SAND2012-4811C

Extended Probabilistic Path Analysis to Evaluate Operational Strategies to Mitigate Insider Adversaries*

Felicia A. Durán and Gregory D. Wyss
Security Systems Analysis – Sandia National Laboratories
P.O. Box 5800, MS 0757, Albuquerque, NM 87185-0757

ABSTRACT

Material control and accounting (MC&A) safeguards operations that track and account for critical assets at nuclear facilities provide a key protection approach for defeating insider adversaries. Probabilistic risk assessment (PRA) methods have been applied to develop an extended probabilistic path analysis methodology in which MC&A protections can be combined with detection by physical protection system (PPS) elements in the calculation for effectiveness of a site's protection systems against insider theft. MC&A activities have many similar characteristics to operator procedures performed in a nuclear power plant (NPP) to check for anomalous conditions. To address the performance of MC&A activities, human reliability analysis (HRA) methods and models for NPP operations have been applied to characterize detection capabilities for MC&A activities. The extended path analysis methodology models insider theft as a race against detection by facility MC&A activities. The HRA techniques are applied to characterize detection and delay timelines for MC&A protection, and convolution mathematics are applied to calculate timely MC&A detection. Event sequence diagrams (ESDs) are applied to incorporate MC&A activities as path elements and to develop evaluation scenarios for insider paths through layers of the PPS. Previous work demonstrated the extended path analysis method with analyses of a hypothetical theft scenario for a single MC&A activity integrated through multiple PPS layers. This effort will review the extended path analysis methods and present analyses for a set of MC&A activities through multiple PPS layers. The analysis will demonstrate how operational strategies might be considered for mitigating the insider threat.

INTRODUCTION AND BACKGROUND

Material control and accountability (MC&A) operations for monitoring, measuring and tracking critical assets at nuclear facilities provide critical information about target materials and a key protection approach against the insider threat. For theft or diversion of material, malicious insiders represent formidable threats because they can have knowledge of and access to target materials. They can take advantage of opportunities to circumvent system elements, take advantage of system vulnerabilities, and interact directly with the target without being detected. 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 a site's protection system.

The insider threat is most often addressed as part of the evaluation of a facility's PPS. A PPS is evaluated using probabilistic analysis of adversary paths on the basis of detection, delay, and response timelines to determine timely detection. Because insider adversaries have various levels of access to, knowledge of, and authority for facility operations, a PPS actually provides minimal protection against the insider threat. 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). 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.

* 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. SAND2012-XXXXC, approved for Unclassified/Unlimited Release.

This paper presents a new approach to incorporate MC&A protection elements explicitly in the existing probabilistic path analysis methodology [1]. Previous work [2] observed that many MC&A activities have "sensing" characteristics with alarm and assessment capabilities of a detector. Characterization of MC&A activities as having detection capabilities is the basis for incorporating MC&A activities as additional sensors in a site's protection system. This work has established a probabilistic basis for extending the existing path analysis method to incorporate the additional detection capabilities of MC&A activities [1, 3]. Previous papers describe the use of human reliability analysis (HRA) methods to determine an appropriate probability of detection (P_D) for MC&A protection elements and the formulation of timely MC&A detection [4]; provide calculations of the values for each of the probabilistic parameters required to determine the probability of timely detection for a one MC&A activity in a single PPS layer for a single timeline [3]; and demonstrate the extended path analysis for one MC&A activity and multiple PPS layers [5]. This paper reviews the extended path analysis methods and presents analyses for a set of MC&A activities through multiple PPS layers. The analyses demonstrate how operational strategies might be considered for mitigating the insider threat.

EXTENDED PATH ANALYSIS METHODS

The extended path analysis methodology developed in this work includes several elements. An object-based state machine paradigm models an insider theft scenario as a race against the MC&A "sensor" system that moves a facility from a normal state to an alert state. The 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 incorporate MC&A activities as events in each PPS layer. HRA methods and models for nuclear power plant (NPP) operations have been applied to determine MC&A detection probabilities. Theft opportunity timelines and MC&A detection timelines are defined, and probabilistic convolution is performed to calculate an overall probability of timely MC&A detection that is incorporated into the ESD for each PPS protection layer. The ESDs provide a framework for propagating probability values to determine the effectiveness of detecting missing material for a given path.

