SAND2012-4140C

Integrated Safeguards and Security for Reprocessing Plant Monitoring*

Rebecca M. Ward
Sandia National Laboratories, University of Texas at Austin

Felicia A. Durán and Benjamin B. Cipiti
Sandia National Laboratories

ABSTRACT

Nuclear fuel reprocessing plants contain a wealth of plant monitoring data including material measurements, process monitoring, administrative procedures, and physical protection elements. Future facilities are moving in the direction of highly-integrated plant monitoring systems that make efficient use of the plant data to improve monitoring and reduce costs. The Separations and Safeguards Performance Model (SSPM) is an analysis tool that is used for modeling advanced monitoring systems and to determine system response under diversion scenarios. The utility of integrating process monitoring and material measurement data has been previously demonstrated with the SSPM. This work extends previous efforts by integrating the facility's physical protection system (PPS) and administrative procedures into the current model. The PPS at the hypothetical facility is modeled using the Adversary Time-Line Analysis System (ATLAS) software to determine detection probability and delay times for material loss pathways. The adversary is assumed to be a non-violent insider. A human reliability-based insider theft methodology is used to generate time-dependent detection probabilities for a sample administrative procedure. Alarms from an administrative procedure, as well as process monitoring or material balance alarms, place the facility in a state of alert, which increases detection probability for many elements in the physical protection system. The goal of this integration is to show that material balance and administrative procedure data can improve the performance of the PPS and thus the timeliness of detection. Model results support this goal, indicating that system integration has the potential to decrease detection time for both abrupt and protracted diversion.

INTRODUCTION

Reprocessing plants are difficult to safeguard because of the continuous, bulk flow nature of the material and because of the difficulties associated with obtaining good spent fuel measurements. Current plants rely on technology with low measurement error to detect small system perturbations and use routine flush-outs for complete material accountancy. These methods are costly and disruptive to plant operations and cannot ensure timely detection of material theft. In an effort to address these shortcomings, reprocessing plant safeguarding systems are moving towards near real-time accountancy (NRTA), which provides much better continuity of knowledge with regards to material accountancy.

---

* Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2012-XXXXC, approved for unclassified/unlimited release.

In order to investigate potential improvements to reprocessing plant safeguarding systems, the Separations and Safeguards Performance Model (SSPM) was developed by Sandia National Laboratories [1]. The SSPM is a simulation model of a UREX+ reprocessing plant that serves as a platform for testing future monitoring systems and observing system response to different diversion scenarios. The user inputs scenario definition information, and the model simulates and tracks material flow through the facility. Process monitoring and plutonium accountancy alarms are built into the model and are triggered according to a Page's test alarm algorithm [2]. In this work, the SSPM was used to examine the integration of data from various plant systems—process monitoring, plutonium accountancy, physical protection, and administrative procedures—to determine whether such integration can improve the timeliness of detecting material theft.

In particular, this work explores whether such systems integration will improve detection timeliness against an insider adversary. Insiders represent a special class of adversary with authority and access at the facility, which allow them to exploit security system vulnerabilities and choose ideal times for theft based on knowledge of plant operations. As such, traditional means for preventing and detecting material theft, like a facility's physical protection system (PPS), are largely ineffective against an insider. This paper demonstrates that for both a protracted or abrupt diversion by an insider adversary, the integration of the material accountancy, administrative procedures and the PPS system can improve the timeliness of detecting a theft.

METHODS

The following section describes the setup for the PPS and administrative procedures. It also outlines the integration of these systems into the SSPM.

Physical Protection System

The PPS modeling focused on theft or diversion of material by an insider adversary during normal facility operations. The insider adversary has access to and knowledge of the plant's operations and is assumed to be a passive, non-violent insider who will undertake diversion activities without the use of any tools. ATLAS [3] (Adversary Time-Line Analysis System) was used to design a hypothetical PPS for two material balance areas (MBAs) in the hypothetical reprocessing facility. Performance data from these ATLAS models were then used to populate the PPS subsystem in the SSPM, which is described in greater detail below. The performance data in the model, namely delay times and detection probabilities, were tailored specifically for the insider, and are based on two key assumptions: (1) the delay times are analogous to adversary task times for an insider; and (2) traditional detection methods would not be effective against a knowledgeable insider, so detection is based primarily on observations of unauthorized activities and attempts at unauthorized access.

