIVITIES

For HRA as a part of an NPP probabilistic risk assessment (PRA) Swain and Guttmann [2] developed a handbook that includes methods, models, and estimated human error probabilities (HEPs) to address human performance of NPP operations. Within the handbook, the authors address checking operations as recovery factors for which dependency is an important characterstic. A recovery factor is defined as "an element of an NPP system that acts to prevent deviant conditions from producing unwanted effects" [2, p. 19-1]. Human redundancy is a type of recovery factor that occurs when one person checks his or her own work or another person's work, detects an error that has occurred and corrects it. The handbook describes a variety of checking operations used in an NPP. Some may involve checking of routine tasks with or without a written checklist that recur on a regular basis performed by the same or different persons. Others may involve one person checking another person's work; special short-term, one-of-a-kind checking with alert factors; or special measurement tasks.

MC&A Activities as NPP Checking Operations

MC&A activities have many characteristics similar to operator tasks performed in an NPP in that the reliability of these activities depends significantly on human performance. Many of the procedures involve human performance in checking for anomalous conditions. As an example, checking the status of a valve in an NPP is similar to checking the status of target material in a vault. The respective associated anomalous conditions are that a valve should be closed but is partially or completely open (perhaps after a maintenance activity), and that a target in a vault is not where it should be located. Both can be characterized as checking procedures, in which an identified checking opportunity exists, and a person discovers or fails to discover an anomalous condition. Further characterization of MC&A activities as procedures that check the status of critical assets provides a basis for applying HRA models and methods to determine probabilities of detection for

MC&A protection elements. Table 1 identifies MC&A activities and similar characteristics of operator tasks identified by Swain and Guttman [2, Table 19-1]. The table also includes an estimated baseline HEP (BHEP) associated with the NPP operator tasks as determined by the HRA work of Swain and Guttman [2]. These estimated BHEPs can be applied to MC&A protection elements – the probability of detection is defined as the complement of the BHEP for performing a given MC&A activity.

Dependence of Recurring MC&A Activities

Within a PPS, sensor elements are designed to detect unauthorized activity. This work has provided additional insights to the characterization of MC&A activities as sensors within a site's protection system. MC&A activities are actually interwoven within each protection layer of the PPS and provide additional detection and delay opportunities within the S&S protection system. These activities are important protection elements against insider theft and can serve to discourage malicious insider activity. They provide many, often recurring opportunities to observe the status of critical items (for example, *daily* administrative checks). As an example, Table 2 lists some key administrative MC&A activities that are performed on a recurring basis. A year-long detection opportunity timeline can be constructed from the compilation of the recurrence of these activities and demonstrates the importance of these activities as protection elements against insider threats.

Table 1. Characterization of MC&A activities as different types of NPP checking operations estimated probabilities (HEPs) that a checker will fail to detect an error (columns 2 and 3 from [2, Table 19-1])

MC&A Activity	**Nuclear Power Plant Checking Operation**	**BHEP**
Plan of the Day	Checking routine tasks using written materials	0.10
Material Measurement	Checking that involves active participation, such as special measurements	0.01
Forms Reconciliation	Special short-term, one-of-a-kind checking with alerting factors	0.05
Process Call	Special short-term, one-of-a-kind checking with alerting factors	0.05
Material Request	Checking routine tasks using written materials	0.10
Material Transfer	Checking by reader/checker of the task performer in a two-man team, or checking by a second checker, routine task	0.50
Product Storage	Checking by reader/checker of the task performer in a two-man team, or checking by a second checker, routine task	0.50
Daily Administrative Check	Checking routine tasks using written materials	0.10
Physical Inventory	Checking that involves active participation, such as special measurements	0.01
Inventory Audit	Checking that involves active participation, such as special measurements	0.01

In this work, MC&A activities have been characterized as a type of human redundancy recovery factor. Generally, MC&A activities would be considered independent events. However, because many of the MC&A activities are recurring, it is important to consider and to understand the dependence between the recurrences of the same activity or between the occurrences of two different activities and whether they are performed by the same or different persons. Dependence is a characteristic used in HRA methods to consider how the success or failure of a subsequent task depends on the success or failure of the immediately preceding task.

