SANDIA REPORT
SAND2008-6458
Unlimited Release
Printed October 2008

Data Validation and Security for Reprocessing

Benjamin B. Cipiti, Felicia A. Durán, Peter B. Merkle and Keith M. Tolk

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

SAND2008-6458
Unlimited Release
Printed October 2008

Data Validation and Security for Reprocessing

Benjamin B. Cipiti, Advanced Nuclear Fuel Cycle Technology
Felicia A. Durán, Security Systems Analysis
Peter B. Merkle, Nuclear Material Monitoring & Advanced Technology
Keith M. Tolk, Nuclear Material Monitoring & Advanced Technology
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0748

Abstract

Next generation nuclear fuel cycle facilities will face strict requirements on security and safeguards of nuclear material. These requirements can result in expensive facilities. The purpose of this project was to investigate how to incorporate safeguards and security into one plant monitoring system early in the design process to take better advantage of all plant process data, to improve confidence in the operation of the plant, and to optimize costs. An existing reprocessing plant materials accountancy model was examined for use in evaluating integration of safeguards (both domestic and international) and security. International safeguards require independent, secure, and authenticated measurements for materials accountability—it may be best to design stand-alone systems in addition to domestic safeguards instrumentation to minimize impact on operations. In some cases, joint-use equipment may be appropriate. Existing domestic materials accountancy instrumentation can be used in conjunction with other monitoring equipment for plant security as well as through the use of material assurance indicators, a new metric for material control that is under development. Future efforts will take the results of this work to demonstrate integration on the reprocessing plant model.

Contents

Figures

Acronyms

AFCF	Advanced Fuel Cycle Facility
AFCI	Advanced Fuel Cycle Initiative
ASSESS	Analytic System and Software for Evaluation of Safeguards and Security
ATLAS	Advanced Time-Line Analysis System
AVERT	Automated Vulnerability Evaluation for Risks of Terrorism
CCD-PEG	Cesium/Strontium Extraction
CUSUM	Cumulative Sum
DBT	Design Basis Threat
DEPO	Design Evaluation Process Outline
DOE	Department of Energy
EWMA	Exponentially Weighted Moving Average
GNEP	Global Nuclear Energy Partnership
IAEA	International Atomic Energy Agency
ID	Inventory Difference
JCATS	Joint Conflict and Tactical Simulation
JUA	Joint Use Agreement
JUE	Joint Use Equipment
MBA	Material Balance Area
MC&A	Material Control and Accountability
MTIHM	Metric Tons of Initial Heavy Metal
NRC	Nuclear Regulatory Commission
NRTA	Near Real-Time Accountability
PDCF	Pit Disposition and Conversion Facility
PPS	Physical Protection System
S&S	Safeguards and Security
SEID	Standard Error of the Inventory Difference
SNF	Spent Nuclear Fuel
SRS	Savannah River Site
TALSPEAK	Rare Earth Fission Product Extraction
TIE	Tamper Indicating Enclosure
TRU	Transuranic Isotopes (Np, Pu, Am, Cm)
TRUEX	Transuranic Actinide Extraction
UDS	Undissolved Solids
UREX	Uranium Extraction
VA	Vulnerability Assessment
VR	Vulnerability Review

1.0 Introduction

Current nuclear fuel reprocessing plants throughout the world have separate systems for managing materials accountability, international safeguards, and plant security. Reprocessing plants are faced with the difficult challenge of accounting for and protecting nuclear material, and the requirements will probably only become more stringent with time. One integrated plant monitoring system may not only be much more efficient, but may also improve the ability to safeguard next generation reprocessing plants.

The purpose of this project was to investigate how to begin to incorporate materials accountability, international safeguards (data validation), and security into one integrated system early in the design process. Much of the data used in these systems overlaps or could be better used if all areas had access to that data, so an integrated system could be much more efficient. It would also open the door to taking advantage of new data sources to strengthen the security of the plant.

The Advanced Fuel Cycle Initiative (AFCI) is interested in building a new reprocessing capability in the United States. However, it has been many years since a commercial-scale plant has been built in this country, and technology has improved significantly in that time. It also makes sense to learn from past projects around the world to prevent future plants from becoming too expensive.

Existing work in the AFCI program has developed a Safeguards Performance Model which has focused on designing the materials accountancy system for a reprocessing plant. The model could be extended to incorporate data validation and security as well. This paper provides a path forward on how to integrate these aspects into the model.

2.0 Safeguards Performance Model

The Safeguards Performance Model is a transient materials tracking model of a UREX+1a reprocessing plant. The Simulink toolbox, part of Matlab, has been used to develop a flow model. This model tracks cold chemicals, bulk fluid flow, solids, and the individual elemental quantities of uranium, plutonium, neptunium, americium, curium, cesium, and strontium. Expected separation efficiencies are modeled to determine the quantity of nuclear material going into different streams. Measurement models are used to simulate an expected measurement from a particular piece of instrumentation. The model has been used for materials accountability analyses, but it can be extended to evaluate the integration of security and data authentication as well. The following sections describe the mass balance, measurement models, and statistical analyses in more detail.

2.1 Mass Balance

The Simulink model is broken down into five different sub-models: front end, UREX extraction, CCD-PEG extraction, TRUEX extraction, and TALSPEAK extraction. Dividing the plant up in this manner will be useful for potential changes to the separation steps in the future. An entire plant simulation runs each model in sequence. The model currently does not include product conversion at the end of each separation step, but this can be added later if appropriate. The final product from each separation step (in dissolved fluid form) is used as the plant output.

A complete mass balance was used as the basis of the model, so at any point in the model the total mass entering a component equals the total mass leaving a component unless the component volume or state is changing. Cipiti et al. [1] provide more detailed information about the mass balance. Every stream in the model contains information about the volume and mass flow rate, the concentration of the 7 key elements tracked, and the solids flow rate where appropriate (at the front end). Separation efficiencies are used in the dissolver and the contactors to determine the percentage of each element going into a specific output stream. Section 2.3 includes pertinent data about the flow rates and separation efficiencies.

Tanks are modeled assuming a well-mixed volume. In other words, it is assumed that if sampled, the tank will be at a perfectly mixed state based on the input and output streams. The modeling of the contactor trains is less intuitive, but simplified since details about the individual contactors may not be known (from the materials accountability standpoint). Each contactor train is broken up into three different model blocks to represent the extraction, strip, and scrub stages. Each contactor block contains a volume equal to the number of stages within that block. Each block has two inputs and two outputs (organic and nitric acid), and the elemental content in the outputs is defined by a total separation efficiency.

2.2 Measurement Models

A universal measurement block has been designed for use in any location within the model. This block can be used to simulate any type of desired measurement having to do with mass, volume, flow rate, or concentration. The purpose of the block is to simulate measurements and then log

that measurement history as a variable in Matlab. Once the measurements are collected, statistical tests can then be used to analyze the data. Variations of these measurement blocks can be used for non-accountability measurements such as item accounting which will be important for international safeguards and security.

Each measurement block contains parameters that are supplied by the user. The user specifies which stream variable is going to be measured (such as the bulk fluid flow or an individual element's concentration) and the sampling period of the measurement. Finally, the random error, systematic error, drift, and calibration period can be defined for that particular measurement. The data from this measurement is recorded into a matrix with one value for each time period.

2.3 UREX+1a Model

This section provides a summary of the model for background to better visualize how the model can be extended to include data validation and security aspects. The following five figures show the complete UREX+1a model in Simulink. Plant equipment is labeled below the block, and each type of equipment shows the number of in-flows and out-flows. The main dissolver solution output from each sub-model becomes the input for the next sub-model. Measurement blocks are labeled by the measurement type below the block.

The measurement blocks at first glance will appear to be excessive. The measurements shown in Figures 1-5 are for an advanced plant that may be able to take advantage of technology advances to include more in-process measurements. For a more conservative approach that only uses measurements that are available on plants today, much of this added measurement data can simply be ignored as if it did not exist.