The two MBAs that were modeled for the reprocessing plant include the front end, where spent fuel is received, chopped, dissolved and then measured in an accountability tank, and the back end, where the chemical separations occur. Front end activities occur in the fuel building, while back end activities occur in the extraction building.

Figure 1 is the adversary sequence diagram (ASD) for the front end of the hypothetical facility. An ASD is a two-dimensional graphical representation of all PPS layers and protection elements defined for a facility, as well as all possible adversary paths through the facility. The target material is chopped, used fuel pieces containing uranium and plutonium oxide, which is indicated at the bottom of the ASD. The ASD shows four layers of protection onsite: the limited area, the protected area, the fuel building and the target area. Within each layer are physical protection elements, and each element contains safeguards to delay or detect an adversary. A key for the protection elements is shown in the upper right-hand corner of the ASD.

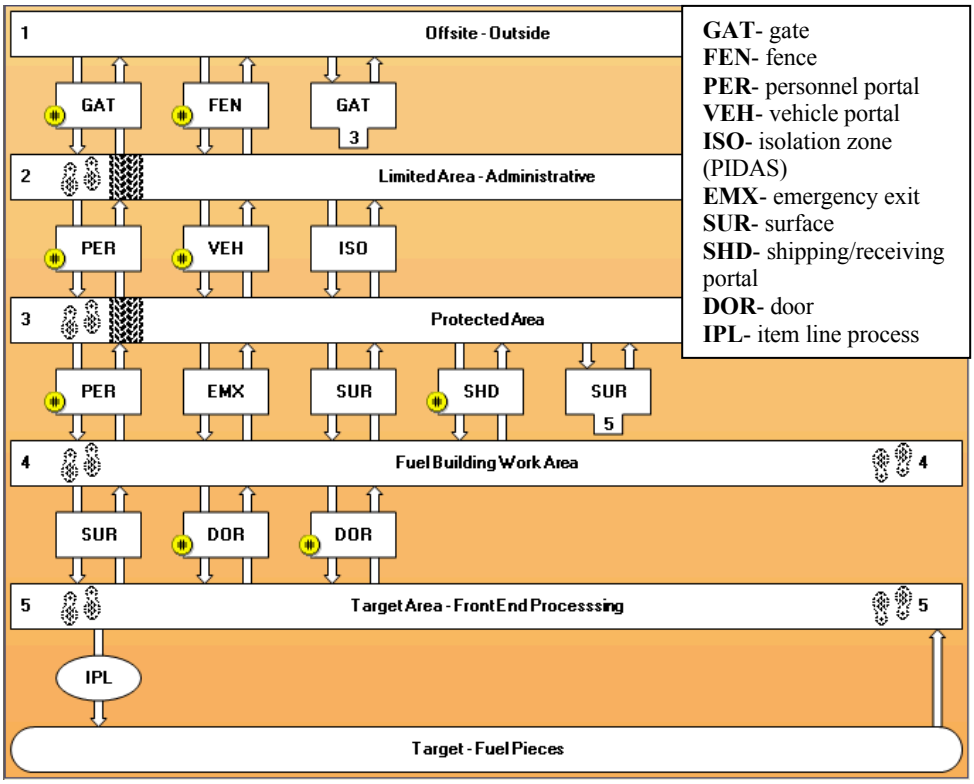

Figure 1: Adversary sequence diagram for the front end

Figure 2 shows the ASD for MBA2. Here the target material for theft is transuranic (TRU) solution contained in a product tank. Diversion analyses were carried out in ATLAS for both MBAs, and the resulting detection probabilities and delay times were incorporated into the SSPM PPS subsystem model.