The failure to address the issues of dependence "may lead to an optimistic assessment of joint HEPs for NPP tasks" [2, p. 10-1]. One method for assessing dependence is a positive dependence model for estimating conditional probabilities for two tasks. Positive dependence "implies a positive relationship between events, that is…failure on the first task increases the probability of failure on the second task" [2, p. 10-4]. The positive dependence model can also be applied even in

Table 2. 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
Inventory Audit	365

situations where actual data on conditional probabilities of success or failure in the performance of tasks is not available.

Equation 1 provides the failure equation that is used to calculate the conditional probability of failure on Task M given failure on the previous Task M-1 for different levels of dependence. The general formulation for the failure equation is:

$$P(F_M \mid F_{M-1}) = \frac{1 + aP_{M-1}}{a+1} \tag{1}$$

where a ranges from 0 to ∞. Values of a equal to ∞, 19, 6, 1, and 0 correspond, respectively, to points of zero, low, moderate, high and complete positive dependence [2, Equations 10-14 through 10-18].

To explore dependence that may generally be associated with recurring MC&A activities, the failure equation for the positive dependence model from Swain and Guttmann [2] was applied for one daily MC&A activity that occurs over a 30-day period. Figure 1 shows how the daily probability of MC&A detection varies across five different levels of dependence for a low (0.02) initial probability of detection (complement of the BHEP for a type of NPP operation associated with a specific MC&A activity). This plot demonstrates how, in most cases of human performance, it is expected that a person performing a recurring activity has a decreasing likelihood of successfully detecting an anomaly given that the previous opportunity has failed. With no dependence between recurring MC&A activities, the initial probability of detection is maintained over the 30-day timeline. The decrease in probability of detection for each subsequent recurrence of the same activity or of two activities, however, will vary with the level of dependence between the two activities.

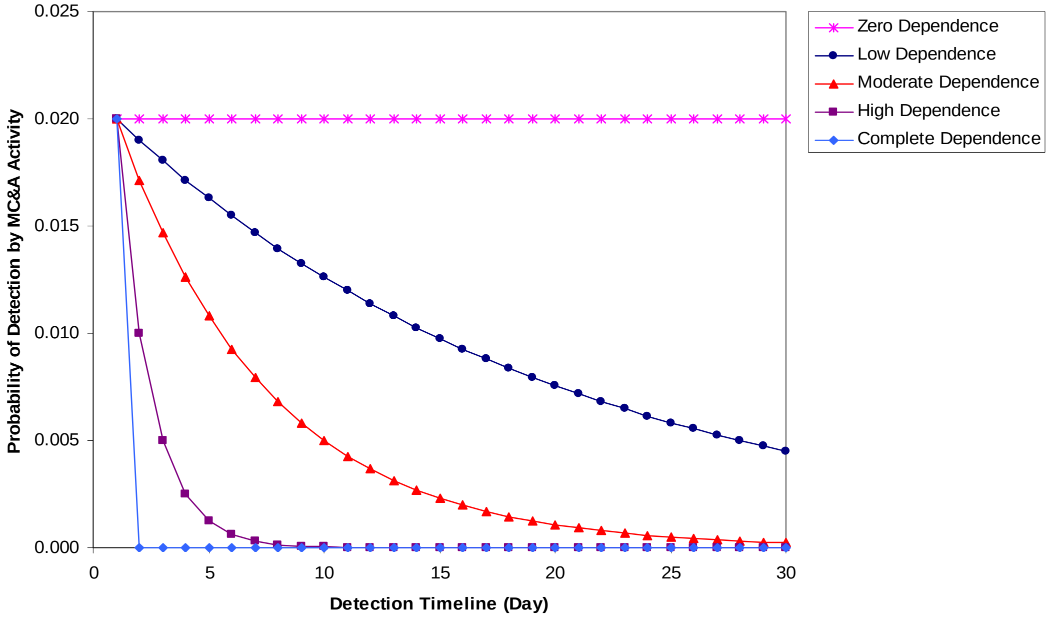

Figure 1. Daily probability of detection over a 30-day period for one MC&A activity performed once a day based on a BHEP of 0.98, or an initial probability of detection of 0.02, for five different levels of dependence.