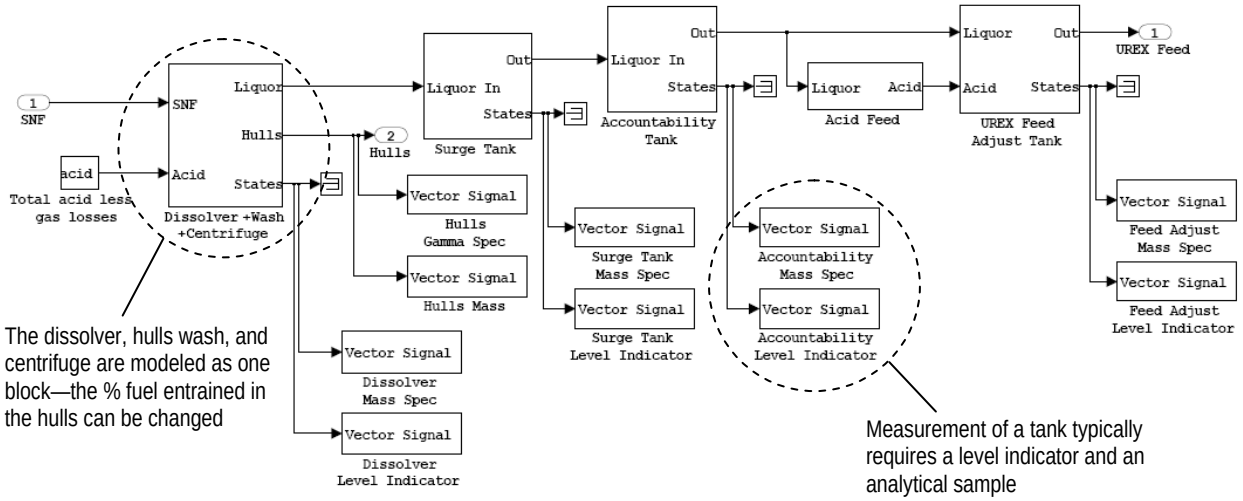

Figure 1: Front End Model

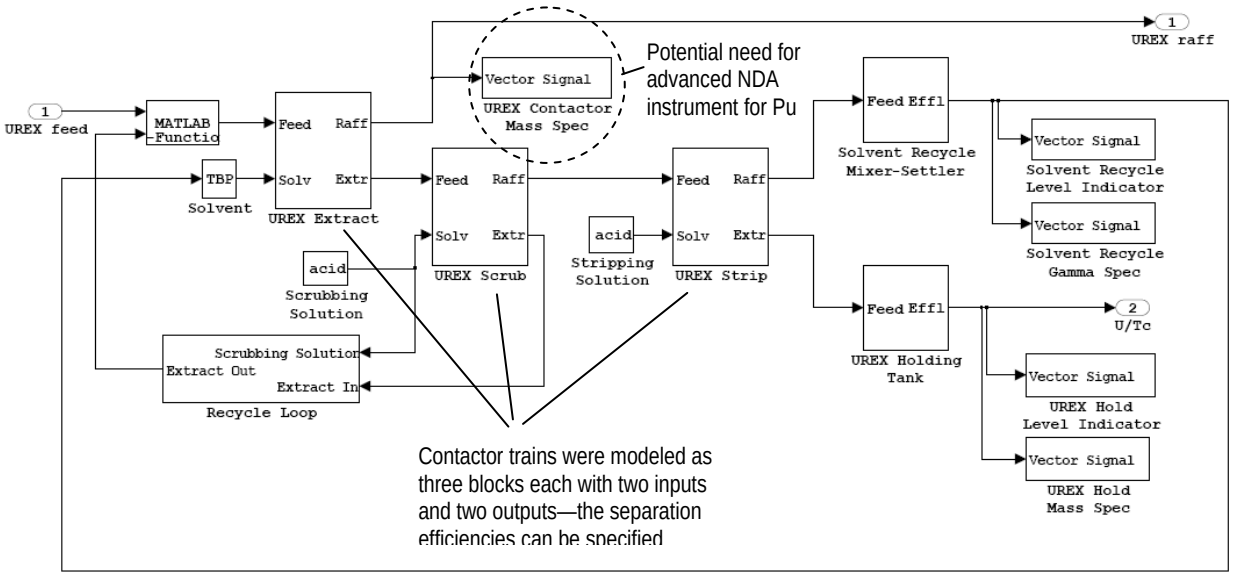

Figure 2: UREX Extraction

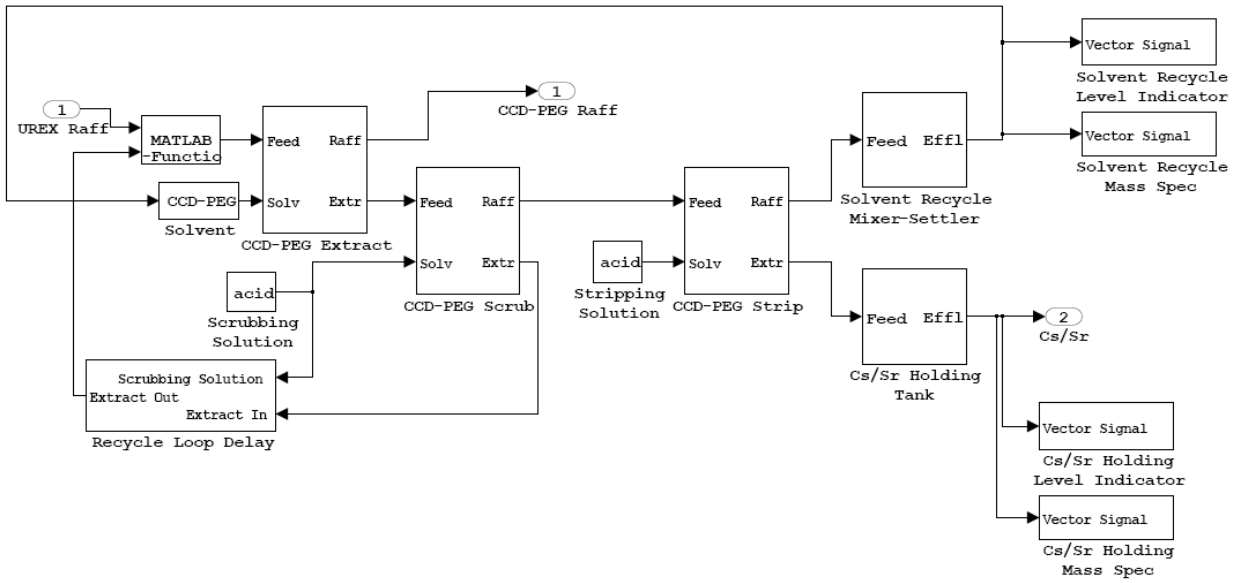

Figure 3: CCD-PEG Extraction

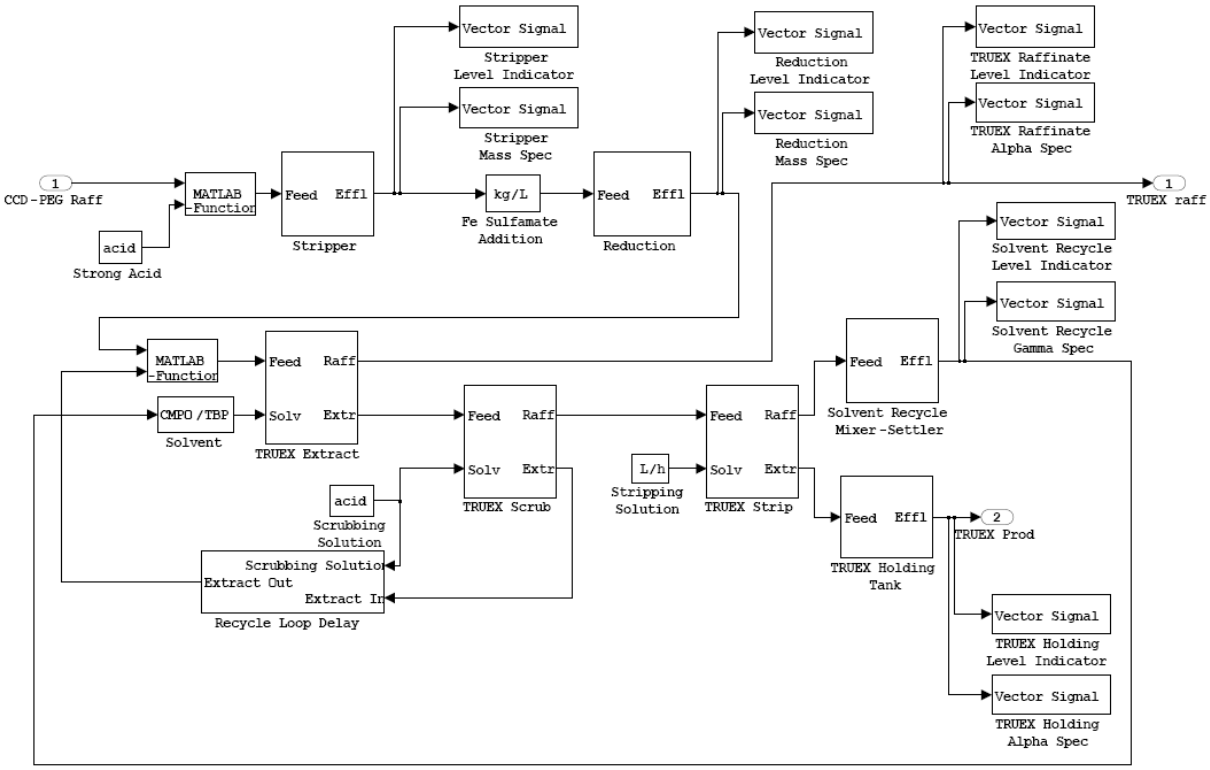

Figure 4: TRUEX Extraction

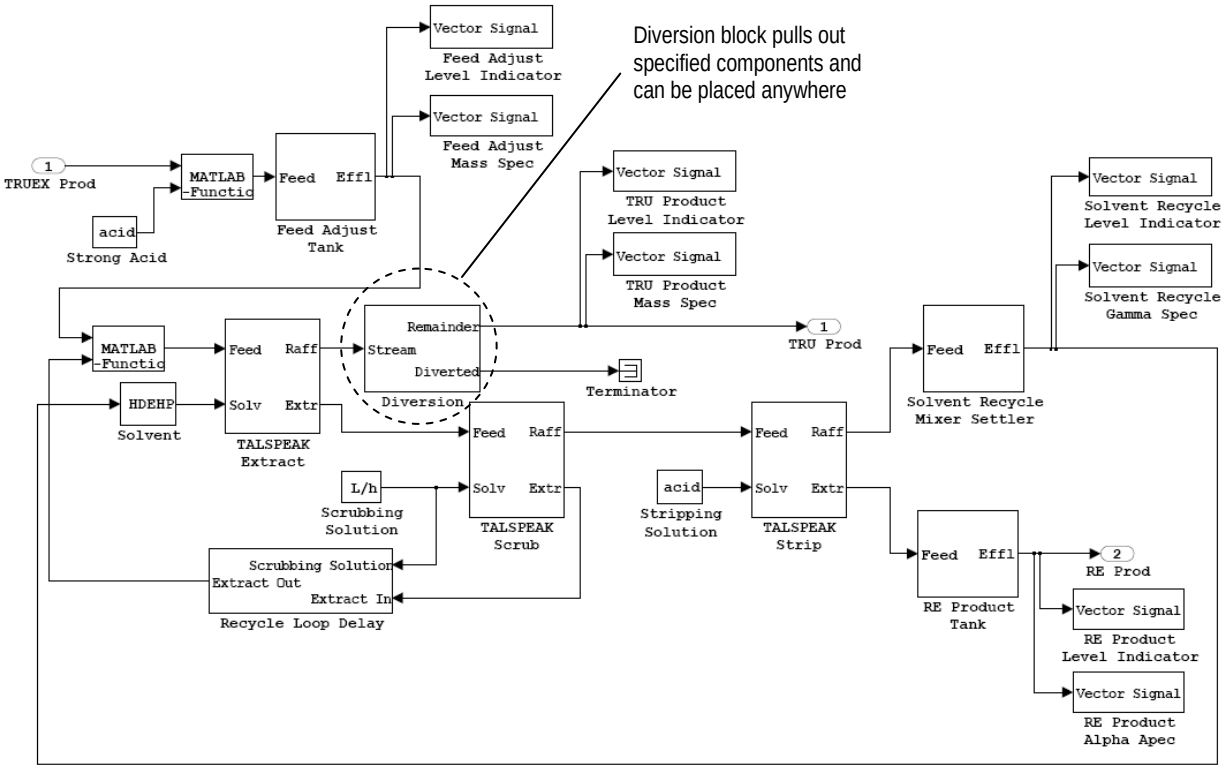

Figure 5: TALSPEAK Extraction

The Safeguards Performance Model already contains the process stream data, and measurement blocks simulate measurements of both process monitoring and materials accountancy information. It will not be much of an extension to include additional measurements or monitoring points that are used for security or international safeguards.

For example, item accounting and radiation monitors have not been included in the model yet, but these could be added. This information will be useful for both materials accountability and plant security. For international safeguards, authenticated measurements from independent instrumentation is required. These additional measurement points can be added to the model to compare domestic accountability systems with the international accountability systems.

The overall goal of this work is to design integrated data management and control systems to improve the effectiveness and lower the cost of safeguards and security of future plants. This goal is long-term, and demonstration using a model will be accomplished in future work. The next two sections describe the attributes of data authentication and security which will be used to help guide model development in the future.

3.0 International Safeguards

The international expansion of nuclear power will lead to greater needs for new domestic and international safeguards systems. Nuclear materials accounting activities within AFCI will be international in scope, and will likely involve safeguards partnerships of different types among the numerous countries. In the context of these partnerships, safeguards protocols will be applied to international shipments of nuclear materials, as well as to associated reactors, nuclear material storage, and processing facility inventories. The full scope of AFCI safeguards activities must be compatible with the specific requirements of each partner's domestic nuclear materials control and accounting regime; at present, these are not uniform. These future AFCI safeguards systems must also support any regional and international safeguards regimes under the purview of the International Atomic Energy Agency (IAEA) that will pertain to AFCI transactions. The support of the IAEA for nuclear cooperation is promising in this regard. Ideally, a new and unified system of nuclear material inventory tracking and control will be deployed throughout the AFCI partnership, satisfying at least the essential requirements of domestic, regional, and international safeguards protocols.

In order to draw valid safeguards conclusions, a national or international safeguards authority must rely upon process and inventory data that are assured to be accurate and complete. Calculations of process mass balance and inventory are only as valid as the supporting data. Assurance of data validity may be provided by authentication measures integral to the safeguards equipment and their data records. Some unavoidable disadvantages to the operator are presented by the necessity of data validation under external safeguards control. In the case of IAEA monitoring, data authentication requires that inspectors have direct electronic and physical access to the safeguards equipment, during which time the operator's access is severely limited. Operator support for IAEA personnel access, such as providing escort and logistical aid, can be intrusive and potentially disruptive to plant operations. The operator has limited freedom to repair and maintain safeguards equipment in joint use with the IAEA due to authentication measures. The cost and inconvenience of authentication grows as tamper indicating conduits and enclosures are required, due to burdens of installation, sealing, and inspection activities. However, the benefits to the AFCI operator of authentication measures will be substantial, especially when the advantages of remote and unattended safeguards monitoring systems are considered. A full treatment of data authentication for safeguards monitoring is beyond the scope of this work; a comprehensive reference is available [2].

3.1 Data Authentication

A key element of any nuclear material tracking and control system is its authentication capability. Authentication is accomplished by measures that give the recipient of information or material the assurance that it is genuine, and has not been altered from its original state or replaced with a counterfeit. The value of nuclear material diversion to an adversary drives their efforts to subvert safeguards monitoring and controls. The IAEA assumes that the threat to their safeguards equipment in a facility is the facility operator acting with the support of the host nation. This type of "insider" adversary is extremely formidable, driving the need for system authentication architectures that are verifiably robust against all forms of tampering and subversion. The AFCI program has yet to define the level of adversary capability it will consider

for its safeguards design, but it can be assumed that comparable authentication measures will be necessary.

An important aspect of authentication concerns the timing of implementation. The best time to implement data authentication is in the design stage. Practical experience with international safeguards has shown that it is practically impossible, or prohibitively expensive and disruptive to operations, to implement data authentication on systems that are already installed and in use. It may be more expensive to retrofit authentication than it would be to remove and replace the entire safeguards system entirely. The AFCI safeguards design process should adopt a policy of "authentication by design" as a general policy.