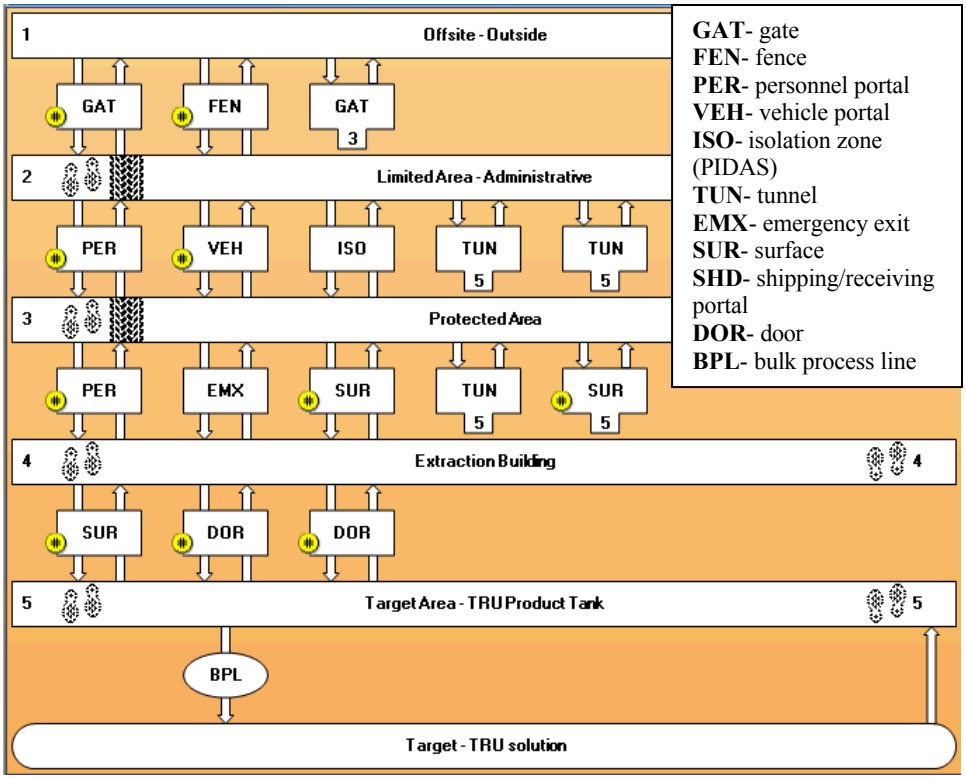

Figure 14: Adversary sequence diagram for separations

MC&A Administrative Procedures

In addition to modeling the PPS at a hypothetical reprocessing facility, a material accounting and control (MC&A) administrative procedure was also modeled, as MC&A procedures can serve as a type of sensor to bolster both delay and detection against the insider threat. The MC&A procedure was modeled using a human reliability-based insider theft methodology that was developed previously at Sandia [4]. The procedure was assumed to be a daily administrative check (DAC) with a baseline detection probability of 0.90.

Because the insider theft methodology is based on human reliability analysis (HRA), it prescribes a positive dependence relationship between checking activities, meaning the success of one activity depends on the success of the activity immediately preceding it. In the context of a DAC, the failure to detect an anomaly one day increases the probability that the anomaly will not be detected the next day. The mathematical relationship between successive checking activities is given in Equation 1 below. It describes the probability that an anomaly will not be detected on day *n*, given that the anomaly was not detected the previous day.

$$P(ND_n|ND_{n-1}) = \frac{1 + aP_{ND_{n-1}}}{a + 1} \quad \text{(Eq. 1)}$$

Here *a* is the dependency factor, with values of 19, 6, and 1, corresponding to low, moderate and high dependency, respectively. This equation was used to calculate daily probabilities of MC&A detection for the over the course of the simulation in the SSPM.

The complication is that the calculation for HRA cannot be applied until there is enough data present to detect the anomaly. In the case of a protracted diversion, many inventory balances may be required until there is enough confidence that the diversion should be detected. In order to model this, an additional factor must be used that represents the detection probability as a function of time, based on the diversion fraction. This correction factor was applied to the detection probability calculation.

Integration in the SSPM

The primary goal of the integration is to determine how additional plant data can improve the overall plant monitoring system. This was accomplished by integrating both the PPS and administrative procedure subsystems into the SSPM. The integration was undertaken such that the state of the PPS subsystem could be influenced by alarms triggered in other systems, including the administrative procedures, plutonium balance or process monitoring data.

