SANDIA REPORT
SAND2009-6781
Unlimited Release
Printed October 2009

Integrated Safeguards & Security for Material Protection, Accounting, and Control

Benjamin B. Cipiti and Felicia A. Durán

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2009-6781
Unlimited Release
Printed October 2009

Integrated Safeguards & Security for Material Protection, Accounting, and Control

Benjamin B. Cipiti, Advanced Nuclear Fuel Cycle Technology
Felicia A. Durán, Security Systems Analysis
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0747

Abstract

Traditional safeguards and security design for fuel cycle facilities is done separately and after the facility design is near completion. This can result in higher costs due to retrofits and redundant use of data. Future facilities will incorporate safeguards and security early in the design process and integrate the systems to make better use of plant data and strengthen both systems. The purpose of this project was to evaluate the integration of materials control and accounting (MC&A) measurements with physical security design for a nuclear reprocessing plant. Locations throughout the plant where data overlap occurs or where MC&A data could be a benefit were identified. This mapping is presented along with the methodology for including the additional data in existing probabilistic assessments to evaluate safeguards and security systems designs.

Contents

Figures

Tables

Acronyms

AFCI	Advanced Fuel Cycle Initiative
AMUSE	Argonne Model for Universal Solvent Extraction
ASSESS	Analytic System and Software for Evaluation of Safeguards and Security
ATLAS	Advanced Time-Line Analysis System
CAS	Central Alarm Station
DEPO	Design Evaluation Process Outline
ECF	Entry Control Facilities
IAEA	International Atomic Energy Agency
ID	Inventory Difference
JCATS	Joint Conflict and Tactical Simulation
LISSAT	Livermore Safeguards Systems Analysis Tool
MBA	Material Balance Area
MC&A	Material Control and Accounting
MPAC	Material Protection, Accounting, and Control
MPACT	Material Protection, Accounting, and Control for Transmutation
NRC	Nuclear Regulatory Commission
PA	Protected Area
PIDAS	Perimeter Intrusion Detection Alarm System
PPA	Property Protection Area
PPS	Physical Protection System
SAS	Secondary Alarm System
SMES	Safeguards Measurement Evaluation System
SNM	Special Nuclear Material
SSPM	Separations & Safeguards Performance Model
UREX	Uranium Extraction
VA	Vulnerability Assessment
VPSIM	Variance Propagation by Simulation

1.0 Introduction

As world conditions change and the number of threats increases, the protection costs for nuclear fuel cycle facilities will also increase. The traditional approach of designing safeguards and security systems separately and after facility design is near completion lead to non-optimal systems and can increase costs if design changes are required. The integration of safeguards and security early in the design process will be required to keep costs manageable and improve the effectiveness of the overall system. This concept is also referred to as Safeguards by Design [1].

For commercial U.S. nuclear fuel cycle facilities and transportation of special nuclear material (SNM), domestic safeguards include physical protection (also called physical security) and material control and accounting (MC&A). This project examines the integration of MC&A systems with the physical protection system (PPS) to achieve overall Material Protection, Accounting, and Control (MPAC). Throughout this document, this may also be referred to as safeguards and security.

This need for integration is also driven in part by the continued development of new technology. New MC&A techniques and measurement technologies may make it possible to drastically improve the timeliness of detection of material loss or diversion. Quicker detection times make it more important to have an integrated safeguards and security system that can respond effectively to such events.

This work is part of the Material Protection, Accounting and Control for Transmutation (MPACT) Campaign of the Advance Fuel Cycle Initiative (AFCI) research and development program. The scope of this work is focused on nuclear fuel reprocessing plants and examines domestic safeguards and security. Previous work [2] discussed the critical aspects of the integration of domestic safeguards, international safeguards, and security, but the international safeguards aspects were not included in this study. Future work will need to also examine this integration in more detail.

2.0 Background

U.S. Nuclear Regulatory Commission (NRC) regulations for physical security and MC&A focus on protection against sabotage and theft or diversion of nuclear material by an insider and/or outside adversary. The specific requirements are provided in 10 CFR 73, "Physical Protection of Plants and Materials," and 10 CFR 74, "Material Control and Accountability of Special Nuclear Material." International safeguards requirements, although outside the scope of this work, are provided in 10 CFR 75, "Safeguards on Nuclear Material – Implementation of US/IAEA (International Atomic Energy Agency) Agreement." Physical protection and MC&A include performance-based requirements, as well as other very specific protection measures that must be implemented by licensees. The threats from, vulnerabilities to, and consequences of adversarial acts upon a nuclear facility must be determined and evaluated, and mitigating measures must be applied to establish appropriate levels of protection. For example, the NRC has updated its methods for design certification or combined license applicants to perform a security assessment for new commercial power plants [3, 4].

2.1 Safeguards Overview

For nuclear facilities, material control means the use of control and monitoring measures to prevent or detect loss when it occurs or soon afterward, and material accounting is defined as the use of statistical and accounting measures to maintain knowledge of the quantities of SNM present in each area of a facility. It includes the use of physical inventories and material balances to verify the presence of material or to detect the loss of material after it occurs, in particular, through theft by one or more insiders. Traditional MC&A for reprocessing is centered on the goal of measuring and accounting for all fissionable material in the plant. Uranium and plutonium measurements on the inputs and outputs of mass balance areas (MBA) are used to calculate inventory differences. These inventory differences can detect abrupt and protracted diversion of material.

In traditional reprocessing plants, the MC&A system is distinguished from the PPS. A loss of material would ultimately be reported with a subsequent response by the PPS, but the systems are not well integrated. Part of the difficulty is that traditional MC&A systems may have a significant delay time in detecting a diversion of material. However, new techniques and new measurement technologies being developed in the AFCI program may significantly improve the timeliness of detection, which in turn may provide the PPS with additional opportunities to respond to threats in a timely manner.

The Separations & Safeguards Performance Model (SSPM) is a high-level materials tracking model of a UREX+ (Uranium Extraction) reprocessing plant developed at Sandia that was used for this work [5]. The SSPM is based in Simulink and tracks cold chemicals, bulk fluid flow, solids, and mass flow rates of elements 1-99 on the periodic table. Expected separation efficiencies are modeled to determine the quantity of nuclear material going into different streams. The main reason the model was created was to simulate materials accountancy and process monitoring measurements for safeguards design and evaluation, so it provides a framework for and general configuration of expected measurement technologies. This data is

used to simulate inventory difference calculations and examine the instrumentation response to diversion scenarios.

Reference 5 provides additional detail on the SSPM development that was funded separately from this work. For this project, the model was used to help identify the areas where MC&A measurements can provide value to the physical security system. The model was also used to create a demonstration in one location of the plant of the interaction of MC&A measurements and additional measures (such as surveillance). The front end of the reprocessing plant was set up for this demonstration.