3.2 Data Authentication in Practice

Successful design and installation of data authentication for international safeguards involves specific approval procedures. Before any equipment can be authorized for safeguards use, the IAEA requires either a Vulnerability Review (VR) by IAEA experts or a Vulnerability Assessment (VA) of the design or actual system by an outside party. In these vulnerability studies, the assumed adversary is the facility operator with the support of the host nation. The formal vulnerability reviews are performed to identify security flaws before safeguards equipment is installed, to avoid costly retrofitting and facility disruption.

A good authentication design will incorporate features to protect both equipment and data from tampering and subversion. The IAEA's fundamental authentication requirements address both hardware and software components; additional authentication measures may be needed in specific cases. The most essential authentication measures are tamper protection and indication. All sensors, cables carrying raw data, and all other security critical components must be sealed inside a tamper indicating enclosure (TIE) or tamper indicating conduit. Without such enclosures, the adversary can subtly alter hardware and software or undetectably extract and analyze safeguards information to achieve an undetected material diversion. Cryptographic authentication must be applied on all data before transmittal outside a tamper indicating enclosure. This prevents data substitution or analysis by the adversary.

Note that data authentication benefits both the facility operator and the national party under safeguards, as well as the IAEA. With robust authentication in place, the safeguards analysis of the IAEA can be based on high-confidence data records. With an unauthenticated system, data errors or deliberate subversions by an unknown adversary may place a legitimate facility operation under needless suspicion of nuclear material diversion, with attendant costs and disruptions.

3.3 Data Authentication Scenarios in Nuclear Reprocessing

An authentication capability establishes objective measures of confidence that the hardware, software, and data components of a nuclear materials safeguards system have or have not been compromised or otherwise subverted by an adversary. If successful in their attack on the safeguards system, the adversary would be able to divert nuclear material for illicit use. To

illustrate the types of safeguards compromises that data authentication can deter and detect, consider the following examples from a hypothetical nuclear fuel reprocessing facility:

- An automatic sampler collects a small liquid volume hourly from a bulk solution tank and places the sample in a shielded canister by a remote operator. The canister is transported by pneumatic tube system to an analysis station several hundred meters away. The adversary has designed an intercept in this tube system, a concealed location where an operator retrieves the canister and slightly dilutes the sample in a very brief time, returning the canister. The data obtained from the sample analysis is rendered inaccurate. This allows undetected diversions of small amounts of solution from the reprocessing area.

- Data from flow meters are collected from a series of sensors throughout the reprocessing plant and stored on a central data server in spreadsheet files. The plant operator uses these files for periodic internal material control and accounting. The data files are transmitted to the national safeguards authority for their confirmatory analysis. The adversary modifies certain values in the data files before transmittal, enabling the diversion of small quantities of nuclear material.

In the first example, the lack of authentication measures on the canister being transported allowed ongoing and undetected nuclear material diversions. The data values from the sample analysis were compromised by a physical interference in the process. This example illustrates how physical authentication measures are integral to the authentication of data values. In the second example, the lack of authentication measures (encryption) on the sensor data made it possible for the adversary to provide bogus data to the safeguards authority and carry out a nuclear material diversion successfully.

The sample dilution attack can be defeated by a tamper-indicated enclosure and seal system. Before tube transport, the canister lid is secured with a tamper-indicating seal. The body of the canister is tamper-indicating as well, and has a unique identifying mark to defeat counterfeit substitution. For additional security, the pneumatic tube might be enclosed in a tamper-indicating conduit. Both the conduit and the canister bodies are subject to random inspections for integrity. Before the sample is analyzed, the operator checks the seal integrity and the canister identity as verification. With this system, any attempt to subvert a tube would be detected. If the tube were subverted successfully, the seal or the canister would have to be defeated quickly and repaired to pass an integrity inspection. The level of difficulty required to accomplish this attack serves to deter an adversary as well as provide a confident means of detecting any such attempts.

The database attack can be defeated by data authentication measures for the process sensors. First, the sensor data processing takes place within a sealed tamper-indicating enclosure under control of the national authority. An authentication signature is applied to the data, and it is strongly encrypted with the national authority's public key before transmittal outside the enclosure. This occurs on a regular and continuing basis. The encrypted data records may be securely stored in the local facility before transmittal. After the records are decrypted by the

national authority using their private key, the data records are provided to the facility to perform their analysis.