The PPS subsystem was populated with the detection probabilities and delay times output by the ATLAS model, although in this work notional values are used to represent the performance data. As part of the scenario definition preceding a run, the user defines the physical path the material will take out of the facility, and the material is routed through the proper PPS elements accordingly. The user can also specify whether the material is held up in any one barrier to find a more optimal time to divert. Each pathway has a detection probability associated with it, and a random number generator is used to determine whether an alarm is triggered. An alarm is indicated with a message popup window that gives the PPS element location and the alarm time. Figure 3 is a screenshot of the user interface used to designate the diversion pathway.

As described above, the administrative procedure modeled is a daily administrative check that occurs every 24 hours with an initial detection probability of 0.90. The check was implemented in the SSPM with a DAC subsystem which calculates the detection probability every 24 hours, assuming a constant dependency (which is set by the user). If an alarm is triggered in the DAC subsystem, a signal is sent to the PPS subsystem, and the system is put in a heightened state of alert. A dialogue box also appears notifying the user of the alarm and the time at which it occurred. In the heightened state of alert, the detection probability for individual PPS elements increases. This feedback mechanism is intended to simulate behavior at a facility after an anomaly is detected and increased security measures are implemented. For example, increased security patrols may be dispatched and exit searches may be performed. In addition to the DAC subsystem, the plutonium accountancy and process monitoring systems can place the PPS subsystem in a heightened state of alert. All three of these systems can be seen as inputs to the PPS subsystem alarm boxes on the left-hand side of Figure 3.

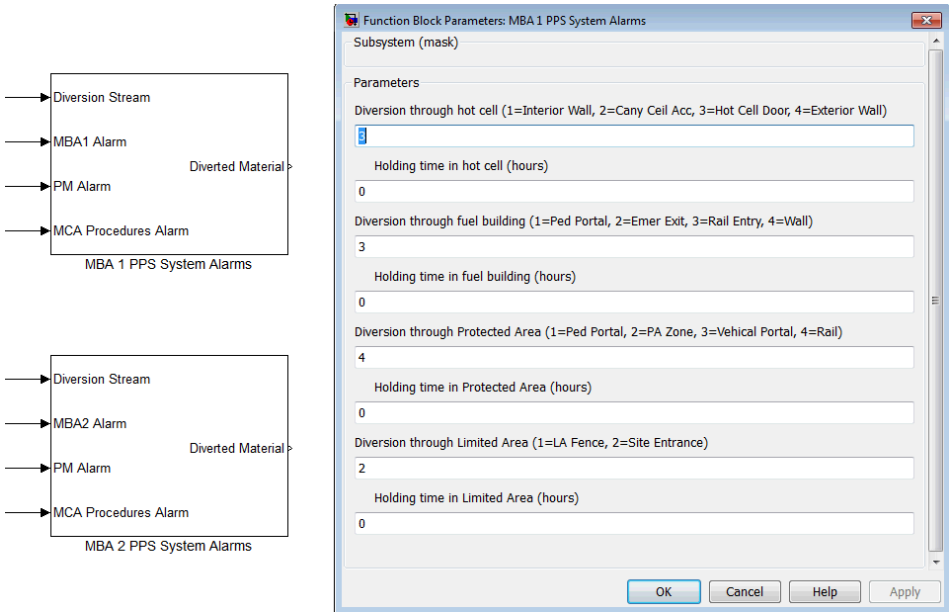

Figure 3. PPS subsystem inputs

RESULTS

Six runs were performed to test the effectiveness of integrating all plant systems. The two scenarios were an abrupt diversion, in which 8 kg of plutonium was stolen over 24 hours, and a protracted diversion, in which 0.1% of the flow was diverted over 1600 hours. For both diversion scenarios, three types of runs were performed: 1) the base scenario, where no system integration was present, 2) the PPS system was integrated with only the process monitoring (PM) and plutonium balance systems, and 3) the PPS system was integrated with the PM, plutonium balance and MC&A administrative procedure subsystems. Results for all six scenarios are presented below.

Abrupt Diversion

The diversion starts at hour 300 in simulation time in MBA1 and occurs over a 24-hour period. A total of 8 kg of plutonium is stolen. The material is assumed to be removed through the hot cell door, then smuggled out on a rail car through shipping/receiving, and then out the rail gate. The detection probabilities are arbitrarily set at 25% for the hot cell door, 10% at shipping/receiving, and 10% at the rail gate. Also it is assumed that two trips are required to get all the material out, so the probabilities are calculated every 10 hours.