TIMELY DETECTION

With the existing path analysis method, detection, delay and response timelines for a PPS are evaluated to determine timely detection. For each path, the probability P_E is calculated to determine if the PPS achieves timely detection and is effective in defeating an adversary who uses that attack pathway. This work has developed several elements to provide a probabilistic basis for extending the existing path analysis method to incorporate MC&A activities [3].

In the extended methodology, an object-based state machine was developed as a basis for characterizing insider theft as a race analogous to the characterization of an outsider attack as a race between the adversary and facility response after detection has occurred. For MC&A activities, the race is between the stages of an insider theft scenario and the MC&A "sensor" systems that transition a facility from a normal state to a heightened alert state having additional detection opportunities. MC&A activities contribute to the effectiveness of the facility protection system by providing alerts that material may be missing. While timely detection for a PPS depends on detection, delay and response that interrupts and neutralizes an attack from an outside adversary, timely detection for MC&A activities depends on detecting that material is not where it should be and providing an alert. The mathematics for probabilistic convolution provide a basis to determine the probability that an MC&A alert (detection) occurs before the insider moves the material past a given physical protection layer. The effectiveness of MC&A activities can be determined by convolving the probability distributions for the MC&A detection timeline with the insider theft timeline to determine the probability that detection occurs before the theft of material can be completed.

Formulation of Timely MC&A Detection

In demonstrating the application of HRA methods for determining a probability of detection for MC&A activities above, only the MC&A detection timeline (in this example for a 30-day scenario) was described without considering the insider adversary theft stages. To implement timely detection, the MC&A detection timeline must be convolved against the insider adversary theft timeline. MC&A activities provide recurring opportunities to detect that material is "missing" such that the facility state transition occurs from normal state to alert state. Because MC&A activities are usually discrete observations, discrete mathematics and discrete probability distributions are appropriate. The frequency of recurrence for MC&A activities (Table 2) is determined in days, this formulation uses one day as the discretization time step. Other discretization time steps could also be used if appropriate based on the frequency of MC&A activities or theft opportunities. If material is detected as missing on day *n* and the material has not been removed from the facility before day *n,* then detection will be timely. To formulate the probability of timely detection by MC&A activities, $P_{D,Timely}$ is the overall cumulative daily probability of timely detection over the scenario timeline of *N* days:

$$P_{D,Timely} = \sum_{n=1}^{N} P_{D,Timely,n} \quad (2)$$

$P_{D,Timely}$ is the sum of MC&A detection that occurs exactly on day *n* and is timely, that is detection happens before the insider moves the material out of the physical protection layer. $P_{D,Timely,n}$, the probability of timely detection on a given day *n,* is given by:

$$P_{D,Timely,n} = P_{DEn} \times P_{NTn} \quad (3)$$

where,

P_{DEn} = the probability that the facility detects material is missing on exactly day *n*

P_{NTn} = the probability that the material has not been removed from the facility before day *n*

P_{NTn} is the complementary cumulative probability that the theft occurred on day *n,* P_{Tn}:

$$P_{NTn} = 1 - \sum_{i=1}^{n-1} P_{Ti} \quad (4)$$

P_{Tn} is the daily probability of theft and is determined from the theft opportunity timeline. For example, if an insider has an equal opportunity to take material once per day over a 30-day time period, then the insider theft timeline is defined as a uniform distribution, and

$$P_{Tn} = \frac{1}{30} = 0.033 \quad (5)$$

P_{Tn} is determined for various timeline scenarios based on the type of insider and his or her access to the target material.