ESD for Multiple PPS layers

Figure 1 is an ESD for three PPS layers and five events – three PPS protection elements and two MC&A activities (gold boxes). The MC&A events are included in each PPS layer in the ESD. Figure 1 also provides an illustration of how the ESD indicates where MC&A activities trigger a change of facility state from normal to "alert," where the facility is searching for "missing" material. This state change is modeled using different detection probabilities for the normal and alert facility states for subsequent events. The ESD represents the paths for insider theft, incorporates MC&A activities in each layer, and provides a framework for propagating probability values to determine effectiveness for detecting missing material.

Human Reliability Methods for MC&A Activities

HRA methods for probabilistic risk assessment (PRA) of an NPP(NPP [6] provide models and estimated human error probabilities (HEPs) to address human performance of NPP operations. These methods have been applied as the basis for determining a P_D for MC&A activities. 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. 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 different types of checking operations identified by Swain and Guttman [6, Table 19-1]. 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. 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 [6]. These estimated BHEPs can be applied to MC&A protection elements – P_D is defined as the complement of the BHEP for performing a given MC&A activity.

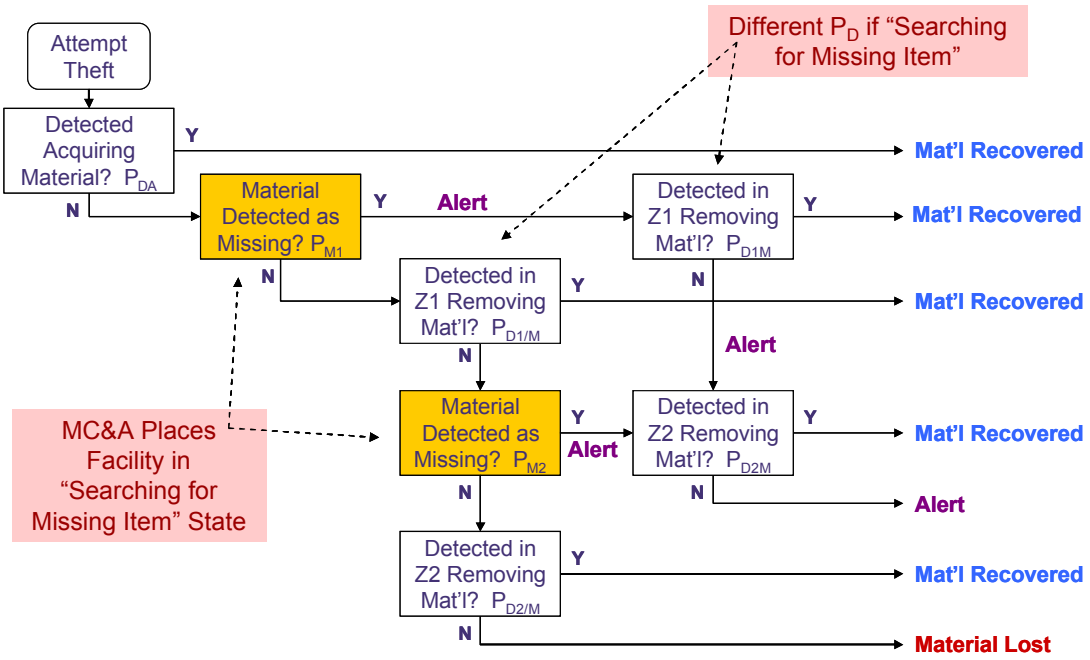

Figure 1: Insider theft modeled as an ESD incorporating MC&A detection events.

Table 1. Nuclear power plant checking operations and estimated probabilities (HEPs) that a checker will fail to detect an error [6, Table 19-1]

Nuclear Power Plant Checking Operation	**BHEP**
Checking routine tasks using written materials	0.10
Checking that involves active participation, such as special measurements	0.01
Special short-term, one-of-a-kind checking with alerting factors	0.05
Special short-term, one-of-a-kind checking with alerting factors	0.05
Checking routine tasks using written materials	0.10
Checking by reader/checker of the task performer in a two-man team, or checking by a second checker, routine task	0.50
Checking by reader/checker of the task performer in a two-man team, or checking by a second checker, routine task	0.50
Checking routine tasks using written materials	0.10
Checking that involves active participation, such as special measurements	0.01
Checking that involves active participation, such as special measurements	0.01

Within a PPS, sensor elements are designed to detect unauthorized activity. This work has provided additional insights to characterize MC&A activities as additional 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 a site'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 provides a notional set of MC&A activities that would be performed on a recurring basis at different frequencies. 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 2: Notional set of MC&A activities and their performance frequencies

Notional MC&A Activity	Activity Frequency (days)
MC&A Activity 1	1
MC&A Activity 2	1
MC&A Activity 3	3
MC&A Activity 4	15
MC&A Activity 5	30
MC&A Activity 6	365

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

Equation 1 provides the failure equations for positive dependence that are used to calculate conditional probabilities 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:

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

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 [6, Equations 10-14 through 10-18].