The examples of material and data authentication measures provided are not a complete defense against all forms of subversion, but do illustrate the utility of authentication for safeguards.

3.4 Authentication of Unattended and Remote Monitoring Systems

Unattended and remote monitoring systems using authentication have many advantages. They increase the efficiency of both the operator and the independent safeguards activity. As facilities become larger and more highly automated, inspector entry into the facility becomes more difficult and more intrusive. Escorting inspectors diverts facility personnel, and normal plant operations can be disrupted. Installation of unattended or remote monitoring equipment lowers costs by reducing of the number of inspector facility visits to verify operations and collect data, also relieving the burden on traveling inspectors. Joint use equipment using authentication reduces the complexity of the facility since less equipment is installed.

Disadvantages of unattended and remote monitoring are the cost of authentication measures and ease of access by the facility operator. Incorporating authentication components and supporting infrastructure in the equipment and facility design phase is most economical. As previously noted, retrofitting existing equipment already installed, even if technically feasible, may be prohibitively expensive and interrupt operations. In a typical authentication operation, after the safeguards authority performs authentication procedures on the equipment, it is placed under seal. The operator is not permitted access to the equipment unless accompanied by an inspector. This constraint may complicate maintenance and repairs of failed equipment, but is unavoidable given the nature of the assumed threat to the safeguards system. On the other hand, the facility operator is completely relieved of all safeguards equipment maintenance burdens.

Inspector visits inside the facility are expensive for the operator. Site personnel must leave their normal duties to serve as visit escorts, disrupting facility operations. While the need for inspectors and technicians to access equipment for inspection, maintenance, and upgrades can never be completely eliminated, such visits can be minimized by implementing the following features for authentication:

- Apply cryptographic data authentication as close to the sensor (data generator) as possible to minimize the need for tamper indicating enclosures.
- Use active (real-time) intrusion detection measures instead of passive tamper detection, since passive tamper elements do not provide timely detections of tampering.
- Use multiple layers of active tamper detection to increase confidence in the integrity of the system and thus data authenticity. Physical inspection of passive tamper indicating features may not be necessary except for resolution of anomalies.
- If the operator has agreed to give remote access to the equipment by virtual private network (VPN) technology, the inspector may be able to remotely maintain the equipment and install upgrades and patches without an inspector visit.
- Design the equipment to minimize the need for inspections.

3.5 Joint Use Equipment and Authentication

Process monitoring and safeguards monitoring equipment can be expensive to install and maintain. For this reason, the joint use of specific equipment between multiple parties can be arranged. In establishing a joint use system, all parties must be satisfied that the equipment is functioning properly and that the data is legitimate. The benefits of Joint Use Equipment (JUE) systems are numerous. Properly developed and deployed joint systems result in ease of data collection, reduction of support burdens, and reduced costs for the IAEA, the cognizant national safeguards authority, and the operator. However, the potential disadvantages are significant. The independence, integrity, and authenticity of data from JUE must be achieved with a high degree of assurance in order to protect the interests of all parties, including proprietary commercial information. The implementation in practice of joint use systems for international safeguards is subject to IAEA policies and the associated technical requirements. These considerations govern the negotiation of a formal Joint Use Arrangement (JUA) implementing the equipment and data sharing arrangements between the IAEA and the external party.

The complete data record from a defined time interval is typically not immediately available to the operator to support inventory analysis. At least some data may not be shared until after an operator's inventory declaration has been received by a safeguards authority, since an independent conclusion must be determined. In the case of IAEA safeguards, any upgrades and software changes to the equipment will require advance approval, and these will likely be carried out by IAEA personnel. Depending on the scope and complexity of the modifications, a new vulnerability analysis could be required to assure security concerns are evaluated and remediated as needed.

3.5.1 Joint Use Data Authentication Example

The following case study presents an example design for data validation in a safeguards instrument to be installed at a hypothetical AFCI facility. For brevity, the details of secure communication of data files outside of the facility are not described.

A new process train will be built at an existing plant. The flow rate and conductivity of a continuously flowing solvent pipe will be measured for accurate safeguards monitoring. Data values will be recorded every 1 second for safeguards analysis. The instruments will be mounted in a remote area of the plant in an elevated radiation area. Worker or safeguards inspector access to the area will not be routine, and will likely only occur during quarterly plant maintenance periods when the pipe is washed out for inventory measurements. The IAEA and the national safeguards authority have agreed to the joint use of the data, which will be shared with the facility operator for their internal inventory control analysis.

The flow and conductivity sensor elements are sited in a pipe access port, in contact with the process solution. A data cable 10 meters long connects to the sensor electronics in a TIE. The cable is enclosed in a metal tamper-indicating conduit, and welded to the pipe to cover the access port completely. The TIE enclosure is secured with an active electronic seal unit. No facility personnel can open the TIE without activating the seal alarm, which would record the event and securely transmit the alarm to the central facility safeguards monitoring control station. Each

day, the safeguards data file is authenticated, encrypted, and stored for later communication to the IAEA central data collection computer in the facility.

The security module in the TIE will store a unique public-private cryptographic sensor key pair. The sensor private key will be generated by the IAEA inspector when the system is activated and sealed. This secure process within the protected security module creates a public-private asymmetric cryptographic sensor key pair. The private half of the sensor key pair is stored within the security module. This private key is never exported from the module and cannot be read from the module. Module tampering will result in the zeroing of the private key and all stored data. Also within the protected module is a monotonically increasing counter, or timer, which is running continually and cannot be altered (except that it could be reset when the key is created). The public half of the sensor key pair is exported from the module and given to the IAEA staff upon initiation, for transfer to the IAEA Certificate Authority, which creates and publishes a public key certificate.

The safeguards data file is supplied to the protected security module, which uses the sensor private key and trusted time to create a digital signature which is appended to the safeguards data file. After secure transmission to the IAEA, the digital signature block is verified using the sensor public key.

3.6 Integration with Domestic Safeguards

Given the constraints on the operator in using dual-use equipment, future plants may find it more desirable for ease of operation to maintain independent systems for safeguards. As long as the independent systems are designed into the plant at an early stage, the cost can be minimized. However, the international instrumentation should be designed in such a way as to minimize impact on operations. Plant operators will only need to be concerned with operation, maintenance, and reporting of their domestic equipment.

Future changes to the Simulink model will design in independent instrumentation for international safeguards. The measurements from the model can go to an independent mass balance and can be compared to the domestic system. The model then can be used to evaluate diversion or misuse scenarios that could slip through one system or both. In this fashion, the model can be used as a basis for designing in authentication early.

Data authentication will provide an essential capability to the AFCI partnership. The entire enterprise will benefit if data authentication is considered from the earliest stages of AFCI design. The technical expertise and experience of the international safeguards community should prove invaluable to AFCI in establishing its data authentication systems.

4.0 Physical Security[1]

Within the NRC body of regulations that apply to nuclear facilities, including fuel cycle facilities, domestic safeguards include physical security and material control and accountability (MC&A). Physical security is implemented by a facility's physical protection system (PPS). Physical protection is defined as the use of technical, administrative, and operational measures to prevent the theft of nuclear material for the purposes of producing nuclear weapons, producing nuclear devices for nuclear terrorism, or using a facility or transportation system for radiological sabotage.

4.1 Regulatory Context

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." Because AFCI facilities, including the advanced reprocessing facilities, may be included on the list of U.S. facilities for inspection by the IAEA, NRC requirements under 10 CFR 75, "Safeguards on Nuclear Material – Implementation of US/IAEA Agreement," may also need to be considered. The focus of international safeguards is protection against material diversion for the manufacture of nuclear weapons by the host state.

Within its regulations, NRC has performance-based requirements to establish a design basis threat (DBT) that is based on the potential consequences of a variety of adversary attacks on their respective operations. Physical protection and MC&A include performance-based requirements, as well as other very specific security 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. Vital area analysis is an approach that defines critical areas of a facility that must be protected. A vulnerability assessment (VA) is a systems analysis methodology that evaluates the effectiveness of a site's safeguards and security (S&S) protection systems against a range of potential threats that include sabotage, theft, or diversion of nuclear material. A VA is conducted to provide a risk-based determination of the appropriate level of protection. The potential consequences of a successful adversary attack determine the level of protection that an S&S system is required to provide.

One of the most recent developments for reactor S&S by the NRC is the security assessment technology manual that provides high-level guidance for new nuclear reactors license applications [3, 4]. The NRC has adopted and adapted the Design Evaluation Process Outline (DEPO) systems analysis methodology that has been applied extensively for the VA of the PPS [5, 6, 7, 8]. The manual updates and revises a previous version of the report to provide conceptual and specific technical guidance for new nuclear power plant license applicants as

[1] This discussion includes excerpts from Section 5.2.4 of Durán, et al., "Consolidate Fuel Treatment Center Regulatory Assessment, Rev. 0," GNEP-CFTC-SAFH-MI-DV-2008-000287, U.S. Department of Energy (2008)

they develop a layout of a facility to enhance protection against sabotage and facilitate the use of physical security features, design the PPS, and analyze the effectiveness of the PPS against the DBT. It is expected that a similar guidance would be developed and required by the NRC for fuel cycle facilities as well. Modeling and analysis tools currently available and under development for licensee use are also described in the technology assessment manual.

4.2 Design and Evaluation of Physical Protection Systems

The PPS is an integral part of any nuclear facility. A PPS should be designed to provide sufficient deterrence, detection, delay, response, and mitigation of the DBT to provide assurance of sufficient nuclear material protection, and prevention the theft, diversion, and/or radiological sabotage of nuclear material. In "balanced" S&S systems, physical protection elements are integrated with nuclear MC&A programs and systems to ensure that accountable nuclear materials do not bypass the MC&A systems.