Further, because detection on exactly day *n* implies that the material has not been detected as missing before day *n* and is detected as missing on day *n,* P_{DEn} is defined as:

$$P_{DEn} = P_{D,MC\&A,n} \times P_{ND,n-1} \quad (6)$$

where,

$P_{D,\,MC\&A,n}$ = the probability of detection for the MC&A activities on the *n*th day

$P_{ND,n-1}$ = the probability that the material has not been detected as missing before day *n*

The detection probabilities for MC&A activities can be determined as described previously by characterizing individual activities as associated NPP operations, defining applicable BHEPs, and dependency relationships. The MC&A detection probabilities are the complements of the BHEPs. An MC&A detection timeline for a given scenario is defined as the set of MC&A activities that are performed on a day to day basis.

$P_{ND,n-1}$, the probability that the material has not been detected as missing before day *n*, is defined as:

$$P_{ND,n-1} = 1 - P_{D<n} \quad (7)$$

$P_{D<n}$ is the cumulative probability that the facility detects material is missing (cumulative P_{DEn}) up to day *n-1*:

$$P_{D,n} = \sum_{i=1}^{n-1} P_{DEi} \quad (8)$$

Thus, combining Equations 2 through 8, the overall cumulative daily probability of timely detection over the scenario timeline of *N* days is given by:

$$P_{D,Timely} = \sum_{n=1}^{N} P_{D,MC\&A,n} \times \left(1 - \sum_{i=1}^{n-1} P_{DEi}\right) \times \left(1 - \sum_{i=1}^{n-1} P_{Ti}\right) \quad (9)$$

Previous work [4] provides a detailed example calculation of the values for each of the probabilistic parameters required to determine the probability of timely detection for one MC&A activity performed once a day in one physical protection layer over a 30-day time period for a moderate level of dependence between recurrences and a BHEP of 0.98. The associated scenario has the insider adversary's opportunity to remove target material occur once every day, and the adversary will make a decision during this time period as to which day will be most advantageous to remove the material from this physical protection layer. Thus, for this example, the daily probability of insider theft is defined as a uniform distribution. The daily MC&A probability of detection is calculated from Equation (9) with $P_{D,\,MC\&A,n}$ determined by Equation (1) for *a*=6 and an initial probability of detection equal to 0.02 (1-BHEP). The example scenario is one of several analyses completed to formulate timely MC&A detection. For the 30-day scenario of one daily MC&A activity in one physical protection layer and a uniform insider theft timeline, calculations of timely MC&A detection were also completed for the five different levels of dependence, for a low (0.02), medium (0.50) and high (0.99) initial probability of detection.

Figure 2 shows the cumulative daily probability of detection that could be achieved by one daily MC&A activity within one physical protection layer over the scenario timeline. As dependence between MC&A observations decreases, the cumulative daily probability of detection improves significantly over the initial probability of detection, in this case a low initial value of 0.020. Table 3 summarizes the increase in the cumulative daily probability of detection after 30 days for each of the initial probabilities of detection and for each of the five dependence levels. Because of the multiple detection opportunities, even an activity with a low initial probability of detection can achieve a significantly higher cumulative detection if the adversary timeline is extended and the dependence between recurrence of MC&A activities is reduced. A more than 10-fold increase is evident for an activity that has 0.02 initial probability of detection and zero dependence between recurrences. The cumulative daily probability of detection is the value that is used for MC&A detection events in each physical protection layer to calculate the overall effectiveness for each adversary path scenario.