The dependence generally associated with recurring MC&A activities was determined by applying the positive dependence model for one daily MC&A activity that occurs over a 30-day period. Figure 2 shows the daily probability of MC&A detection for five different levels of dependence for a low (0.02) initial P_D (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 a previous opportunity has failed. With no dependence between recurring MC&A activities, the initial P_D is maintained over the 30-day timeline. The decrease in P_D for each subsequent recurrence of the same activity or of two activities, however, will vary with the level of dependence between the two activities, as shown in Figure 2.

Timely Detection

The existing path analysis method evaluates the PPS for a facility on the basis of detection, delay and response timelines using probabilistic analysis of adversary paths to determine timely detection. Path analysis calculates the probability P_E that 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 similar 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 an 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

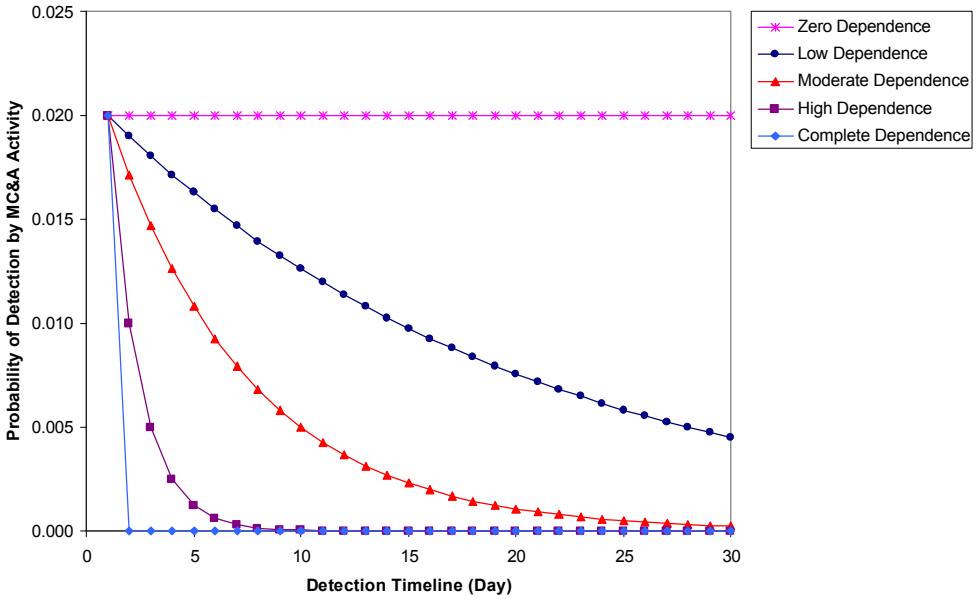

Figure 2: Daily P_D for a 30-day period for one MC&A activity performed once a day with a BHEP of 0.98, or an initial P_D of 0.02, for five different levels of dependence.

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. 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 PPS layer. The effectiveness of MC&A activities is 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 P_D 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. Because 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. The overall cumulative daily probability of timely detection over a scenario timeline of *N* days:

$$P_{D,Timely} = \sum_{n=1}^{N} P_{D,MC\&A,n} \times \left(1 - \sum_{i=1}^{n-1} P_{DEi}\right) \times \left(1 - \sum_{i=1}^{n-1} P_{Ti}\right) \qquad (2)$$

where,

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

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

P_{NTi} = the daily probability of theft and is determined from the theft opportunity timeline

Previous work [3] 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 PPS 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 PPS layer. Thus, for this example, the insider theft opportunity timeline is defined as a uniform distribution. The daily MC&A P_D is calculated from Equation (1) with a=6 and an initial P_D equal to 0.02 (1-BHEP). This example is one of several analyses completed to formulate timely MC&A detection. Figure 3 shows the cumulative daily P_D that could be achieved by one daily MC&A activity within one PPS layer over the scenario timeline. As dependence for an MC&A activity decreases, the cumulative daily P_D improves significantly over the initial P_D, in this case a low initial value of 0.020. Because of multiple daily detection opportunities, even an activity with a low initial P_D can achieve a significantly higher cumulative detection probability 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 P_D and zero dependence between recurrences. The cumulative daily P_D is the value that is used for MC&A detection events in each PPS layer to calculate the overall effectiveness for an insider path.