2.2 Physical Security Overview

Physical protection (also called physical security) consists of a variety of measures for the protection of nuclear material or facilities against sabotage, theft, and diversion. NRC's approach to physical protection is graded based on the significance of the material or facilities being protected. NRC establishes the requirements and assesses compliance with the requirements; the licensees are responsible for providing the protection. References 6 and 7 provide a more detailed presentation on the design and evaluation of a PPS and vulnerability assessment—identifying security system weaknesses that could potentially be exploited by malevolent human threats. These identified weaknesses are potential areas for improvement.

The AFCI Engineering Alternatives Study [8] has evaluated the physical security requirements and strategies for a UREX+ reprocessing plant. This is the most recent security evaluation for a reprocessing plant, but the security requirements are based on Department of Energy (DOE) rather than NRC guidance. DOE requirements are slightly different, but for the level of this study, the physical security system from the Engineering Alternative Study is assumed to be adequate and well-representative. The following description is summarized from Reference 8.

The first level of security is a Property Protection Area (PPA) that encompasses the entire reprocessing plant site. All buildings that process Category II quantities of material are contained in a Protected Area (PA) within the PPA. The PA covers all of the front end, dissolution, extraction, and solidification/storage.

The PA includes a perimeter intrusion detection assessment system (PIDAS). It also must contain entry control facilities (ECF) and vehicle barriers for controlled access. A vault or vault-type room is required in the PA for storage of Category II quantities of materials when not in process. Access controls for entry/exit points include nuclear material, metals, and explosives detection. The two-person rule is established for all access to Category II material. The PA may also contain the central alarm station (CAS) and secondary alarm station (SAS) with backup power.

The basic concepts highlighted above were used in this study to identify areas within the PPS where overlap with MC&A data may occur. However, since integration will occur during the design phase, the design methodology for PPS and MC&A systems must be understood.

2.3 Design and Evaluation Process Outline

The Design and Evaluation Process Outline (DEPO) [4, 7, 9, 10] is a systems-based methodology that has been applied for over 25 years for the design and evaluation of physical protection systems. The foundation of the DEPO methodology is the design of an integrated system that performs the physical security system functions to detect, delay and respond to adversary attacks. Recent work has examined the use of a DEPO-type approach to the design of safeguards systems [11]. The following two sections describe the original DEPO methodology and the extension of DEPO for safeguards design.

2.3.1 Traditional DEPO for Physical Protection

The traditional DEPO process (see Figure 1) starts with a determination of the PPS objectives. This includes facility characterization, threat definition, and target identification within the facility. The second step is the actual design of the PPS and includes methods for detection of events, delay, and response. The final step is the analysis and evaluation of the system to determine gaps. Models, vulnerability assessments, and risk analyses may be used. Based on these results the system will be redesigned until the final design is deemed adequate.

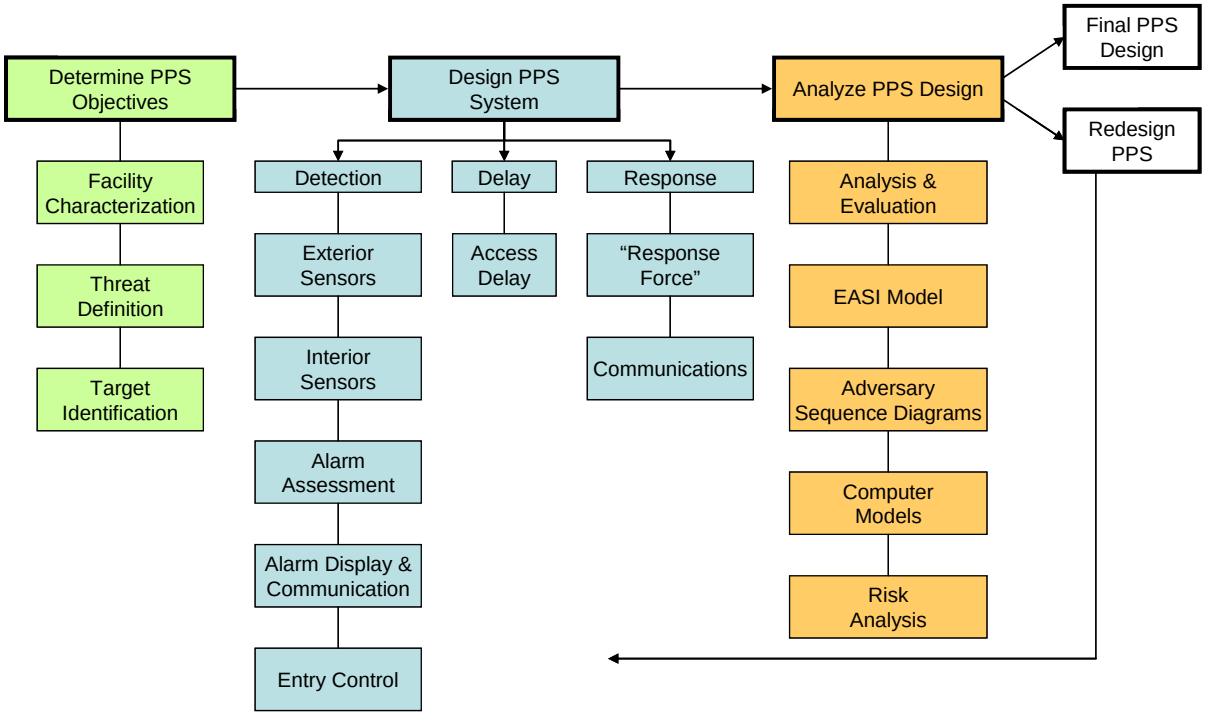

Figure 1: Traditional DEPO Process

2.3.2 Extending DEPO for Safeguards

Recent work has developed a DEPO-like systems engineering process for the design and evaluation of safeguards systems [11]. The initial version of the process uses the same system functions of detect, delay and respond. The implementation of these functions, however, is based on safeguards systems capabilities. For example, while detection for physical protection systems relies on sensors on fences and doors, detection for safeguards systems would rely on materials tracking and process monitoring measurements. The strategy of patterning the safeguards process after DEPO supports efforts to integrate safeguards and physical security.

The elements of the systems engineering process envisioned for safeguards design are shown in Figure 2. The first step in the design for a plant or facility is to determine the safeguards objectives—this includes characterizing the facility, defining the threats, and identifying the targets. The second step in the process is the actual design of the system and includes detection, delay, and response. The final step is to analyze and evaluate the design for various risks. Based on those results the system design will be modified until a final design is agreed upon.