The scenario is first run with no system integration. In this base case, the PPS system is not alarmed. The comparatively low detection probabilities coupled with only two detection opportunities limit the PPS system response.

The same diversion scenario was then run with the integration of the PM, plutonium balance and PPS systems. An alarm in either the PM or plutonium balance system would increase the detection probability for all PPS elements to 50%. The results from this run are shown in Figure 4. It is apparent that in this trial, the PM alarm is triggered four hours after the diversion begins, and the plutonium balance alarm sounds after 24 hours. These alarms put the PPS

system in an alert state, which leads to two PPS alarms, as opposed to the zero alarms seen in the base case. Shipping and receiving detects the material diversion after 30 hours, and the site rail gate detects the material transfer after 50 hours. Note that a lag time is programmed into the model to simulate a delay time before a rail car would leave the facility.

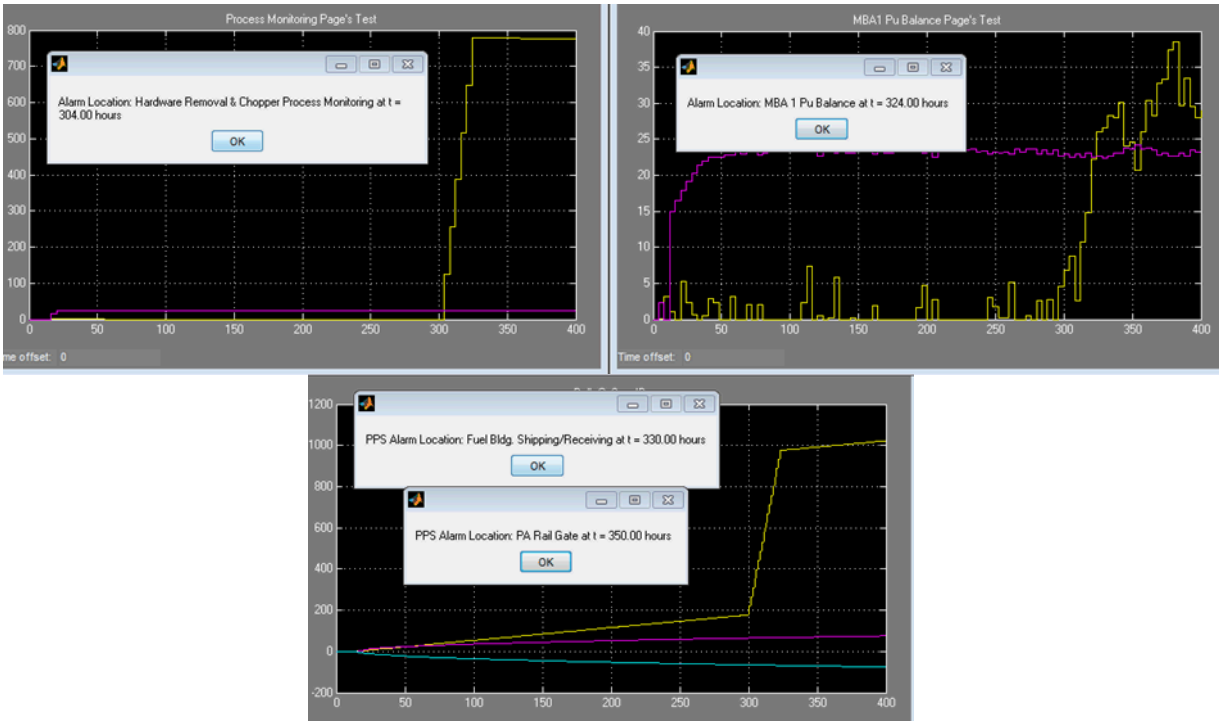

Figure 4. Abrupt diversion in MBA1 with partially integrated systems

The abrupt diversion scenario was run a third time with full system integration, including integration of the MC&A administrative procedure, the daily administrative check. Results for this run are shown in Figure 5. In this case the DAC triggered an alarm 12 hours after the diversion begins, which leads to two PPS alarms. A 24 hour delay time was again built into this run, which is why the PPS system elements alarmed after the material was initially diverted.