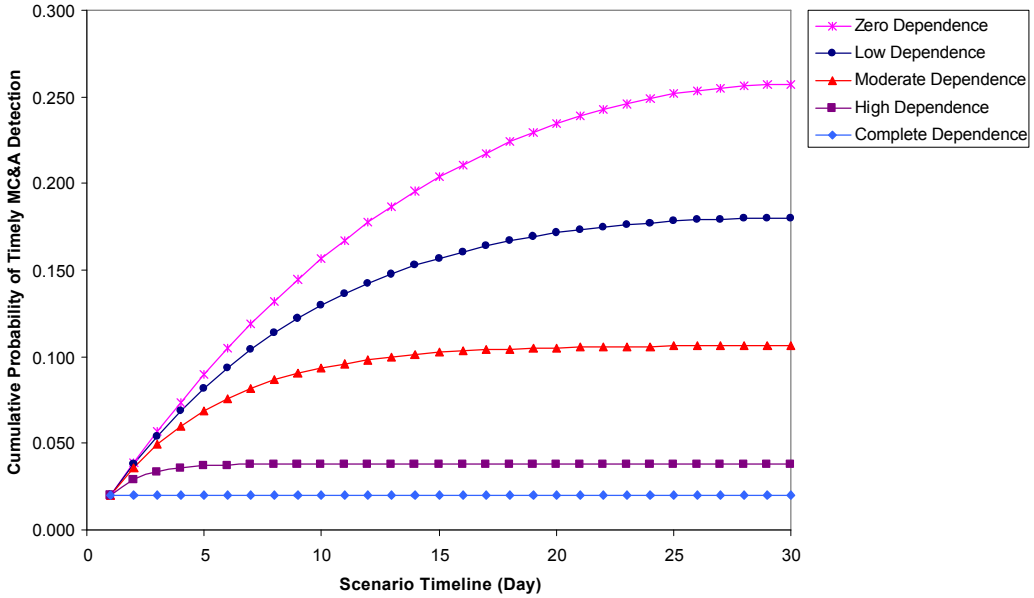

Figure 3: Cumulative daily probability of timely detection over a 30-day scenario timeline for one MC&A activity performed once a day with a BHEP of 0.98, or an initial P_D of 0.02, for five different levels of dependence.

The example analyses summarized above demonstrate the extended path analysis for one daily MC&A event and a single theft timeline that could be incorporated in a single PPS layer. Along with these analyses, others 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 PPS layers, with both uniform and variable theft timeline distributions, including a geometric distribution that was evaluated using Latin Hypercube Sampling. The calculation of timely detection becomes more complex as additional PPS layers and 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 PPS layer. Details are provided in Durán [1] and Durán et al. [5].

EXTENDED PATH ANALYSIS – COMBINED MC&A DETECTION

Actual facility-level MC&A operations are much more complex and involve many MC&A activities that are performed at various intervals to provided combined MC&A detection. To demonstrate the extended path analysis methodology for scenarios that are more representative of the complexity of actual facility MC&A

operations, additional analyses were done for a 5-day/30-day scenario timeline for PPS layers 1 and 2, respectively, for a set of MC&A activities that occur at different intervals.

Table 3 presents 25 days of a detection opportunity timeline for a notional set of four MC&A activities at a facility. Each of the four activities occurs at a different interval and has been assigned a BHEP as determined in Table 1. Also, each activity has been assigned a given level of dependence, and the day-to-day calculations of the BHEP reflect this dependence relationship. For example, Activity 3 occurs every three days and has a high level of dependence between each performance of this activity. Activity 2 occurs every 14 days and has a moderate level of dependence between each performance of this activity. In this example, Activities 1 and 4 are performed once a day by the same person, so these activities are assigned a high level of dependence for the performance of each of these activities.