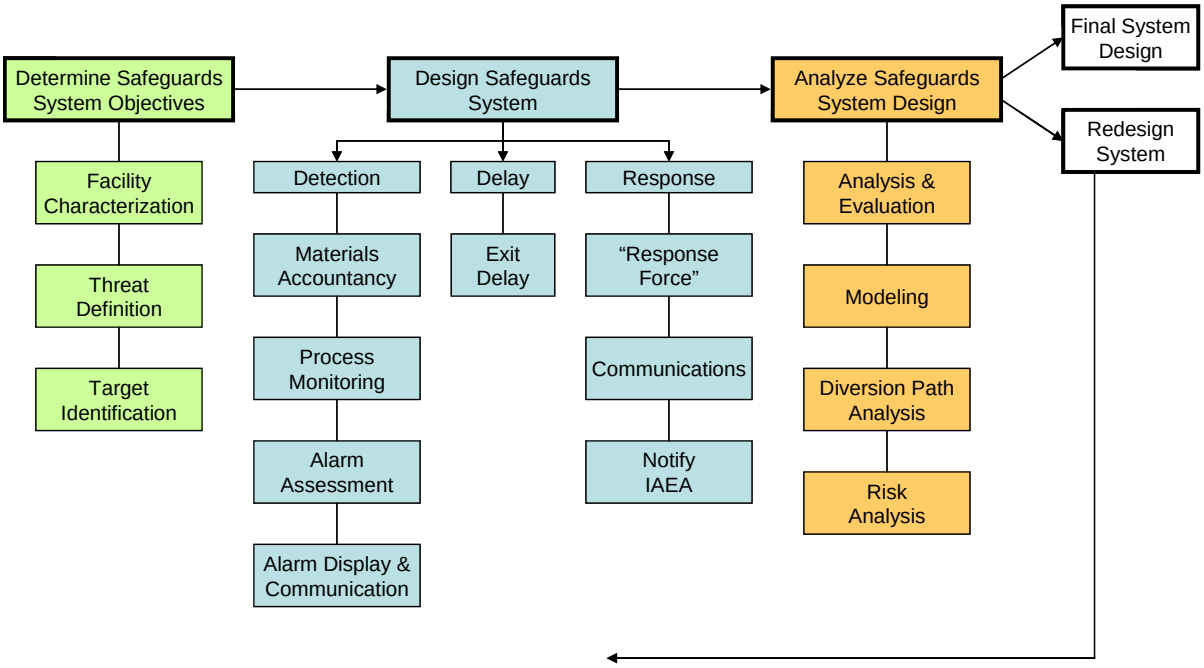

Figure 2: Systems Engineering Process for Safeguards

It is clear in comparing Figures 1 and 2 that many parallels can be drawn between the use of this process for designing security and safeguards systems. The effort in this current work is to provide an initial demonstration of integrating the DEPO processes for physical protection and safeguards systems to develop one overall MPAC system.

3.0 Integrating the DEPO Process

One of the first steps in this work was to identify the areas in the DEPO process where the MC&A and physical protection systems can benefit the most from integration. In this work, it is also recommended that the best practices for design and evaluation of a PPS identified in Reference 3 be extended for integrating MC&A and physical protection system design. The following paragraphs are excerpts of the general best practices as well as those for planning and design extended to address both MC&A and PPS design. Best practices for other specific elements of the DEPO process are also provided in Reference 3.

Where possible, it is always best to determine the MC&A and physical protection objectives and incorporate these objectives into the MC&A and physical protection system designs during the facility master design process. For an integrated design, it may be effective to consider the objectives for the overall MPAC system. This is the most cost-effective and efficient method of conducting risk assessments because it mitigates the need for costly redesign and facility upgrades necessary to protect against identified threats. It also provides an opportunity to engineer MPAC system designs against current and future postulated threats. In addition, it provides opportunities to reduce the cost of the MPAC system over the life of a facility by integrating overlapping support areas and reducing reliance on operational programs.

Effective MPAC system design begins with the planning process. While this is an obvious first step, it is critical to include all necessary stakeholders in the master planning process to achieve a design that meets the requirements of operations, safety, and security. This approach to master planning provides an integrated strategy for engineered design, construction, and maintenance of nuclear power plant facilities that in the long-term is cost-effective and more efficient and helps to re-duce short-term decision-making that tends to occur at the project level. Limiting or excluding safeguards and security representation during the design process will ultimately have a negative impact on system effectiveness and invite unnecessary future costs through retrofitting to mitigate an ever-changing threat spectrum. Addressing security concerns that are based on threat-specific assessments of nuclear power plants with engineered design solutions throughout the master planning and design process will ensure adequate and efficient protection of personnel, equipment, property, and infrastructure. Incorporating effective engineered design elements into the master plan requires subject matter experts representing the detection, delay, and response disciplines. It is also essential to include expert vulnerability analysts who are qualified to assess the identified threats against the identified targets, to assess the performance of an MPAC system design against the identified threats, and to determine MPAC system effectiveness and the associated overall risk.

Best Practices for Planning and Design:

- Establish a safeguards and security team to provide MC&A and physical protection system design requirements.
- Define safeguards and security team roles, responsibilities, and authority as it integrates with the facility design team.
- Determine the resources necessary to support safeguards and security design and analysis.

- Identify and document safeguards and security design requirements early in the facility design process.
- Safeguards and security design requirements should be based on a threat-specific assessment of reprocessing plants.
- Plan for an iterative process of design, analysis, and redesign and reanalysis.

3.1 Determine System Objectives

Both the MC&A and physical protection systems start with facility characterization and the design requirements based on regulations. The regulations have been discussed briefly in Section 2. The facility characterization starts with a preliminary design including process flow sheets and general building layout, but the process is iterative, so this step should occur early in the design process.

Both systems then have the same tasks of defining threats and identifying targets. The threats for a stand-alone MC&A system design are focused on theft or diversion of material, and since the focus of this work is domestic safeguards, the threats come from both outside and insider adversaries. The targets will include fissionable material and any other nuclear material in the plant that could have some value or be used for a weapon (including radiological dispersal devices).

The facility threats that the PPS focuses on include theft and sabotage. The threats for both systems overlap – thus, this is an important point for integration. Sabotage can include any number of threats to destroy or interrupt the operation of the facility and may include the same threat groups of outside and insider adversaries.

3.2 Design the System

The design and evaluation processes for both systems address system functions of detection, delay and response. The implementation of these functions, however, is based on different systems capabilities.

3.2.1 Detect

Both MC&A and physical protection systems design methodologies follow the same structure for detection of an event and alarm display and communication. The type of sensor or measurement varies. For MC&A the detection occurs with material measurements from material accountancy or process monitoring measurements. These include scales, flow rates, bulk volume, concentration measures, gamma detectors, neutrons detectors, etc. Software is used to calculate inventory differences (ID), and alarms can be triggered if the ID is above or below some threshold. Other operational activities may also provide detection opportunities. Alarm assessment includes examining if the alarm is due to measurement uncertainty or likely from a diversion or loss scenario.