The VA systems analysis methodology evaluates the effectiveness of a site's protection systems to calculate a probability of system effectiveness (P_E) for the PPS. P_E is a measure of the degree to which the system can protect targets against a range of potential threats. Several modeling and analysis tools are available to support VAs (e.g., path evaluation using Analytic System and Software for Evaluating Safeguards and Security (ASSESS) [9] and Advanced Time Line Analysis System (ATLAS) [10], and response force evaluation using Joint Conflict and Tactical Simulation (JCATS) [11], table top exercises, and field exercises (force-on-force exercises)).

Depending upon threat motivations and capabilities, a facility's protection strategy can vary from "denial of access," "denial of task," or "containment." The overall S&S system of a facility is designed to protect against the DBT by integrating physical security and MC&A systems and practices. A graded and layered approach and defense-in-depth philosophy for the design of the PPS, supported by the appropriate cost/benefit analyses, can help ensure that a desired protection level is achieved. This approach provides multiple layers of protection in order to achieve an adequate level of facility/material target protection.

4.3 New Facilities Design

For the construction of new facilities, early consideration and inclusion of S&S programs in the conceptual/preliminary design phases of the project improve the overall effectiveness of the PPS, and ultimately reduce the costs associated with design, installation, and sustained operation of the PPS[2]. New facility designs should incorporate proven, standardized S&S equipment and

[2] The objective is to minimize overall lifecycle costs of the PPS, *NOT* initial PPS capital costs. Initial costs may be higher for the "optimum" S&S system than for other options, but the overwhelming majority of lifecycle costs are typically encountered in recurring, variable labor and retro-fit cost incurred once in operation, rather than in the fixed capital expenditures that are incurred early in the design, construction, and start-up phases. Also, from a capital-cost only perspective, establishing the correct, performance-based PPS at the outset is generally less costly in the long term than designing and installing a minimal, yet compliant, PPS initially, and then adding Security features later when more sensitive operations are planned. Such an approach (adding Security to a completed facility) is generally the worst of all worlds, typically involving high capital asset acquisition expenditures, *AND* high recurring premium labor costs (for off hours, higher skill, accelerated schedule, etc.), as well as potentially reducing overall PPS effectiveness.

systems where possible, as well as adopt emerging S&S technologies (when they have been demonstrated to meet the requisite standards), without compromising design flexibility or adherence to overall system effectiveness requirements. This approach provides a mechanism for the establishment of the PPS from the onset of the project, as well as ensuring timely and cost-effective procurement, installation, operation, and testing of identified security features. Additionally, this approach provides a means to integrate physical security and material control equipment, capabilities and strategies.

The commercial-level throughput processes envisioned for GNEP fuel-cycle facilities will require innovation to meet production goals while ensuring adherence to future S&S performance standards. While GNEP facilities will be designed, constructed, and operated in accordance with NRC regulations, due consideration should be given to some of the lessons learned in similar U.S. DOE programs. U.S. DOE sites use a variety of VA applications, processes, and methodologies to determine the optimum PPS design for a given facility. Inclusion of the VA process in the early stages of nuclear facility concepts and designs is an integral part of emerging S&S project management practices. DOE S&S programs provide lessons learned for application of best practices, where appropriate, for GNEP facility designers.

The goal of these efforts is the development and implementation of a framework, methods, and tools that can be applied for modeling and evaluating integrated systems from the beginning of facility design and throughout facility operation. A few recent examples are discussed in the following sections.

4.3.1 Pit Disposition and Conversion Facility (PDCF)

The Pit Disposition and Conversion Facility (PDCF) is a premier example of the concept of accounting for S&S features in the early design phases by performing Preliminary and Conceptual VAs, and using simulations and modeling to refine the final facility design to protect against the DOE DBT. The PDCF design was developed in an iterative process, involving intense collaboration between S&S Analysts, site operations personnel, and Design Engineers. The designers and the Savannah River Site (SRS) VA team worked closely to ensure that accurate ASSESS models were developed, and that the results of numerous JCATS simulations, conducted on “notional” facility designs, were used to refine the facility’s PPS into the most final design.

The SRS VA team used the results of the ASSESS and JCATS “runs” to determine a number of increasingly effective design enhancements, and refine the PPS and facility structural design into the most effective PPS configuration. It was the first time the JCATS system was used in this a manner. It allowed the designers to modify the design, based on the simulations derived, and re-simulate the adversary scenario until they had determined the design met the acceptable risk profile of the customer. All of this was done on a facility that does not yet physically exist, yet an effective PPS has already been determined.

In the event of an escalation of DBT capability or PPS technology enhancements, the system can be evaluated in near-real-time on a simulation to determine the impact of those changes. This approach is not only system-effective it has been demonstrated to be cost-effective as well.

Another ancillary benefit discovered during this project is that while JCATS cannot be used to replace them, this approach is also safer than live Force-on-Force exercises. It is also believed to be an effective training tool to hone the battle-management skills of protective force and response force leaders.

4.3.2 Mixed Oxide Fuel Fabrication Facility (MFFF)

The Mixed Oxide Fuel Fabrication Facility (MFFF) proved to be an ideal opportunity to apply the lessons learned in the design of PDCF to another (at the time "notional") facility. Similar iterative processes (slightly modified to reflect process improvements and site-and operation-specific conditions) were employed in the design and validation of both the MFFF and the PPS designs. The results were satisfactory, in that the MFFF is now in the early stages of construction at SRS. It is believed by those who participated in the MFFF analyses and modeling that the application of the "Security by Design" approach was instrumental in the construction authorization for the MFFF by the NRC, and will be a major determining factor in final licensing once it is completed.

4.3.3 Advanced Fuel Cycle Facility (AFCF)

The AFCF is an AFCI project, and is still in early conceptual stages of design. The AFCF design includes large shielded and remotely maintained areas to validate, demonstrate, and improve spent fuel treatment processes, fuel fabrication processes, and Safeguards monitoring. These systems will be fully integrated and operated at "Engineering Scale," and will be designed, constructed and operated with emphasis on protection of public and worker safety and the environment. In addition, the AFCF is also a technology demonstration facility. Thus, the PPS will be designed to show that applicable IAEA and NRC requirements can be met.

The S&S system for AFCF is intended to be an example of "Safeguards and Security by Design." Its processes, operations, structures, and protection systems are intended to be designed and constructed in a manner that will provide inherently robust protection of special nuclear material and spent nuclear fuel. The unique construction features, the distinctive, "self-protecting" nature of the materials being produced in the facility, and the implementation of advanced S&S measures are designed to provide inherently high levels of proliferation resistance. The AFCF S&S function will meet all current DOE requirements for the production, storage, and transportation of Category I special nuclear material, in a manner sufficient to prevent the theft, unauthorized use, or radiological sabotage by an adversary force as defined in the current (2005) DOE DBT.

As it progresses, the facility design will incorporate innovative, state-of-the-art protection system features to ensure adequate protection, mitigate the impact of future changes in the DBT, and minimize the number of protective force personnel required to achieve a level of protection that is acceptable to the DOE. Those facility design features will be modeled and tested in simulations. The DOE and NRC both have licenses for JCATS, and the DOE is currently evaluating another tactical simulation (automated Vulnerability Evaluation for Risks from Terrorism - AVERT, an emerging simulations technology) for eventual approval as a VA scenario validation tool.

The MC&A program will be based on two levels of requirements. The first level will provide the current safeguards required for licensing, regulating, and/or monitoring the AFCF. The second level will provide the capability to develop advanced safeguards for licensing, regulating, and/or monitoring future full-scale *commercial* nuclear reprocessing facilities. The AFCF will comply with all DOE MC&A requirements. It will also provide the capability to develop and demonstrate advanced compliance methods related to the NRC and IAEA requirements. The above measures are principally directed at proliferation resistance at the sub-national level, by insider or sub-national adversary groups.

The processes and facilities recommended in the AFCI were selected to enhance proliferation resistance at the national level, taking into consideration the future prospect of deployment of the facilities of the AFCI fuel cycle to additional national and international locations. The principal safeguards against national proliferation are the measures applied by the IAEA. The AFCF design has progressed towards making provisions to demonstrate measures that might be applied to facilitate implementation of international safeguards by the IAEA. While the throughputs and inventories of the AFCF may not be significant related to the potential of production facilities anticipated in the future (and the national and international Safeguards measures that will therefore be required), innovative protective measures are being developed and incorporated in AFCF and future production facility designs. A key component of international safeguards for large-scale production facilities involves measures to monitor the locations and movement of nuclear materials as they are transferred into and out of material balance areas. These measures typically consist of surveillance cameras and gross radiation sensors. Their success is tied to the effectiveness of facility features specifically designed to enhance their effectiveness.

The AFCF design, while not specifically requiring these measures to meet the requirements for a facility of its size and throughput, is evolving to include provisions for demonstration of these measures. Recommendations for design of storage facilities and material transport provisions are being incorporated. Another example of effective international safeguards is the timely analysis of samples of nuclear materials from within the operating facilities. Timely results require enhancement of the independent analysis capability of the international organization on-site. The design of the AFCF has evolved to include these capabilities. In addition, measures for verification of the integrity of samples as they are drawn from declared locations and delivered for independent analysis are also being considered for demonstration in the AFCF facility design.

The S&S philosophy of PPS design is evolving to include demonstration of independent and authenticated measurements for verification of operator declarations by international organizations, and to consider reporting through the national system to the international regulatory body, the IAEA. The program has illustrated the need for a comprehensive data collection and evaluation system to support material accountancy and reporting on a national level, similar to that required of future domestic commercial facilities.