The daily P_D can be determined by combining the BHEPs as non-detection probabilities and taking the complement:

$$P_{Dayn} = 1 - \prod_{m=1}^{M} BHEP_m \tag{3}$$

For example, on Day 3, the set of MC&A activities includes Activities 1, 3 and 4, and the daily P_D, $P_{MC\&A,3}$, is calculated as:

$$\begin{aligned} P_{MC\&A,n} &= 1 - \prod_{m=1}^{M} BHEP_m \\ P_{MC\&A,3} &= 1 - \left[(BHEP_1)(BHEP_3)(BHEP_4) \right] \\ P_{MC\&A,3} &= 1 - \left[(0.944)(0.050)(0.972) \right] \\ P_{MC\&A,3} &= 1 - \left[0.046 \right] \\ P_{MC\&A,3} &= 0.954 \end{aligned} \tag{4}$$

The probability of MC&A detection on Day 3 is higher than that for the previous two days because additional MC&A activities have occurred on this day to contribute to a higher level of detection for the set of MC&A activities. The MC&A detection timeline for the scenario is determined from the daily probabilities of MC&A detection and is illustrated in Figure 4. Over the 25-day timeline, the daily probability of MC&A detection increases as additional activities occur to contribute to detection, or decreases as the dependence relationships reduce detection between observations. The underlying effect of the dependency relationships is also evident in Figure 4.

The detection timeline for the set of MC&A activities was evaluated against an adversary timeline in which MC&A detection in the PPS layer 1 represented as a 5-day uniform distribution and MC&A in PPS layer 2 was represented as a 30-day uniform distribution. For the 5-day timeline, the daily values of MC&A detection for the first five days (Table 3) are used in the convolution calculation. For this case, timely MC&A detection for Event 2 in the ESD is calculated to be 0.98. For the composite timelines, the daily values of MC&A detection for the 35-day composite timeline are used in the convolution calculation, and timely MC&A detection for Event 4 in the ESD is calculated to be 0.938. The sequence probabilities for the Material Recovered and Alert end states are 0.750 and 0.249, respectively. Thus, the set of MC&A activities result in a level of MC&A detection similar to that for a single MC&A activity with a high initial P_D, even though some of the MC&A activities in the set have high and moderate levels of dependence between observations and across activities.

This analysis demonstrates the applicability of the extended path analysis methods for more realistic facility conditions. The daily P_D in Figure 4 provides insights for evaluating the protection level provided by MC&A activities over time and identifying gaps in that protection level. For example, daily P_D from days 15 through 25 indicate that additional protection is needed and action should be taken to reduce dependency in the

Table 3: Detection timeline for a notional set of four MC&A activities

Day (n)	MC&A ACTIVITIES									
	Activity 1		Activity 2		Activity 3		Activity 4		Combined BHEP	$P_{D,MC\&A}$
	Interval	BHEP	Interval	BHEP	Interval	BHEP	Interval	BHEP		
	once a day	0.10	every 14 days	0.05	every 3 days	0.05	once a day	0.10		
1	0.100						0.550		0.055	0.945
2	0.775						0.888		0.688	0.312
3	0.944				0.050		0.972		0.046	0.954
4	0.986						0.993		0.979	0.021
5	0.996						0.998		0.995	0.005
6	0.999				0.525		1.000		0.524	0.476
7	1.000						1.000		0.999	3E-04
8	1.000						1.000		0.999	1E-04
9	1.000				0.763		1.000		0.762	0.238
10	1.000						1.000		1.000	0.000
11	1.000						1.000		1.000	0.000
12	1.000				0.881		1.000		0.881	0.119
13	1.000						1.000		1.000	0.000
14	1.000		0.050				1.000		0.050	0.950
15	1.000				0.941		1.000		0.940	0.060
16	1.000						1.000		1.000	0.000
17	1.000						1.000		1.000	0.000
18	1.000				0.970		1.000		0.970	0.030
19	1.000						1.000		1.000	0.000
20	1.000						1.000		1.000	0.000
21	1.000				0.985		1.000		0.985	0.015
22	1.000						1.000		1.000	0.000
23	1.000						1.000		1.000	0.000
24	1.000				0.993		1.000		0.993	0.007
25	1.000						1.000		1.000	0.000

performance of MC&A activities, or to add other activities that would increase the protection level during that time period. The importance of MC&A activities is also evident – while a single MC&A activity has the potential to contribute significantly to cumulative detection, a set of activities has the potential to maintain cumulative detection over time.

Mitigating Potential Malicious Insider Activity

One purpose for analyzing a PPS is to identify vulnerabilities or gain insights on the possible impacts of additional protection elements. Another application of HRA methods for characterizing MC&A activities was an exercise to demonstrate how these methods might be used to explore strategies for mitigating malicious insider activity. This analysis used a 5-day/5-day scenario timeline for PPS layers 1 and 2, respectively, with uniform distributions for the theft timelines and the detection timeline developed for a set of MC&A activities. This scenario timeline has a two-day to ten-day possible duration and 25 possible composite timelines. Three cases for the MC&A detection timeline were addressed: one for the baseline set of combined MC&A activities described in Table 3; a second assuming a malicious insider performs activities 1 and 4, which have a high level of dependence; and a third assuming the dependency relationship is removed for activity 4. The baseline case assumes that the insider has access to the material, but is not in a position of performing MC&A tasks.