For the PPS, detection occurs through the use of internal and external sensors. These may include the PIDAS, motion detectors, tamper indicators, surveillance cameras, etc. Alarms and

alarm assessment is used to determine if an unauthorized action has taken place. Exit or entry control is important to detect unauthorized tools and personnel entering an area and prevent material from leaving the area.

The idea proposed here is that these areas of the designs are combined into one MPAC system. Detection would include the full suite of measurements and plant sensors to coordinate and track information more efficiently. Alarms and alarm assessment would be completely integrated to coordinate effective and timely response. Entry control would include both unauthorized entry and unauthorized exit of equipment, material or personnel.

3.2.2 Delay

Delay means different things for MC&A and PPS. Delay for MC&A is mostly about exit delay since the threat is removal of material. Delay includes all the barriers or checks in place to increase the time required to remove material once diverted. For example, delay might include the amount of time it would take to cut through a fence. Delay can also be applied directly to the MC&A system in the length of time required to slowly divert material.

Delay for the PPS focuses on access delay and may include delay in getting into the facility or in accessing specific areas for threats associated with sabotage or theft. Threats associated with theft also need to be concerned with exit delay.

Again, this is an area where the PPS requirements encompass the MC&A requirements. The delay provided by or based on MC&A measurements should be incorporated into the delay provided by the PPS design. The challenge is in the characteristics of the timelines for each of the two systems – the PPS delay timelines are most often on the order of minutes, especially for attacks from outside adversaries. For theft or diversion of material, the integrated system will need to consider protracted and discontinuous timelines.

3.2.3 Response

Response is also slightly different for MC&A and PPS. In PPS design, the response force is part of the design. The response force must be able to deal with all identified threats in multiple locations. Communication is important in coordinating the response whether it involves protective force, facility lock-down, or a combination of both.

MC&A response should be devoted to communicating the alarms to the PPS so that they can determine the proper response. Clearly, an integrated MPAC system could stream-line this process so that the MC&A alarms are part of the response scenarios which the response force is designed to address.

3.3 Analyze the Design

Finally, the analysis step includes modeling of threat scenarios and risk analysis. In the safeguards world this is typically called diversion path analysis, while in the security world adversary sequence diagrams are examined.

This area has been identified to be a hole in the integration effort since current computer models are either focused on safeguards or security, not both. Several modeling and analysis tools are available to support the evaluation of a PPS. Path analysis is examined using Analytic System and Software for Evaluating Safeguards and Security (ASSESS) [12] and Advanced Time Line Analysis System (ATLAS) [13]. The response force is evaluated using Joint Conflict and Tactical Simulation (JCATS) [14], table top exercises, and field exercises (force-on-force exercises)). MC&A and diversion path analyses have been much more informal using a variety of codes [15] such as LISSAT, AMUSE, Safeguards Measurement Evaluation System (SMES), VPSim, and the SSPM.

It is possible to continue to use separate codes for MC&A and PPS analysis, but a unified model will help to make the analysis more efficient. Previous work has examined methods for integrating MC&A operational activities within the path analysis for a PPS [16].

4.0 Demonstration of Integration

This work examined only the front end of the reprocessing plant to develop a demonstration of the integration of safeguards and security. The front end includes spent fuel receipt/storage, hardware removal and fuel chopping, dissolution, hulls wash, clarification, and finally the accountability tank and associated surge tank. Future work will examine the rest of the plant.

Current measurement technology is not able to account for fissionable material in solid fuel assemblies with low uncertainty—the fuel must be dissolved before an accurate measurement can be taken. For this reason, inventory differences typically start at the accountability tank. The rest of the front end relies more heavily on item accounting and other security measures like surveillance to ensure that material is not diverted. Therefore, the front end already includes an integration of safeguards and security, and this project seeks to formalize and extend that relationship.

The Separations and Safeguards Performance Model (SSPM) was used to identify the measurements in the front end of the plant. However additional measurement points were added to the front end. The next several sections describe the MC&A measurements in the front end, the general security layout, key safeguards and security integration points, and a discussion of how the two systems can be integrated.

4.1 Front End MC&A

The front end of the SSPM was modified to include more measurements representing domestic safeguards, item accounting, and surveillance. Various techniques are used for item accounting including gross radiation measurements to detect the presence of spent fuel assemblies, video surveillance, and shipper-receiver information identifying each assembly.

The modeling of item accounting measures or procedures is not as straight-forward as material measurements. Whereas material measurements in the model are looking at specific quantities of actinides, item accounting measurement blocks in the model are designed to count assemblies that pass through an area.

Figure 3 shows the front end of the SSPM with all the instrumentation that would be used for accountability. The black boxes represent the actual processing vessels contained in the front end. The blue boxes represent MC&A measurements that would be used for domestic safeguards, and the green boxes represent measurements for international safeguards. Finally, the red block is a diversion block that can be used in the SSPM to determine instrumentation response to material loss.

The MC&A measurements may include stream monitoring, sampling from tanks, or surveillance. For example, the measurement labeled, “Acc MS” represents the plutonium concentration measurement from sampling the accountability tank. “Surv&Rad1” represents item accounting of spent fuel assemblies entering the plant. The functionality behind the blocks determines how the data is generated. The concentration measure is taken once every 8 hours and includes the

measurement uncertainties to generate a simulated measurement. The surveillance measurement is simply a running count of assemblies moving into the plant.

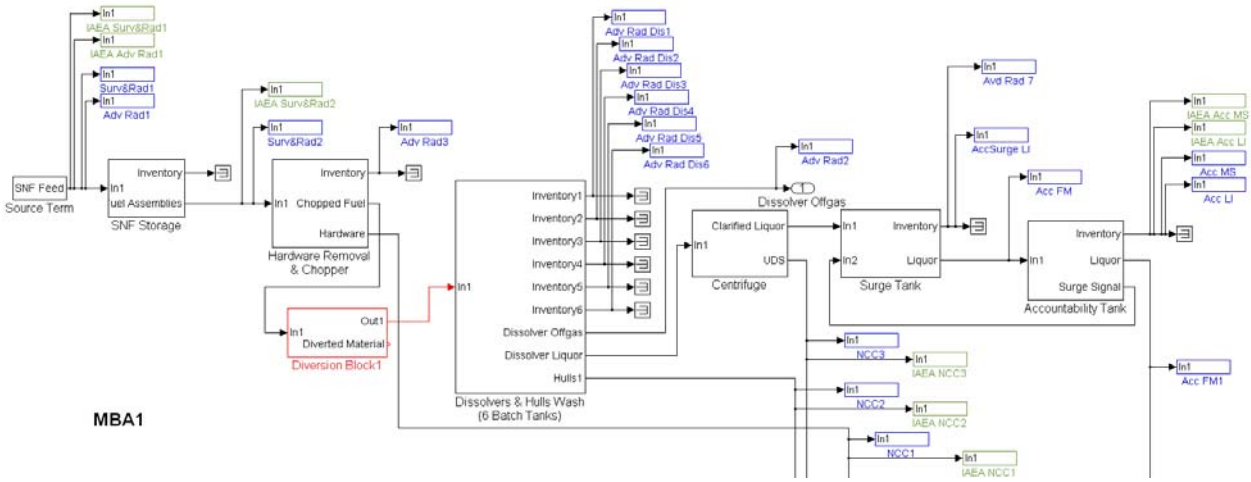

Figure 3: Reprocessing Front End

4.2 General Security Layout

The security layout includes the overall site, but only the front end building will be included. This general layout was extrapolated from Reference 8.