4.4 Integrating Safeguards and Security for Nuclear Facility Design

The need for integration of S&S, as well as safety and operations is an issue that is being addressed in all of the current efforts for developing future nuclear facilities (Generation IV,

AFCI, IAEA). In the past, individual assessments of these areas have been performed through the use of detailed analyses techniques that have not been integrated in the design, evaluation, and operation of a facility. This has often led to inefficient and costly design and operational requirements. The major benefit of integrating these areas is more cost-effective and efficient design and operation of nuclear facilities. Effective integration of these areas, however, will require the development and implementation of validated systems analysis and risk-based tools for modeling and evaluating integrated facility design and operation.

One approach for addressing integration issues is to look at extending established methods and tools. Several evolutionary activities are extending the established DEPO methodology and tools and look to provide different types of integration. The DEPO methodology is a conditional risk approach based on the occurrence of an adversary attack. Wyss et al. [12] developed a risk-based approach for safeguards and security decision-making that provides additional data to consider adversary activities before an attack. Several other efforts address integration of adversary activities to determine a wider range of threats beyond a design basis [13, 14, 15]; to develop an uncertainty risk analysis (URA) [16, 17, 18, 19] technique to evaluate the risks of intentional acts; and to provide total risk assessment capability (TRAC) that addresses adversary threat, vulnerability and consequence [20].

Dawson and Hester [21] developed a real-time effectiveness metric to aid in protecting nuclear materials against theft and sabotage. The material assurance indicator (MAI) considers what materials are being protected, where they are in the facility, and when the material was last handled or monitored. The MAI is designed to provide a quantitative metric of MC&A system effectiveness and to integrate with already-established methods for computing the effectiveness of facility protection systems to create a more complete picture of materials protection system performance. As an additional demonstration of this integration approach, the MAI will be exercised with the AFCI Safeguards Performance Model [22] and is related to an overall effort to develop advanced process data acquisition, authentication, and management for civilian nuclear facilities [23]. In related work, Durán, Dawson, and Wyss [24, 25, 26] have been applying reactor risk methods, including human reliability analysis, and object-based event sequence trees [27] to develop a probabilistic analysis approach to integrate the MC&A protections and operational activities in a VA analysis. These efforts focus on integrating MC&A protections, as well as other operational and process information to provide a measure of effectiveness for this level of system integration.

Darby et al., [28] have also worked on the development of a risk analysis methodology for the analysis of integrated cyber and physical security elements within critical infrastructures. The methodology applies evidenced-based uncertainty analysis techniques with attack graphs to evaluate "blended" security systems to determine the likelihood that a threat defeats a cyber or PPS. In a similar effort to address the insider threat, system dynamics modeling is being applied to model the employee life-cycle and employee interactions with physical, cyber, and operational security system elements and to investigate the development of intrinsic security [29].

As the focus of U.S. nuclear technology development has moved to the international arena, IAEA security and safeguards requirements for non-proliferation are more of a consideration for domestic facilities. The Generation IV (Gen IV) International Forum has had a working group

that has developed the Proliferation Risk and Physical Protection (PRPP) Methodology [30], a risk-based evaluation method that integrates proliferation resistance and physical protection. The PRPP has been in development for more than five years and has been endorsed by the body of Gen IV countries. The Gen IV PRPP working group has exercised the methodology for a sabotage scenario and is also looking at a material theft for proliferation scenario. More recently, the Gen IV Safety Working Group and PRPP working groups have been addressing safety and security integration [31].

Another effort in looking at international safeguards is the demonstration of advanced transparency at the Monju reactor [32, 33, 34, 35]. This work includes the development of a probability model for the calculation of diversion risk and advanced transparency [35], integration of safeguards, security, operations, and safety (SSOS) [34], utilization of system-generated data for advanced transparency [33], and calculation of expected and observed risks in an advanced transparency framework [32].

The Safeguards by Design activities by the DOE (NE and NA) are focusing near-term on addressing DOE requirements for integrating safeguards, physical security, and proliferation resistance to develop a fully integrated design process and achieve institutionalized safeguards by design.[3]

Darby et al. [36] provide a framework for integrating the disciplines of safety, operations, safeguard and security in the design and operation of nuclear facilities. This work references several of the approaches mentioned above, and provides a preliminary framework that begins at the facility design and extends to facility operation. It systematically addresses commonalities and differences among the disciplines and develops strategies for harmonization among them.

The methodologies and technologies described above have significant similarities and overlap in their efforts to address integration of safeguards and security, and in some cases, safety and operations. It speaks to the need for coordination of these activities and the development of an overall approach for achieving integration in these areas. The majority of these approaches are combining or extending existing methodologies, often in an ad hoc manner, to achieve some integration, the level of which, in some cases, is limited by the available analysis tools and techniques. This speaks to the significant need for the development of advanced analysis techniques to provide modeling and assessment of integrated systems. To support the design, licensing, and operation of future nuclear facilities, one key issue is to define the level of integration that is desired and to address the question of the extent of integration among safeguards, security, as well as safety and operations that is achievable. Within this context, future efforts should look to coordinating and leveraging ongoing efforts, systematically addressing commonalities and differences, and developing strategies for an overall framework, then envisioning advanced analysis techniques for implementation.

[3] T. Bjornard, "Fully-Integrated Design Process Institutionalizing Safeguards by Design," presented at GNEP Safeguards Working Group, (December 5-6, 2007).

4.5 Extending System Effectiveness for Physical Protection and MC&A

To determine the effectiveness of a PPS, path analysis is performed to evaluate adversary paths and the associated detection, delay and response timelines. Path analysis determines a probabilistic quantitative measure of timely detection on an adversary path. Adversaries who attempt theft or diversion of material represent formidable threats because they may be in a position to circumvent system elements and interact directly with target material without being detected. The delay and detection timelines associated with the path of adversary through a PPS may not be as relevant because these adversaries can choose the most opportune times and optimum strategies. One strategy for addressing this type of threat would be to optimize the control and accountability of materials, the MC&A component of the facilities S&S system. The previous and ongoing work described in the following sections will be exercised within the Safeguards Performance Model to investigate the applicability of these methods to supporting advanced safeguards development.

4.5.1 Material Assurance Indicator

Dawson and Hester [21] developed the deterministic MAI algorithm as a real-time effectiveness approach for protecting nuclear materials. Before this, no measures or standards for comparison were defined to determine whether a protection system provided effective control of nuclear materials, that is, the effectiveness of an MC&A system. The development of MAIs can be viewed as an extension of VA methodology that provides a quantitative measure, albeit a deterministic one, of MC&A effectiveness. Initial testing for scenarios at hypothetical facilities has demonstrated the algorithm is applicable for evaluating MC&A system capability to provide detection of theft or diversion of nuclear material.

A perfect materials control system would ensure that all the attributes and each location of materials in a system are known all the time. The MAI algorithm estimates real-time effectiveness for each item and indicates material assurance continuously. MAI can also be calculated for groups of items within a single container or vault. The two-part formulation accounts for the attributes, locations, and time interval of materials:

$$MAI = \frac{\sum_{i}^{N} MCF_i \times \left[(H_R, A_R, R_R) \times LF_i \right]}{N} \qquad (1)$$

$$LF_i = \frac{\Delta t}{\max(t, \Delta t)} \qquad (2)$$

where,

MAI = Material Assurance Indicator
MCF = Material Characterization Factor
H_R = Handling

A_R = Attribute Monitoring
R_R = Gamma/Neutron Monitoring
LF = Latency Factor
Δt = Critical time
t = Time when the last handling/monitoring occurred, subtracted from Δt
N= The number of items defined

The algorithm currently provides a deterministic point estimate for each item or group, separate from the pathways analysis methods for determining system effectiveness. This approach will be exercised within the safeguards performance model to determine its applicability for the bulk volume operations in a reprocessing facility.

4.5.2 Extending System Effectiveness for a VA to Incorporate MC&A

A PPS includes many different types of sensors for detection of unauthorized activities. In the MAI work, Dawson and Hester [21] observed that, similar to other sensors that perform a detection function in a PPS, many MC&A activities could be considered a type of sensor system, with alarm and assessment capabilities necessary for detection. Additionally, MC&A procedures and technologies, from monitoring to inventory measurements, as well as process control operations, include methods that provide information about the attributes and location of materials as well as defining possible adversary path elements for theft or diversion of material.

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 VA methodology. Other MC&A elements, however, have been difficult to characterize in ways that are compatible with VA's. The development of the MAI was one step toward addressing this gap and providing a measure of MC&A system capability. Additional development focuses on incorporating MC&A protection elements within the existing probabilistic VA methodology to estimate P_E both physical protection and MC&A.

The MAI algorithm was developed separate from the probabilistic VA methodology for P_E calculations. The VA P_E calculations address the physical protection component of the security system that focuses on external threats while the MAI algorithm development focused on material control. The work of Durán et al. [24] and Durán and Wyss [25, 26] has focused on developing a probabilistic analogue to MAI algorithm in order to enable VA analysts to explicitly incorporate MC&A protections into the P_E calculations performed under the existing probabilistic VA methodology. The goal of these efforts is to provide an integrated effectiveness measure of a protection system that addresses physical protection and MC&A.

4.5.2.1 Object-Based Paradigm for Theft of Material

Adversaries who attempt theft and diversion of material are formidable threats, especially if they have extensive knowledge of and access to target materials. They can take advantage of opportunities that arise to circumvent system elements and to interact directly with target material without being detected. The delay and detection timelines associated with the path of

adversary through a PPS may not be as relevant because these adversaries can choose the most opportune times and optimum strategies. One strategy for addressing this type of threat would be to optimize the control and accountability of materials, and to more fully incorporate and account for MC&A elements in the VA of the PPS.