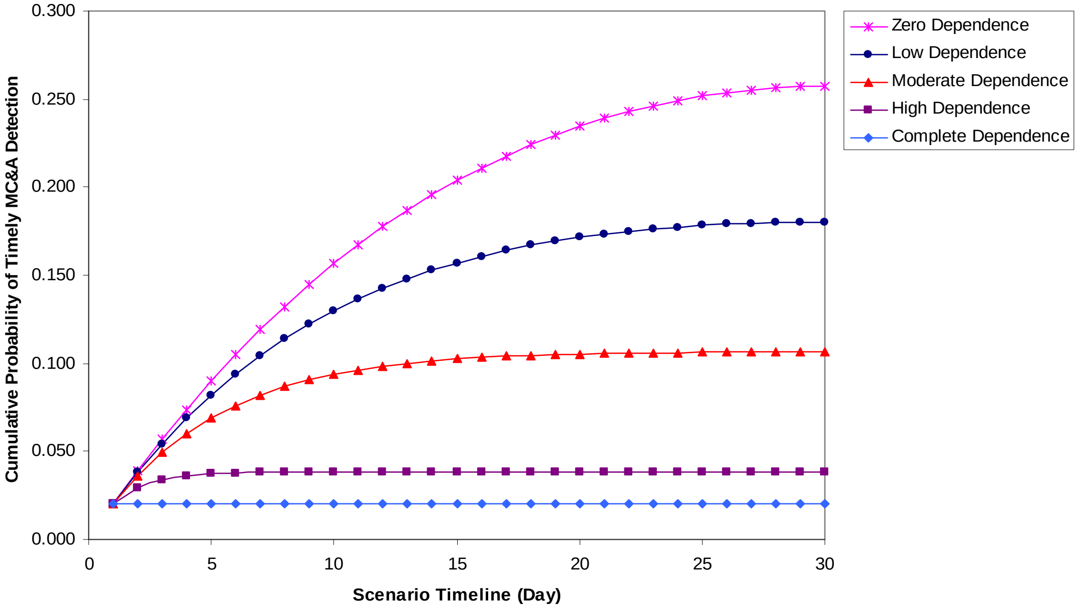

Figure 2. Cumulative daily probability of timely detection over a 30-day scenario timeline for one MC&A activity performed once a day based on a BHEP of 0.98, or an initial probability of detection of 0.02, for five different levels of dependence.

EXTENDED PATH ANALYSIS – MULTIPLE PHYSICAL PROTECTION LAYERS

The extended path analysis methodology developed in this work includes several elements. An object-based state machine paradigm is applied within which an insider theft scenario races against MC&A "sensor" systems that move a facility from a normal state to a heightened alert state having additional detection opportunities. This object-based state machine provides the framework for addressing the protracted and discontinuous insider theft timelines. Event sequence diagrams (ESDs) describe insider paths of each theft scenario through the PPS and also incorporate MC&A activities as events in each physical protection layer. The ESDs provide a framework for propagating probability values to determine the effectiveness of detecting missing material for a given path. As described above, HRA models and methods used in NPP PRA are applied to define detection probabilities for MC&A activities. Theft opportunity timelines and MC&A detection timelines are defined, and probabilistic convolution is performed to calculate an overall probability of detection for MC&A activities that is incorporated into the ESD for each PPS protection layer.

Table 3. 30-day cumulative probability of MC&A detection for five dependence levels for low (0.20), medium (0.50), and high (0.99) initial probability of detection

Initial Probability of Detection	Level of Dependence				
	Complete	High	Moderate	Low	Zero
0.02	0.020	0.038	0.106	0.180	0.258
0.50	0.500	0.699	0.939	0.963	0.967
0.99	0.990	0.997	0.999	0.999	0.999

The example above for the formulation of timely detection demonstrates extended path analysis for one daily MC&A event and a single theft timeline that could be incorporated in a single physical protection layer. Figure 3 illustrates an ESD for three physical protection layers and five events – three PPS protection elements and two MC&A activities (gold boxes).

The MC&A events are included in each internal physical protection layer in the ESD. Figure 3 also provides an illustration of how the ESD 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. The ESD represents the paths of insider theft, incorporates MC&A activities within each layer, and provides a framework for propagating probability values to determine effectiveness for detecting missing material.