Spent nuclear fuel (SNF) will be delivered with NRC-licensed shipping casks (rail or truck). Fuel receipt and storage is not required within the PA, but the casks will be housed in shielded, reinforced concrete encasements. A berm surrounding the storage facility will provide a vehicle barrier. A dedicated transfer facility transports the casks across the PA boundary. The casks are sealed with tamper-indicating devices for inspection upon entering the PA.

The Fuel Building is located inside the PA and contains pool storage of fuel casks. Removal of the used fuel assemblies from the casks is performed in a shielded hot cell or canyon utilizing remote manipulators. The fuel assemblies are fed into the fuel chopper within the canyon. The rest of the processing steps from the front end all occur within the canyon as well. These vessels include the dissolvers and hulls wash tanks, centrifuge, surge tank, and accountability tank.

Figure 4 shows a general layout that may be used for physical security design, but only the building for the front end processes is shown. The entire site makes up the PPA and is surrounded by a fence. The PA is contained within a double fence and includes the PIDAS. The front end building is shown within the PA.

General physical protection elements can be considered for the PPS design. These include, for example, a variety of fence configurations, sensors, doors, gateways and building surfaces that may have different probability of detection and delay time characteristics. Different combinations of protection elements options provide different design options. The

characteristics of these protection elements should be considered in the master facility design process.

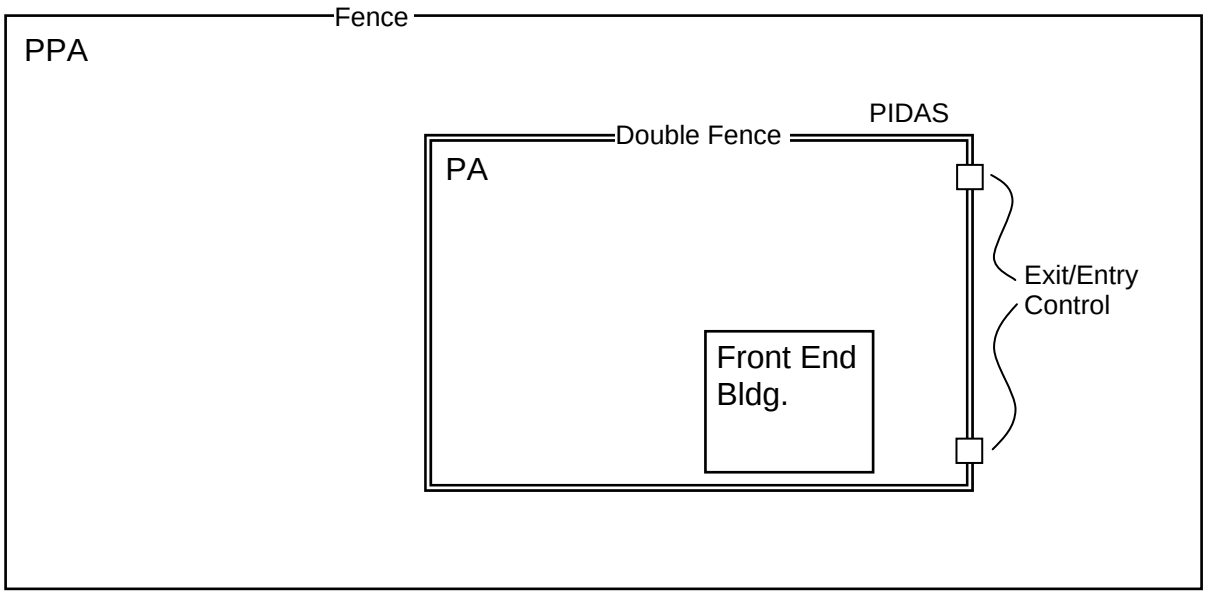

Figure 4: General PPS Layout

4.3 Key Integration Points

Traditional MC&A measurements tend to be "operational" whereas PPS measures tend to be "static." A tank level or concentration measure provides somewhat continuous data, but PPS systems tend to only alarm given a certain condition. One of the key threats to a reprocessing plant is an insider which is difficult to protect against since insiders have more knowledge of the facility and operations. Insiders can bypass alarms and sensors, but the continuous data from MC&A is more difficult to bypass. This provides one of the key reasons for integrating MC&A with security—it helps to develop an integrated strategy to protect against the insider threat.

Abnormal events or alarms in the MC&A system can be used to alter the state of the facility. For example, if a cumulative mass balance passes below some threshold, an alarm condition could trigger a heightened state of alert. Both MC&A and physical security personnel could be dispatched to reconcile the problem. This may involve a determination of whether a diversion occurred and if so, an attempt to locate the material and lock down the facility.

Figure 5 shows the front end plant processes with an overlay of key areas where better integration may help both systems. These integration points can be used to determine both how modifications in the plant design may help safeguards and security and how best to integrate the data.