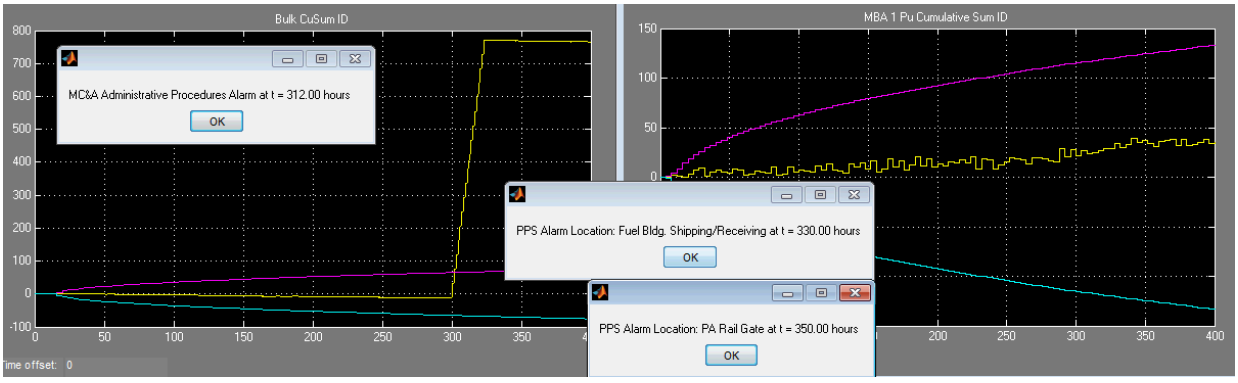

Figure 5. Abrupt diversion from MBA1 with fully integrated systems

The summary of all results is shown in Table 1. Note that because a random number generator is used the results vary from run to run. The results displayed are meant to be representative of model output for a given diversion scenario.

Protracted Diversion

A protracted diversion scenario in MBA2 was examined to look at response times when material is removed little by little over long periods of time. In this diversion scenario, 0.1% of the flow into the stripper tank was diverted over 1600 hours (starting at hour 300). The material was assumed to be removed from the process cell by the canyon ceiling access, then through the emergency exit, and then smuggled onto a rail car to leave the facility. The detection probabilities were arbitrarily assumed to be 5% for the ceiling access, 10% for the emergency exit, and 5% for the rail car exit. As with the abrupt diversion scenario, the alert state was designed to increase these probabilities to 50% for all three elements. It was assumed that there would only be one chance per day to remove material in this manner, so the detection probabilities were only calculated once every 24 hours.

The protracted diversion scenario was first run with no system integration. The detection probabilities for an insider are low, but there are a large number of detection opportunities, which in this case leads to three PPS alarms (recall that the PPS is not in an alert state). The ceiling access alarm was seen 180 hours after the start of the diversion, followed by the rail gate alarm after 276 hours, and lastly the building emergency exit after 324 hours. The PPS system was able to respond to this material diversion before half of a significant quantity was removed.

The scenario was run again for the case of limited system integration, where the PM and plutonium balance systems are integrated with the PPS system. In this run the process monitoring alarm was triggered after 108 hours and the plutonium balance after 124 hours, putting the PPS system into a state of alert. This led to three PPS alarms. One alarm occurred 108 hours after the start of the diversion, and the other two occurred 132 hours after the start. Note that the diversion started at hour 300, but the PPS elements did not alarm until the alert state was achieved.

The protracted scenario for full systems integration differed slightly, with 8 kg of plutonium being diverted over 1900 hours, starting at hour 400. In this case the DAC detects an anomaly after 128 hours, placing the PPS system in an alert state and leading to two PPS alarms. Interesting, one PPS alarm was triggered before the DAC alarm was triggered. Results from this run are shown in Figure 6.