MC&A activities, from monitoring to inventory measurements, provide information about target materials and define security elements useful against insider threats. In a sense, MC&A protection elements are interwoven within each physical protection layer, and provide additional detection and delay opportunities within the S&S system. Activities that discourage material theft provide many, often reoccurring opportunities to determine the status of critical items (for example, *daily* administrative checks).

Considering these observations about MC&A protection elements, Durán and Wyss [25, 26] applied an object-oriented modeling approach [27] to develop an object-based state machine paradigm to characterize the material theft scenario. The object-based state model is shown in Figures 6 and 7. The "system" is characterized by two objects – a Material Theft object and a Facility Status object. The Material Theft object describes the possible steps in a specific theft scenario. The figures below illustrate the state transition diagrams for each object – the Material Theft object (6) and the Facility Status object (7) and their interrelation. Each box in the diagrams is a "state" in which the object can be at a point in time. The arcs between each state are events that can occur to move the object from one state to another. This approach characterizes material theft as a "race" between the theft stages from internal to external physical protection layers and the MC&A system elements that detect material is not where it should be. The Facility Status object indicates how MC&A protection elements act as a "switch" that change the state of the facility from normal to heightened alert where the facility is searching for material that is discovered "missing." This characterization of material theft is similar to the characterization of the attack by an outside adversary as a race between the adversary and PPS facility response team after detection has occurred.

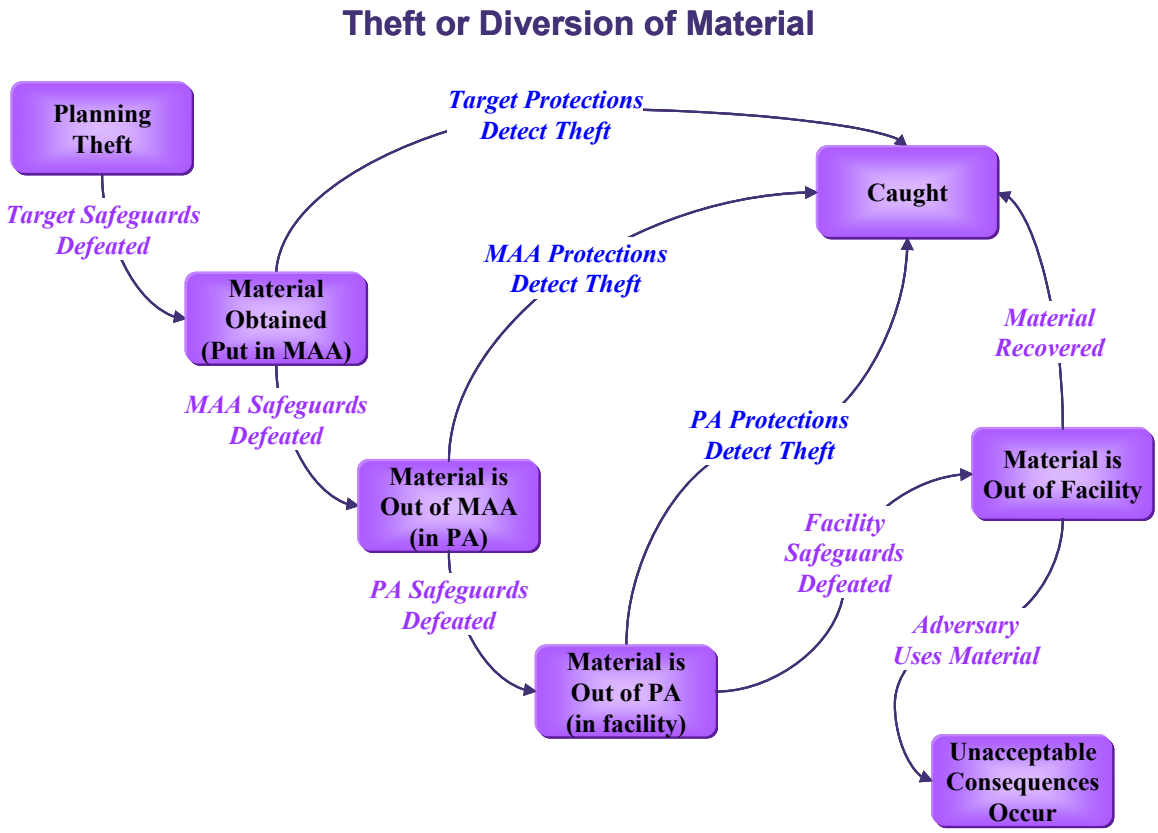

Figure 6: State Transition Diagram for Material Theft Object

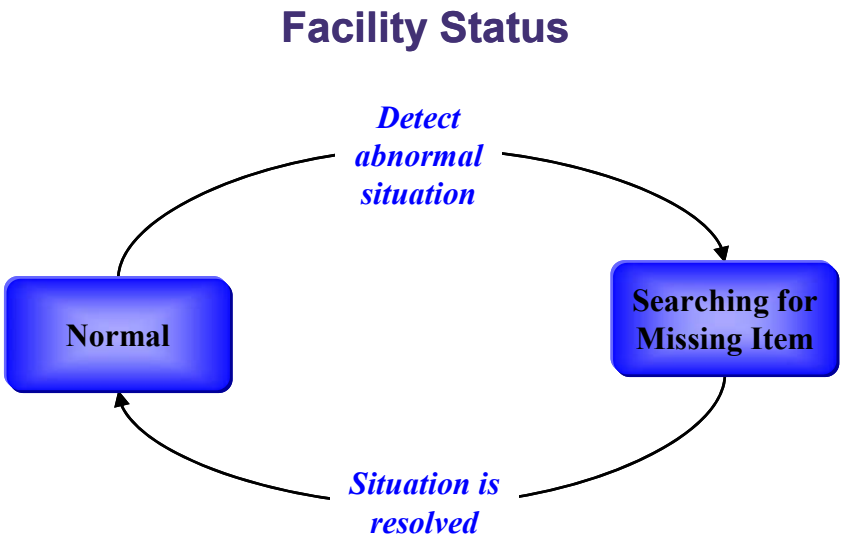

Figure 7: State Transition Diagram for Facility Status Object

4.5.2.2 Timing for Material Theft

One of the challenges for evaluating the effectiveness of an S&S protection system against theft and diversion of material is that the detection and delay timelines determined for the outside adversary and the PPS are not as relevant because an insider adversary can choose the most opportune time to take advantage of system vulnerabilities. Indeed, the various theft events may be separated by large gaps in time. 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. Probabilistic convolution is a method that has been used previously in nuclear power plant PRA [37] and security timeline analyses [38].

As a material theft is initiated and proceeds through the physical security layers of a facility, we can define the following probabilistic time variables:

T_{R1} - Time for adversary to successfully remove target material from Physical Security Layer 1. Time interval begins when the adversary obtains the material and ends when adversary removes target from Physical Security Layer 1.

T_{R2} - Time for adversary to successfully remove target material from Physical Security Layer 2. Time interval begins when T_{R1} ends and ends when adversary removes target from Physical Security Layer 2.

T_{R3} - Time for adversary to successfully remove target material from Physical Security Layer 3. Time interval begins when T_{R2} ends and ends when adversary removes target from Physical Security Layer 3.

$T_{MC\&AAlert}$ - Time when MC&A activities may indicate that target material is missing. Time interval begins when theft occurs and ends when MC&A alert occurs.

Each of these times is represented as a probability distribution in order to represent the variation in *both* the time before a removal opportunity presents itself and the time to accomplish the removal task. Time and associated probabilities [$P(T_{R1})$, $P(T_{R4})$, $P(T_{R3})$] depend on the defeat methods used in scenario (e.g., removal through SNM monitor after disabling monitor). These data are often available in the existing VA methodology data base. Distributions for a "Normal" facility state can be degraded if MC&A alert has occurred and the facility state is "Searching for Missing Material." Logically, if an MC&A alert has occurred, the facility has a higher probability of detecting and finding the material, and the adversary has a lower probability of successfully removing the material from a Physical Security Layer.

For the last time variable, $T_{MC\&AAlert}$, this is the time when the Facility state transitions from "Normal" state to "Searching for Missing Material" state (Alert). Times and associated probabilities [$P(T_{Alert})$] are dependent on specific MC&A activities included in scenarios. Distributions can be developed considering specific MC&A activities and associated operational considerations. Human reliability analysis (HRA) methods for evaluating operator attention to unannuciated alarm signals during nuclear power plant operations [39] provide insights for developing these distributions. These methods also show how the effectiveness of repeated

inspections decreases over time if an anomalous condition is not recognized the first time it occurs.

MC&A activities contribute to the effectiveness of the facility protection system by providing alerts that material may be missing. The effectiveness of MC&A activities can be determined by comparing the probability distributions for the time for MC&A alerts [$T_{MC\&AAlert}$] with the probability distributions for the time for removal of material by the adversary [T_{R1}, T_{R2}, and T_{R3}] using probabilistic convolution to determine the probability that detection occurs before the material is removed from the facility. The set of possible scenarios to be evaluated can be deduced by analyzing the object model as an event tree.

4.5.2.3 Convolution Integral

As a general example considering removal of material, let T_M and T_R be random variables over time. Let t_M and t_R be specific values of these random variables. The range of T_M and T_R is $[0, \infty]$.

Let $P(t_M)$ denote the probability density function for T_M and let $P(t_R)$ denote the probability density function for T_R. Let $P(t_M, t_R)$ denote the joint probability density function for T_M and T_R.