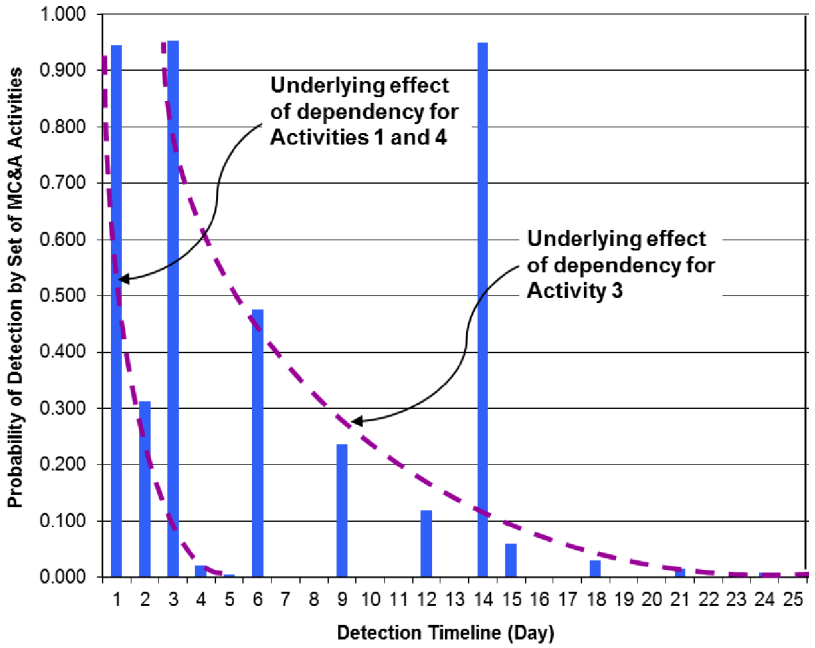

Figure 4: Daily P_D over a 25-day period for a set of MC&A activities

For the first ten-day composite timeline, the detection timeline used the daily MC&A detection probabilities for the first ten days from the baseline set of combined MC&A activities (Table 3). In this baseline set of activities, it was assumed that activities 1 and 4 are performed by the same person on a daily basis, and therefore they are assigned a high level of dependence between recurrences of these activities. The next variation for this timeline assumes that the person who performs activities 1 and 4 is a malicious insider who is seeking to steal material. Consequently, the BHEP for these activities is set to 1 and the P_D is 0 because the thief is concealing the activities by misstating the results of the MC&A tasks. In the third variation, the facility does not know about any malicious insider activity, but an operational change is made to remove the dependency relationship among these activities – instead of one person performing both activities, two people perform these activities. The person who performs activity 1 is still assumed to be the malicious insider, and activity 4 is assumed to have the high level of dependence, the same as for the baseline set of activities because a single person (but not the malicious insider) always performs these tasks.

Tables 4 and 5 provide the detection timelines for the variations with the malicious insider and the insider mitigation, respectively. Figure 5 is a plot of these detection timelines. The original BHEPs for activities 1 and 4 provided in Table 3 for the set of MC&A activities no longer apply. For the case of the malicious insider, these values in Table 4 are set to 1.0, as the insider who performs both these activities is trying to conceal malicious activity. The P_D for these individual activities is zero. Because activities 1 and 4 are the only ones performed on days 1 and 2, the daily probability of MC&A detection is also zero. Over the ten-day timeline for this case MC&A detection occurs only on days 3, 6 and 9 when an activity other than 1 or 4 is performed. Activity 3 is performed on these days and is defined to have a high level of dependence for its performance. For the case with malicious insider mitigation for activity 4, the daily BHEP values reflect the removal of the dependency between activity 1 and activity 4, but there is still a high level of dependence for the performance of activity 4 because the same person (although not a malicious insider) always performs this task. The operational change to remove the dependence between activities 1 and 4 to mitigate possible malicious insider actions results in additional daily MC&A detection that is at least as high as or higher than the baseline case.