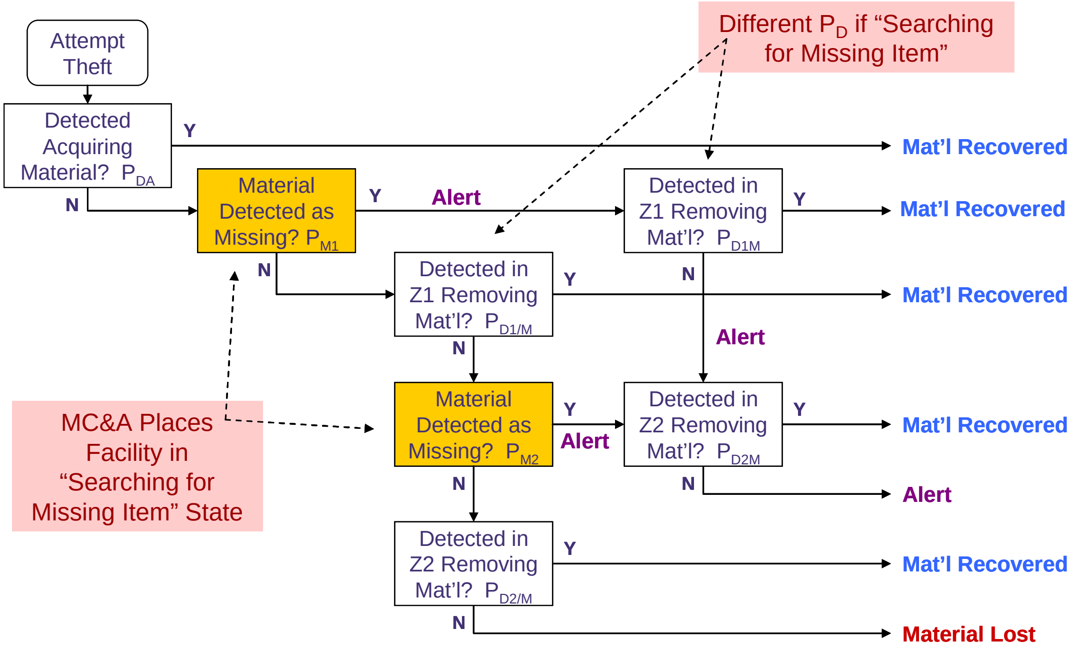
Attempt Theft
Detected Acquiring Material? P_{DA}
Y
N
Material Detected as Missing? P_{M1}
Y
Alert
N
Detected in Z1 Removing Mat'l? P_{D1M}
Y
N
Alert
Detected in Z1 Removing Mat'l? $P_{D1/M}$
Y
N
Material Detected as Missing? P_{M2}
Y
Alert
N
Detected in Z2 Removing Mat'l? P_{D2M}
Y
N
Detected in Z2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

Figure 3: Insider theft modeled as an ESD incorporating MC&A.

Along with the examples discussed in this paper, other analyses have been completed to demonstrate the extended path analysis methodology, including several combinations of 5-day, 30-day, and 90-day composite timelines for multiple security layers, with both uniform and variable theft timeline distributions, including a geometric distribution that was evaluated using Latin Hypercube Sampling. In addition, calculations for sets of MC&A activities that occur at different time intervals have been completed. The calculation of timely detection becomes more complex as the number of security layers increases and more MC&A detection activities are considered. Methods are required for probabilistic inference to determine the values of timely MC&A detection for layers two and beyond and for composite timelines determined from the timelines for each physical protection layer. An example of step-by-step extended path analysis calculations for an insider theft scenario at a hypothetical facility through multiple physical protection layers is provided in [5].

INTEGRATING MC&A EFFECTIVENESS FOR SAFEGUARDS PERFORMANCE

The extended path analysis methods described in this paper are also being applied for integrated safeguards and security modeling. The Separations and Safeguards Performance Model (SSPM) [6] has been developed to design and evaluate advanced monitoring strategies for future nuclear facilities. The SSPM is a transient reprocessing plant model in Matlab Simulink based on a UREX+ reprocessing plant. Elemental and bulk material flows are tracked throughout the various unit functions in a plant. Measurement blocks are used to simulate materials accountancy and process monitoring instrumentation, and the data generated is used to perform inventory differences as the model runs. Various approaches have been considered including integration of process monitoring data and utilization of advanced measurement technologies for tracking plutonium throughout the entire plant. Some of the latest model development and simulation analyses have focused on integrating material measurements, MC&A procedures, process monitoring and physical protection [7].