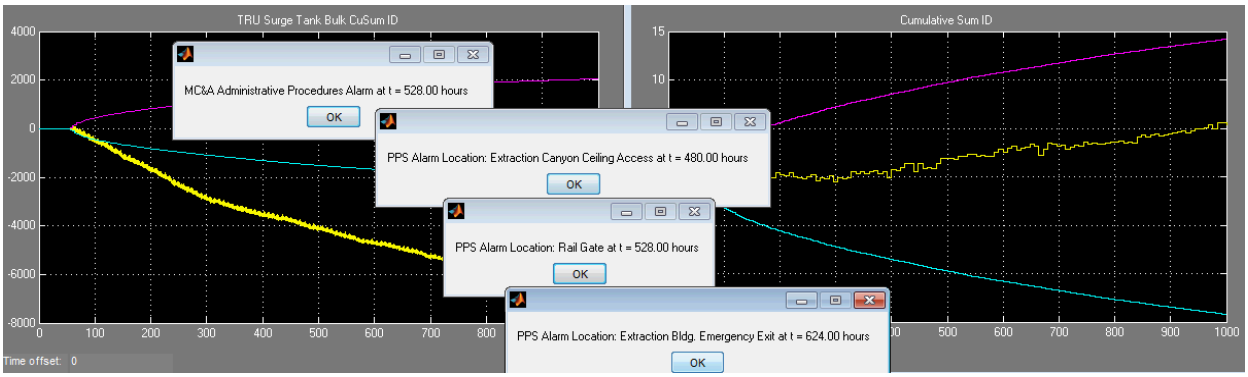

Figure 6. Protracted diversion from MBA2 with fully integrated systems

Table 1. Time of PPS alarms for each run. Note that alarms are random and runs cannot be compared directly, but results are meant to be representative for the given scenario

	Abrupt Diversion	Protracted Diversion
Base Case	No PPS alarms	PPS alarms: hour 180, 276, 324
Partial Integration	PPS alarms: hour 30, 50*	PPS alarms: hour 108, 132, 132
Full Integration	PPS alarms: hour 30, 50*	PPS alarms: hour 80, 128, 224**

* 24 hour delay built in

** Slightly different scenario; see text for details

DISCUSSION

The results above indicate that the integration of systems at a reprocessing plant increase the probability and/or timeliness of detecting a material theft by an insider. In the case of the abrupt diversion, PPS alarms were seen only when the plant systems were integrated, and not in the base case. This result suggests that the use of plant monitoring systems to place the PPS in an alert state could increase the probability of detecting material as its being smuggled out of the building. In the case of the protracted theft, it is less obvious that the alert state contributes to the detection of the theft, as three PPS alarms are triggered in all three scenarios, including the base case with no system integration. The results do suggest, however, that the integration of plant systems can increase the timeliness of detection, as the PPS alarms trigger earlier in the diversion when the plant systems are integrated. This earlier detection could provide valuable time to lock down a facility and recover missing material.

CONCLUSIONS

The SSPM was modified to model PPS and administrative procedures that are used to protect reprocessing plants from material loss. A PPS system was included to model pathways through which material can exit the MBAs. An example administrative procedure was modeled to demonstrate the effectiveness of such procedures in countering the insider threat. The material balances from the process monitoring system and plutonium accountability system were used with the administrative procedures to trigger an alert state in the PPS, which increases the probability of detecting material loss through the various PPS elements.

Diversion scenario testing showed that without the integration of the material balance and administrative procedures, the PPS elements were much less likely to alarm. Abrupt diversions in particular could occur without detection, but protracted diversions were usually detected due

to multiple detection opportunities. With integrated systems, the PPS elements in all scenarios alarmed earlier. It should be noted that the process monitoring system generated the earliest alarms, but this type of monitoring is unable to detect substitution diversions. Thus, in the case of a substitution diversion, the plutonium balance or administrative procedures would be required to trigger an alert state. The early detection advantage afforded by integrated detection systemps is critical because every additional hour makes it more likely that a response force can respond to a situation before a significant quantity of material is removed. The integration of near real time bulk and plutonium balance at low uncertainty and administrative procedures with the facility's PPS provides a clear advantage as compared to existing plants that do not have such timely data.

REFERENCES

1. 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.
2. B.B. Cipiti, F.A. Durán, B. Middleton and R. Ward, October 2011, "Fully Integrated Safeguards and Security for Reprocessing Plant Monitoring," SAND2011-7292, Sandia National Laboratories, Albuquerque, NM.
3. ATLAS (Adversary Time-Line Analysis System) software, Version 4.4, Sandia National Laboratories, Copyright 2003-2009.
4. F.A. Durán, "Probabalistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Materials," PhD Dissertation, The University of Texas at Austin (2010).