Table 4: Detection timeline for set of combined MC&A activities with a malicious insider performing activities 1 and 4

Day (n)	MC&A ACTIVITIES									
	Activity 1[1]		Activity 2		Activity 3		Activity 4		Combined BHEP	$P_{D,MC\&A}$
	Interval	BHEP	Interval	BHEP	Interval	BHEP	Interval	BHEP		
	once per day	~~0.10~~	once every 14 days	0.05	once every 3 days	0.05	once per day	~~0.10~~		
1	1.000						1.000		1.000	0.000
2	1.000						1.000		1.000	0.000
3	1.000				0.050		1.000		0.050	0.950
4	1.000						1.000		1.000	0.000
5	1.000						1.000		1.000	0.000
6	1.000				0.525		1.000		0.525	0.475
7	1.000						1.000		1.000	0.000
8	1.000						1.000		1.000	0.000
9	1.000				0.763		1.000		0.763	0.237
10	1.000						1.000		1.000	0.000

[1] The original BHEPs for activities 1 and 4 provided in Table 13 no longer apply. For the case of the malicious insider, these values are set to 1.0, as the insider who performs both these activities is trying to conceal malicious activity.

Table 5: Detection timeline for set of combined MC&A activities with a malicious insider performing activity 1 and mitigation of a malicious insider performing activity 4

Day (n)	MC&A Activities									
	Activity 1[1]		Activity 2		Activity 3		Activity 4[2]		Combined BHEP	$P_{D,MC\&A}$
	Interval	BHEP	Interval	BHEP	Interval	BHEP	Interval	BHEP		
	once per day	0.10	once every 14 days	0.05	once every 3 days	0.05	once per day	0.10		
1	1.000						0.100		0.100	0.900
2	1.000						0.550		0.550	0.450
3	1.000				0.050		0.775		0.039	0.961
4	1.000						0.888		0.888	0.112
5	1.000						0.944		0.944	0.056
6	1.000				0.525		0.972		0.510	0.490
7	1.000						0.986		0.986	0.014
8	1.000						0.993		0.993	0.007
9	1.000				0.763		0.996		0.760	0.240
10	1.000						0.998		0.998	0.002

[1] The original BHEPs for activity 1 provided in Table 3 no longer apply. For this case of the malicious insider, these values are set to 1.0 for activity 1, as the insider is trying to conceal malicious activity.

[2] For the case with malicious insider mitigation for activity 4, the daily BHEP values reflect the removal of the dependency between activities 1 and 4, but still a high level of dependency between the performance of this activity (always by the same person, but not the a malicious insider).

Table 6 provides the values for timely MC&A detection in the MAA and PA and the end state summaries for each of the three cases. These results show that the case for malicious insider mitigation allows overall detection to recover up to the baseline case. These analyses demonstrate the application of the extended path analysis methodology to evaluate the effectiveness of a set of MC&A activities, to identify possible vulnerabilities and to provide insights for operational strategies to address possible malicious insider activity.