For the front end and extraction processing material balance areas, a physical protection design has been incorporated in the SSPM to set up pathways for material diversion assuming an insider theft scenario. The system architecture has been developed to integrate traditional materials accountancy measurements, process monitoring measurements, physical protection elements, and MC&A administrative procedures to determine improvements in system response to material loss. The SSPM has been used to design and test the system under various diversion scenarios and to explore and demonstrate how the various subsystems contribute to improve material tracking and detection of material theft or diversion. The approach developed in the extended path analysis methods for having an MC&A detection trigger an alert state for the facility has also been implemented in the SSPM modeling and simulation for MC&A administrative procedures as well as for process monitoring and material accountancy measurements. The latest simulation analyses demonstrate how any of these three subsystems might trigger an alarm and subsequent detection in the physical protection system. Preliminary results from the SSPM modeling and simulation demonstrate that process monitoring and MC&A administrative procedures can contribute to improvements in triggering alarms when material diversion occurs.

CONCLUSION

This work has demonstrated the application of HRA methods used in NPP PRAs for defining detection probabilities for MC&A activities. The approaches used to characterize and evaluate MC&A activities highlight their importance as protection elements for insider theft. In addition, this work has identified three key MC&A factors that can be manipulated to enhance the effectiveness of MC&A as a "sensor" within the larger PPS. The overall MC&A detection probability can be increased by proper selection of MC&A activities. The effectiveness of subsequent observations can also be increased by reducing the dependence between observations through the use of HRA and human factor techniques. Finally, steps can be taken to lengthen the adversary's timeline by reducing the frequency of potentially vulnerable states and providing more opportunities for MC&A detection.

Defining MC&A detection probabilities has supported the probabilistic basis for and enabled the development of an extended path analysis methodology in which MC&A protections can be combined with traditional sensor data in the calculation of PPS effectiveness. In evaluating the initial modeling and analysis, it is evident that these methods are most applicable for protracted theft and discontinuous timeline scenarios – current methods are adequate for abrupt theft scenarios. Explicitly incorporating MC&A protection into the existing S&S system evaluation provides the basis for an effectiveness measure for insider threats. The resulting P_E calculations provide an integrated effectiveness measure that addresses both outsider and insider threats.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support of Dr. Sheldon Landsberger, Felicia's doctoral Co-Advisor at The University of Texas at Austin. Thanks to Ben Cipiti, Rebecca Ward, and Brad Key for their collaboration on further development of these methods for the application to advanced fuel cycle facilities, Pamela Dawson for her contributions on insider analysis, MC&A, and MAIs at the outset of this work, and John Darby for the much needed instruction on probabilistic convolution.

Sandia National Laboratories is a multi program laboratory managed and 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. SAND2011-4906C, approved for unclassified/unlimited release.

REFERENCES

[1] 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*, Institute of Nuclear Materials Management, Deerfield IL, 2006.

[2] A.D. Swain III and H.E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants," SAND80-0200, Sandia National Laboratories, Albuquerque NM, 1983.

[3] F.A. Durán and G.D. Wyss, "Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials," in *Proceedings of the 49th Annual Meeting of the Institute of Nuclear Materials Management*, Institute of Nuclear Materials Management, Deerfield IL, 2008.

[4] 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," presented at the 10th International Probabilistic Safety Assessment and Management Conference, June 7-11, Seattle WA, 2010.

[5] F.A. Durán G.D. Wyss, and B.B. Cipiti, "Extended Probabilistic Path Analysis to Evaluate the Performance of Protection Systems Against Insider Theft," in *Proceedings of the 52th Annual Meeting of the Institute of Nuclear Materials Management*, Institute of Nuclear Materials Management, Deerfield IL, 2011.

[6] B.B. Cipiti, "Separations and Safeguards Performance Modeling for Advanced Reprocessing Facility Design," *Journal of Nuclear Materials Management,* 39/2 pp. 4-14, March 2011.

[7] B.B. Cipiti, F.A. Durán, B. Middleton, and R. Ward, "Fully Integrated Safeguards and Security for Reprocessing Plant Monitoring," Sandia National Laboratories, 2011.