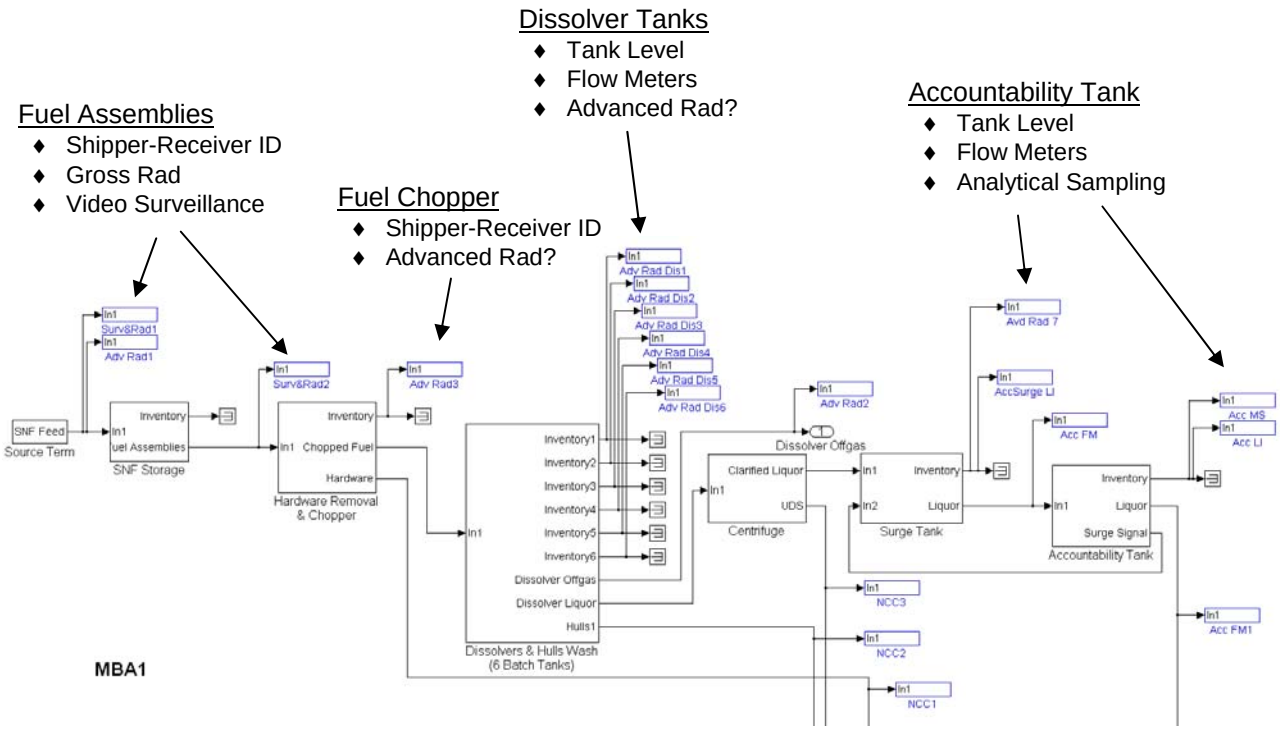

Figure 5: Integration Points on the Front End

Fuel Assemblies

The tracking of fuel assemblies in the front end is a current example of MC&A and PPS integration. Three different methods/technologies are used. Shipper/receiver data is essentially bookkeeping to keep track of specific fuel assemblies. This data contains rough estimates of the amount of nuclear material based on the initial fuel enrichment and burnup, and falls in the category of MC&A. Gross gamma measurements are also used to track when an assembly enters or leaves SNF storage. These detectors only detect that an assembly has passed by, but cannot distinguish between assemblies. Again, these are part of the MC&A system. Finally, video surveillance is used to monitor movement of assemblies, but this is part of the PPS as it is more typically used to assess alarms or other problems.

A single integrated system would better manage and correlate the data from these three measurement types. For example, shipper-receiver data would likely be entered into the system when fuel arrives and it could be linked to a bar code on the assemblies. Any transfer would require scanning of the bar code. Gross gamma measurements that detect a transfer would be correlated with the specific bar code. Video surveillance could even use image recognition technology to cross-reference with the transfers. If any one of the data sets does not correlate with the others, an alarm would be triggered to reach a heightened state of alert. Operations and security could then review video surveillance and track assemblies to determine if a problem or theft occurred. Using the same system, the shipper-receiver data provides rough accountability numbers for materials accountability through the plant, so the plant operator knows roughly how much fissionable material is at any one point in the front end.

Advanced technologies being investigated currently in the MPACT program may allow for fissionable material measurements of spent fuel assemblies with low uncertainty. A future plant should expect some type of advanced measurement that would also feed into the integrated system. Considering the reliability and human performance of the associated operational activities can provide additional measures to evaluate the performance of the system.

Fuel Chopper

The fuel chopper has traditionally not been an area for MC&A measurements. Since the chopper is contained within a hot cell or canyon, the facility provides material protection from theft. Bar code scanning may be used to verify when an assembly is chopped and fed into the dissolver tanks.

Advanced MC&A technologies in the future may also be used to provide inventory measurements in areas with difficult geometries like the chopper. An integrated MPAC system would cross-reference the shipper-receiver data with the measurement data from an advanced technology. Again, considering the reliability and human performance of the associated operational activities can provide additional measures to evaluate the performance of the system.

Dissolver Tanks

The dissolver tanks in existing plants do not contain measurements of fissionable material but do include process monitoring measurements like tank level and flow meters on cold chemicals. This is an area where process monitoring measurements can be integrated into the overall MPAC system to provide useful data for both safeguards and security. The process monitoring data provides a starting point for bulk tracking of processing fluids throughout the facility. Bulk fluid flows and liquid inventories can augment an MC&A system based on mass balances of fissionable material. Advanced MC&A technologies in the future may play a role here as well to provide fissionable material inventory measurements on each of the dissolver tanks.

Bulk material balances through the use of process monitoring data provides a line of defense against material theft or loss. If an alarm is signaled, the heightened state of alert will trigger both MC&A reconciliation and protective force investigation. Plant process data can be examined to determine if an off-normal process caused an upset. Surveillance can be used to determine if a leak in the processing vessel occurred. An integrated MPAC system will streamline the necessary response.

Accountability Tank

The accountability tank traditionally provides the first precise measurement of fissionable material going through the rest of the plant. It typically serves as an end to the front end mass balance area (MBA) and a beginning to the MBA for the separations portion of the plant. Process monitoring measurements such as level measurements and flow meters are used in conjunction with analytical samples to determine fissionable inventories per batch.

If advanced technologies provide incoming spent fuel measurements and inventory measurements of fissionable material in the front end, the accountability tank data serves to close out the front end mass balance. Any alarm condition in the mass balance could require a multitude of security responses to determine where the problem occurred or if it was just a false alarm.

4.4 Evaluating Integrated Safeguards and Security

In previous work, deterministic Material Assurance Indicators (MAIs) were developed to estimate a real-time effectiveness for protecting nuclear materials [17]. Many MC&A activities can be considered a type of sensor system with alarm and assessment capabilities that provide reoccurring opportunities for "detecting" the status of critical items. This characterization was a first step at an approach to incorporating MC&A activities as additional "sensors" in a site's protection system. MC&A activities were further characterized in Reference 16 as protection elements that are interwoven within each physical protection layer to provide additional detection and delay opportunities within the site's protection system. MC&A activities provide many, often reoccurring opportunities to determine the status of critical items (for example, *daily* administrative checks). To incorporate MC&A protection elements with PPS elements as sensors in a facility security system, a basis for defining detection probabilities for MC&A activities is required. Further characterization of MC&A activities as procedures that "check" the status of critical assets provides a basis for applying human reliability analysis models and methods [18] to determine probabilities of detection for MC&A protection elements.