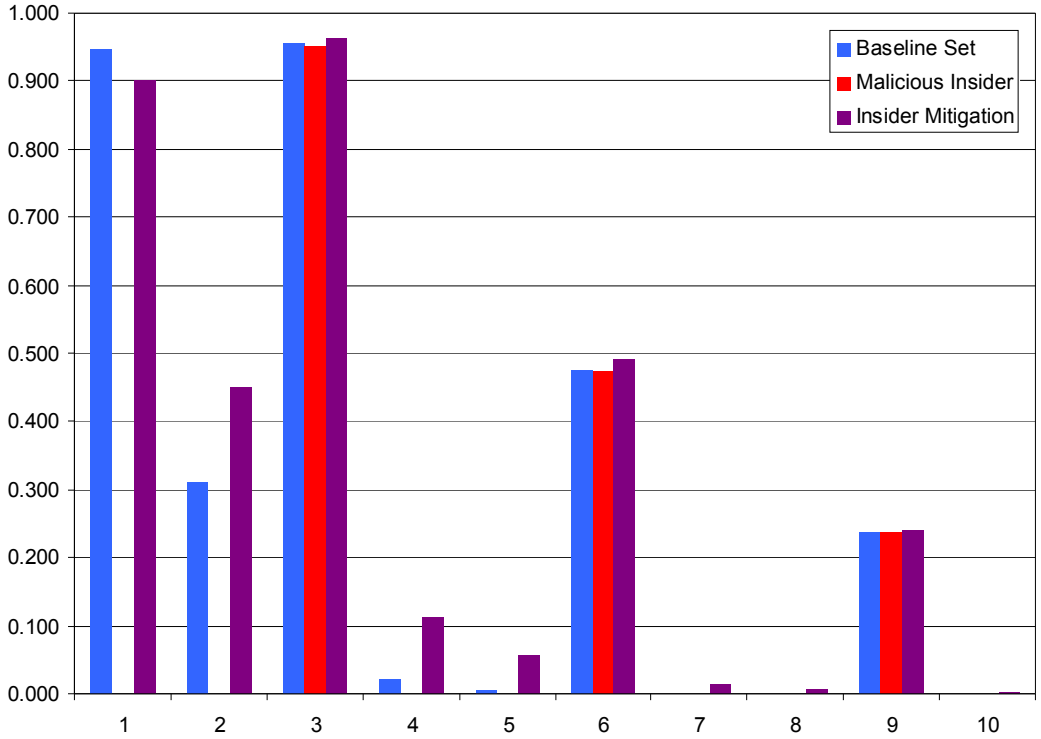

Figure 5: Detection timelines for baseline set of MC&A activities, malicious insider, and insider mitigation.

Summary of Methods for Combined MC&A Detection and Multiple PPS layers

The analyses presented in this paper further demonstrate the use of the extended path analysis to model insider theft and integrated PPS and MC&A protection elements and to quantify the effectiveness of these protection elements against an insider threat. The methods provide tools to evaluate the protection level MC&A activities provide over time, identify gaps, and model potential insider activity. The results provide insights on how MC&A activities can be implemented in facility operations to provide a desired level of protection over time.

CONCLUSION

This work has provided additional analyses to demonstrate the extended path analysis methodology for combining MC&A protections with traditional sensor data in a calculation for timely MC&A detection. This paper presented analyses for a set of MC&A activities through multiple PPS layers that more realistically reflect facility MC&A operations. The analyses demonstrate how operational strategies might be considered for evaluating a set of MC&A protections and for mitigating the insider threat. The approaches used to characterize and evaluate MC&A activities highlight their importance as protection elements for insider theft. Overall, 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. One can increase the detection probability for each MC&A observation by proper selection of MC&A activities. One can also increase the effectiveness of subsequent observations by reducing the dependence between observations through the use of HRA and human factor techniques. Finally, one can take steps to lengthen the adversary's timeline by reducing the frequency of potentially vulnerable states in order to provide more opportunities for MC&A detection. 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 path analysis 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.

Table 6: Timely MC&A detection in PPS Layer 1 (Event 2) and PPS Layer 2 (Event 4) and end state summary for baseline set of MC&A activities, malicious insider activity and insider mitigation

5-day/5-day timeline scenario with uniform theft distributions	Timely MC&A Detection		End State Summary	
	Layer 1 Event 2	Layer 2 Event 4	End State	Probability
MC&A detection timeline for baseline set of activities and dependency relationships	0.980	0.507	Material Recovered	0.746
			Alert	0.245
			Material Recovered + Alert	0.991
			Material Lost	0.009
MC&A detection timeline assuming malicious insider for daily activities 1 and 4 with high dependence relationship	0.570	0.641	Material Recovered	0.583
			Alert	0.272
			Material Recovered + Alert	0.855
			Material Lost	0.145
MC&A detection timelines assuming insider mitigation for activity 4	0.968	0.699	Material Recovered	0.743
			Alert	0.248
			Material Recovered + Alert	0.991
			Material Lost	0.009

ACKNOWLEDGEMENTS

This work was funded in part by the Doctoral Studies Program at Sandia National Laboratories. 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, 2010, *Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials*, Ph.D. Dissertation, The University of Texas at Austin, Austin TX.
2. P.G. Dawson and P.Hester, 2006, "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.
3. F.A. Durán & G.D. Wyss, 2010, "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, PSAM10, June 7-11, Seattle WA.
4. F.A. Durán & G.D. Wyss, 2010, "Human Reliability-Based MC&A Models for Detecting Insider Theft," in *Proceedings of the 51st Annual Meeting of the Institute of Nuclear Materials Management*, Institute of Nuclear Materials Management, Deerfield IL.
5. F.A. Durán, G.D. Wyss, & B.B. Cipiti, 2011, "Extended Probabilistic Path Analysis to Evaluate Performance of Protection Systems Against Insider Theft," in *Proceedings of the 52nd Annual Meeting of the Institute of Nuclear Materials Management*, Institute of Nuclear Materials Management, Deerfield IL.
6. A.D. Swain III & H.E. Guttmann, 1983, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants," SAND80-0200, Sandia National Laboratories, Albuquerque NM.