Methods were developed in Reference 16 that include an object-based state machine paradigm 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. Probabilistic convolution is used to calculate an overall probability of detection for a set of MC&A activities that could be incorporated into the existing PPS path analysis methodology. Characterizing the MC&A protection elements in a facility in terms of an object-based state machine provides a framework for defining timing distributions for insider theft stages and facility alerts triggered by MC&A activities that can be convolved to determine the probability of theft or detection happening first. Event sequence diagrams (ESDs) describe insider paths of each theft scenario through the PPS and also incorporate MC&A activities as path elements.

Operational Performance

MC&A activities have many 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. As an example, checking the status of a valve in an NPP is similar to checking the status of a nuclear material target in a vault. The respective associated anomalous conditions are that a valve that should be closed 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 one person, in checking his or her own work or another person's work, discovers an anomalous condition.

Table 1 shows MC&A activities and similar characteristics of operator tasks identified in Reference 18 (Table 19-1), as well as associated baseline human error probabilities (BHEPs). These estimated BHEPs can be applied to MC&A protection elements by using the complement as a probability of detection for a given MC&A activity.

Table 1: Characterization of MC&A activities as different types of checking operations for HRA of an NPP and estimated probabilities (BHEPs) that a checker will fail to detect an error (columns 2 and 3 from Table 19-1 in Reference 18).

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

Reconciliation of Timelines

Reconciliation of timelines is also important in the integration of safeguards and security. Detection of material loss may take hours to months depending on whether material loss is abrupt, discontinuous, or protracted. Delay techniques through the plant (such as the time to get through multiple barriers) may take minutes to hours. Protective force operations may be

designed to respond to events on the order of minutes. As long as the threat can be stopped before it is complete, the system is successful.

An approach to integrating timelines for the MC&A system and PPS focusing on theft of material by a knowledgeable insider was developed in Reference 16. Within each layer of the PPS, a theft timeline and an MC&A detection timeline are defined. The theft timeline includes the time for the material to be removed from a PPS layer and the time for the material to be removed from the facility. The MC&A detection timeline considers the intervals for which MC&A activities, for example measurement points in the SSPM, occur and combines these into an overall daily MC&A probability of detection. This approach provides the flexibility to analyze timeline combinations for a variety of theft and diversion scenarios that would be developed as part of the design and evaluation process, as well as with SSPM simulations.

Timely detection by MC&A activities on a given day is the product of the probability that the facility detects material is missing on that day and the probability that material has not been removed from the facility before that day, which means, if detection occurs on that day, the detection will be timely.

Figure 6 provides an example of an Event Sequence Diagram that illustrates the possible theft and detection event sequences, and well as how detection by the PPS and MC&A system can be integrated. The yellow boxes are MC&A detection; if MC&A detection occurs, the facility goes into an alert state "Searching for Missing Item." The other events in the diagram represent detection opportunities in the PPS.

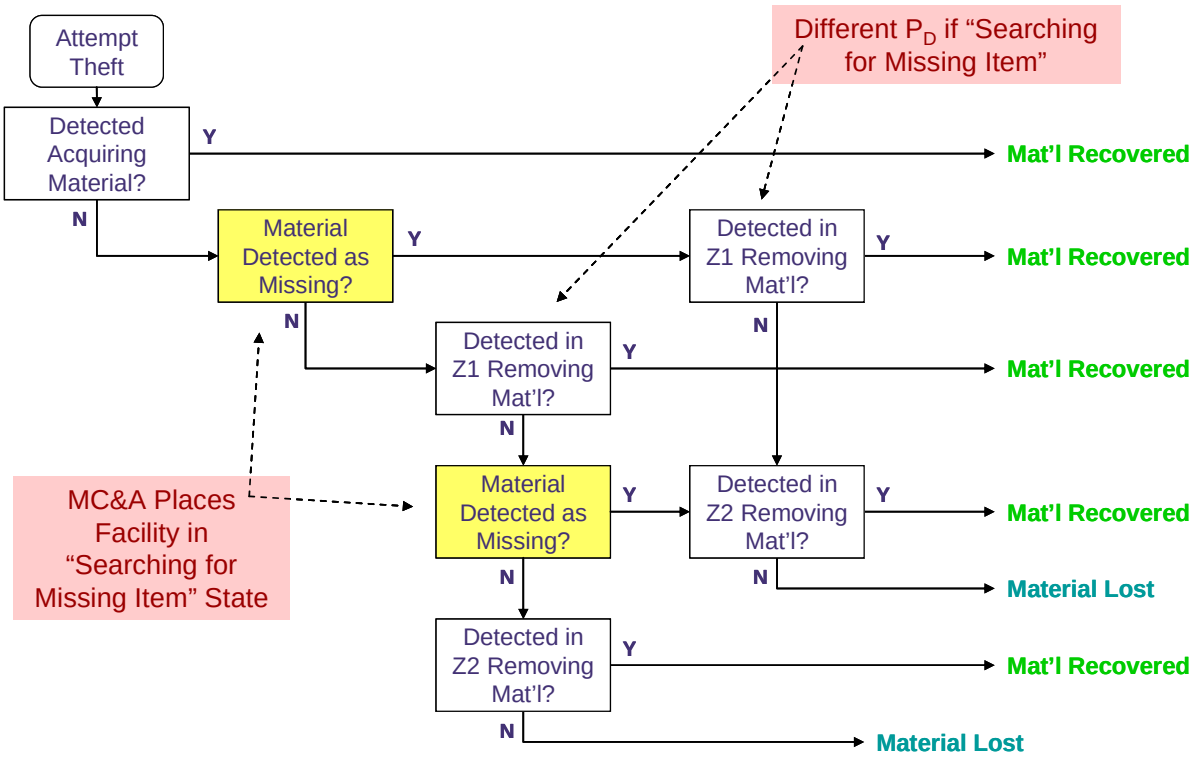

Figure 6: Event sequence diagram for material theft and detection.

4.5 Demonstration Summary

This demonstration of the integration of safeguards and security has brought together key elements need for such an activity. The front-end MC&A from the SSPM has provided the context for the operational function of the facility – a reprocessing plant has specific operations that must be performed within the facility. Within this operational framework, the structure and configuration of the facility design can be considered and key integration points identified. In this effort, the general PPS layout is provided as an example of facility configuration. Additionally, facility function and configuration are considered in using the SSPM to identify key integration points for MPAC system design. The operational context also provides the framework for the needed MC&A and physical protection system elements. The methods for evaluating the integrated system demonstrate how facility functions, operations and structures, MC&A and physical protection system elements, and operational performance might be brought together for a more complete evaluation of MPAC system performance.

5.0 Discussion

The work described here provides a framework for integration of safeguards and security, and this framework will be developed further in on-going work. It is difficult to provide specific details about the integration before a preliminary plant design is available. In many ways, the purpose of this report is to provide a framework that should be employed during the design stage of future fuel cycle facilities. An integrated MPAC system will most definitely need to be incorporated early in the design process.

The DEPO methodology provides a starting point for the integration of safeguards and security, but ultimately an MPAC system will need to include an integrated database developed around performance and operational data from both the (traditionally) MC&A and PPS measurements and sensors. This database and associated control structure will require a level of authentication and performance requirements beyond the scope of this work. The requirements, all associated inputs, and necessary outputs to design that control structure would be additional system design considerations incorporated in implementing the DEPO methodology.

The work has also pointed to the need to develop systems that are flexible for working with advanced technology and changing requirements. Advanced measurement or surveillance technologies should be easily incorporated into an MPAC system design. New technologies, however, will need to develop appropriate performance data that can be used for evaluating overall system performance.

The SSPM model is a useful tool for the materials accountancy and process monitoring data in a reprocessing plant, and it could be useful in the future for diversion path analysis coupled with the safeguards and security design codes. It is likely that the NRC will require diversion path analysis for the licensing of future reprocessing plants. A better understanding of how the SSPM and integrated analysis methods can be applied for diversion path analysis is required.

Work to incorporating MC&A into existing security evaluation methods will continue, but a more extensive effort will be required to make changes to the codes and achieve acceptance by the community that uses them. This has been identified as an existing need for system evaluation during the design phase.

Future efforts in this on-going work will continue to integrate MC&A elements into security evaluation methods. However, existing methods provide static evaluations of plant designs and cannot provide transient simulations of operations. The SSPM will be used to provide transient simulations and to develop the control architecture for combining the traditional physical protection measures and alarms with the material accountancy measures and inventory balances. This transient modeling ability will allow the various timelines to be integrated, and it can form the model for an integrated control system that would be used in a future plant in, for example, the central alarm station.

6.0 Conclusion

This work provides a framework and initial demonstration for the integration of safeguards and security into one MPAC system design. The DEPO methodology was used to identify areas of overlap between safeguards and security system designs. The significant amount of overlap shown here justifies the case for the integration of both systems.

For the front-end reprocessing operations considered in the effort, MC&A activities would typically be seen as occurring operationally within the flowsheet level, and PPS activities are typically seen as occurring operationally beyond the flow sheet level. There are in fact a number of key points for integration. This work identified four areas within the front end of the reprocessing plant and how data could be better integrated to support one uniform MPAC system.

The specific integration of MC&A activities into the existing methodology for evaluating physical protection systems was also examined. MC&A measurements can be interwoven into the overall protection system design to provide additional detection and delay opportunities. The reliability and performance of operational activities was discussed as a basis for additional measures to support the evaluation of integrated system performance. Since MC&A and PPS systems may have different timelines, a reconciliation of timelines is important to consider as well.

This effort brought together key elements to demonstrate how facility functions, operations and structures, MC&A and physical protection system elements, and operational performance might be brought together for a more complete evaluation of MPAC system performance

7.0 References

1. T. Bjornard et al. “Institutionalizing Safeguards-by-Design: High Level Framework,” Volume 1&2, Idaho National Laboratory, INL/EXT-14777 (not yet published).
2. B.B. Cipiti, F.A. Durán, K. Tolk, and P. Merkle. “Data Validation and Security for Reprocessing, SAND2008-6458, Sandia National Laboratories, Albuquerque, NM (2008).
3. D.W. Whitehead, C.S. Potter, III, and S.L. O’Connor. “Nuclear Power Plant Security Assessment Technical Manual,” SAND2007-5591, Sandia National Laboratories, Albuquerque, NM (2007).
4. ISL, “Nuclear Power Plant Security Assessment Format and Content Guide,” Part 1 of 3, Information Systems Laboratories, Rockville, MD (2007).
5. B.B. Cipiti. “Separations and Safeguards Performance Model,” SAND2009-4896, Sandia National Laboratories, Albuquerque, NM (2009).
6. M.L. Garcia. *The Design and Evaluation of Physical Protection Systems*, Second Edition, Boston: Butterworth-Heinemann (2008).
7. M.L. Garcia. *Vulnerability Assessment of Physical Protection Systems*, Boston: Elsevier Butterworth-Heinemann (2005).
8. “Engineering Alternative Studies for Separations Preliminary Physical Security Strategy for a Spent Fuel Separations Facility,” PS-G-ESR-G-00012, Engineering Alternatives Study, (2007).
9. IAEA. “The Physical Protection of Nuclear Materials and Nuclear Facilities,” IAEA-INFCIRC/225/Rev. 4 (Corrected), International Atomic Energy Agency (IAEA), Vienna (1999).
10. U.S. Army. *Physical Security*, Report FM 3-19.30, U.S. Department of the Army (2001).
11. F.A. Durán and B.B. Cipiti, “Systems Engineering Process for Safeguards Design,” in *Proceedings of the Institute for Nuclear Materials Management 50th Annual Meeting*, Institute of Nuclear Materials Management (2009).
12. ASSESS (Analytic System and Software for Evaluating Safeguards and Security), Version 2.56, Lawrence Livermore National Laboratory, Copyright 1989-2003.
13. ATLAS (Adversary Time-Line Analysis System) software, Version 4.2, Sandia National Laboratories, Copyright 2003-2006.
14. W.D. Henry, B. A. Brady, V. Koonce, C.D. Velasquez, and L.J. Myers, “Sandia JCATS Operator Manual,” SAND2004-3463P, Sandia National Laboratories, Albuquerque, NM (July 2004).
15. R. Parker, “Inventory of Safeguards Software,” LA-UR-07-6881, Los Alamos National Laboratory (2007).
16. F.A. Durán and G.D. Wyss. “Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Material,” in *Proceedings of Institute for Nuclear Materials Management 49th Annual Meeting*, Institute of Nuclear Materials Management (2008).
17. P.G. Dawson and P. Hester. “Real-Time Effectiveness Approach to Protecting Nuclear Materials,” in *Proceedings of the Institute for Nuclear Materials Management 47th Annual Meeting*, Institute of Nuclear Materials Management (2006).
18. A.D. Swain III and H. E. Guttmann, “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants,” SAND80-0200, Sandia National Laboratories (1983).

Distribution

1 Mike Miller (Los Alamos National Laboratory)
1 Brad Williams (Department of Energy)
1 Trond Bjornard (Idaho National Laboratory)

1 0736 John Kelly, 6770
1 0747 Ken Sorenson, 6774
1 0747 Ben Cipiti, 6774
1 0757 John L. Darby, 6414
1 0757 Felicia A. Durán, 6414
1 0757 John Russell, 6414
1 0757 Consuelo Silva, 6414
1 0757 Carla Ulibarrí, 6414
1 0757 Gregory Wyss, 6414
1 0759 Betty Biringer, 6411
1 1202 Rebecca Horton, 5640
1 0899 Technical Library, 9536 (1 electronic copy)


Sandia National Laboratories