A random variable for time of possible "detection" is defined as $T_D = T_M - T_R$ and t_D is a specific value of this random variable. The probability density function for T_D is:

$$P(t_D) = \int_0^\infty \{P(t_M, t_R) \mid t_R = t_M - t_D\} dt_M \tag{3}$$

If T_M and T_R are independent, then $P(t_M, t_R) = P(t_M) \cdot P(t_R)$, and

$$P(t_D) = \int_0^\infty P(t_M) \cdot P(t_M - t_D) dt_M \tag{4}$$

The range of T_D is $[-\infty, \infty]$. The probability that T_D is less than zero is:

$$P(t_D < 0) = \int_0^\infty P(t_D) dt_D \tag{5}$$

This is the probability that an MC&A alert occurs and the facility transitions from the "Normal" state to the "Searching for Missing Material" before the insider is successful in moving the material past that physical protection layer.

4.6 Model Development and Analysis

The methods discussed in Section 4.5 will be further developed to be integrated with the Safeguards Performance Model and data authentication activities for a hypothetical UREX+1a

reprocessing facility. To implement these methods, a hypothetical facility and physical protection system design will be developed based on consideration of the existing safeguards performance model as well as data authentication operations. This will allow these new techniques for evaluating the effectiveness of MC&A protection elements to be exercised, evaluated and further developed.

The ATLAS and ASSESS software programs [10, 9], and VA tools, which comprise a systematic approach for evaluating safeguards and security effectiveness against theft or sabotage of nuclear material by different adversaries, will be used to develop the hypothetical facility model and adversary sequence diagram to do a preliminary theft analysis. A set of preliminary material theft scenarios will be defined, for which MC&A activities will be identified as possible "sensors." The elements of the complete theft scenarios will be further evaluated with the application of additional probabilistic risk analysis methods. Additionally, interfaces with process monitoring and measurement data from the safeguards performance model and the data authentication will be defined and integrated to demonstrate how this information can be used to develop and evaluate more effective safeguards systems and improve the overall S&S for a facility.

5.0 Conclusion & Future Work

The integration of data authentication for international safeguards with domestic safeguards will ultimately require two separate MC&A systems. In some cases, joint use equipment may be appropriate, but operational impacts will need to be considered. The additional instrumentation required for international monitoring will add cost, but the costs can be minimized if these considerations are introduced early in the design process. The design of the plant should allow for international inspections and maintenance of equipment to be as un-intrusive as possible on plant operations. Data authentication and encryption technology can be optimized if these needs are assumed at the onset of plant design.

The integration of plant security with safeguards will take advantage of much of the accountability data that it already required. Process monitoring and material accountancy measurements can feed into the MAI for security analyses. However, additional measures such will be incorporated as well. Again, the integration of security with safeguards can save considerable costs if incorporated early in the design process.

Future work on the Safeguards Performance Model will extend the front and back end to include additional measures. One location in the plant model will be chosen to use as a demonstration of the integration of data authentication and security. Additional instrumentation will be added to represent secure, independent measurements for international safeguards. Instrumentation and controls will also be added as appropriate for completing an MAI evaluation for that portion of the plant. This model can then serve as a template for future expansion for full plant integration.

6.0 References

1. B.B. Cipiti, P.E. Rexroth, N.L. Ricker, "Safeguards Performance Modeling of a UREX+1a Reprocessing Plant," SAND2007-6586 (October, 2007).
2. IAEA, "Security Architecture for Unattended and Remote Monitoring Systems," International Atomic Energy Agency, Division of Safeguards, Department of Safeguards Technical Support, Vienna, Austria (2003).
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. M.L. Garcia, "The Design and Evaluation of Physical Protection Systems," Boston: Butterworth-Heinemann (2001).
6. M.L. Garcia, "Vulnerability Assessment of Physical Protection Systems," Boston: Elsevier Butterworth-Heinemann (2005).
7. IAEA, "The Physical Protection of Nuclear Materials and Nuclear Facilities," IAEA-INFCIRC/225/Rev. 4 (Corrected), International Atomic Energy Agency, Vienna, (1999).
8. U.S. Army, *Physical Security*, Report FM 3-19.30, U.S. Department of the Army (2001).
9. ASSESS (Analytic System and Software for Evaluating Safeguards and Security), Version 2.56, Lawrence Livermore National Laboratory, Copyright 1989-2003.
10. ATLAS (Adversary Time-Line Analysis System) software, Version 4.2, Sandia National Laboratories, Copyright 2003-2006.
11. 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).
12. G.D. Wyss, J.L. Darby, P.G. Dawson, K.J. Page, and E.E. Ryder, "Risk-Based Decision Approaches for Safeguards and Security Management," in *TRANSACTIONS*, Vol. 95, pp. 84-85, American Nuclear Society, LaGrange, IL (2006).
13. P.B. Merkle, "Advanced Container Security Device: Adversary Plausible Threat Envelope," SAND2005-5505, Sandia National Laboratories, Albuquerque, NM (2005).
14. P.B. Merkle, "CBRN Weapons and Container Shipping: Adversary Plausible Threat Envelope," SAND2006-0899, Sandia National Laboratories, Albuquerque, NM (2006).
15. P.B. Merkle, "Extended Defense Systems: I. Adversary-Defender Modeling Grammar for Vulnerability Analysis and Threat Assessment," SAND2006-1484, Sandia National Laboratories, Albuquerque, NM (2006).
16. J.L. Darby, "Evaluation of Risk from Acts of Terrorism: The Adversary/Defender Model Using Belief and Fuzzy Sets," SAND2006-5777, Sandia National Laboratories, Albuquerque, NM (2007).
17. J.L. Darby, "Evaluation of Risks from Acts of Terrorism Using Belief and Fuzzy Sets," *Journal of Nuclear Materials Management*, Vol. XXXV, Number 2, p. 19, Instutite of Nuclear Materials Management, Deerfield, IL (2007).
18. J.L. Darby, "Linguistic Belief: A Java Application for Linguistic Evaluation Using Belief, Fuzzy Sets and Approximate Reasoning," SAND 2007-1299, Sandia National Laboratories, Albuquerque, NM (2007).

19. J.L. Darby, "Linguistic Evaluation of Terrorist Scenarios: Example Application," SAND2007-1301, Sandia National Laboratories, Albuquerque, NM (2007).
20. G.D. Wyss, D. Pless, R. Rhea, C.J. Silva, P. Kaplan, R. Aguilar, and S.E. Conrad, "Total Risk Assessment Methodology," not yet published, Sandia National Laboratories (2008).
21. P.G. Dawson and P. Hester, P., "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).
22. F.A. Durán and B.B. Cipiti, B.B. "Material Assurance Indicator for Safeguards Performance Modeling," submitted for The 8th International Conference on Facility Operations – Safeguards Interface, SAND2007-7804A, Sandia National Laboratories, Albuquerque, NM (2007).
23. D.H. Saltiel, G.T. Baldwin, B.B. Cipiti, D.D. Glidewell, P.E. Rexroth, G.E. Rochau, T.A. and K.M. Tolk, "Advanced Process Data Acquisition, Authentication, and Management for Civilian Nuclear Facilities," in *Proceedings of Institute for Nuclear Materials Management 48th Annual Meeting*, Institute of Nuclear Materials Management (2007).
24. F.A. Durán, F.A., P.G. Dawson, and G.D. Wyss, "Probabilistic Basis and Assessment Methodology for Effectiveness of Protecting Nuclear Material," in *TRANSACTIONS*, Vol. 95, pp. 80-81 American Nuclear Society, LaGrange, IL (2006).
25. 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 48th Annual Meeting*, Institute of Nuclear Materials Management (2007).
26. 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).
27. G.D. Wyss and F.A. Durán, "OBEST: The Object-Based Event Scenario Tree Methodology," SAND2001-0828, Sandia National Laboratories, Albuquerque, NM (March 2001).
28. J.L. Darby, J. Phelan, G.B. Varnado, and G.D. Wyss, "A Cyber-Physical Security Assessment Methodology (CPSAM)," in *TRANSACTIONS*, Vol. xx, No. pp. 82-83, American Nuclear Society, LaGrange, IL (2006).
29. F.A. Durán, S.E. Conrad, G.N. Conrad, and P.L. Campbell, "Intrinsic Security for Insider Threats: A Feasibility Study," not yet published, Sandia National Laboratories (2008).
30. PRPP, "Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems," Revision 5, Generation IV International Forum, GIV/PRPPWG/2006/005, <http://www.gen-4.org/Technology/horizontal/PRPPEM.pdf> (2006).
31. R. Bari, P. Peterson, G-L. Fiorini, and T. Leahy, "Integration Efforts and Activities of the Risk and Safety Working Group and the Proliferation Resistance and Physical Protection Experts Group," Generation IV White Paper (2007).
32. Cleary, V., Rochau, G., Vugrin, E., andYork, D., 2007. "Calculating Expected and Observed Risks in an Advanced Transparency Framework," in *Proceedings of Institute for Nuclear Materials Management 48th Annual Meeting*, Institute of Nuclear Materials Management (2007).

33. Mendez, C., Cleary, V., Rochau, G., Vugrin, E., and York, D., 2007. "Utilizing System-Generated Data for Advanced Transparency," in *Proceedings of Institute for Nuclear Materials Management 48th Annual Meeting*, Institute of Nuclear Materials Management (2007).
34. Rochau, G., Cleary, V., and York, D., 2007. "Integration of Safeguards, Security, Operations, and Safety (SSOS)," in *Proceedings of Institute for Nuclear Materials Management 48th Annual Meeting*, Institute of Nuclear Materials Management (2007).
35. Vurgin, E.D., White Vurgin, K.E., Cleary, V., Rochau, G., York, D., and Mendez, C., "A Probability Model for the Calculation of Diversion Risk and Advanced Transparency," in *Proceedings of Institute for Nuclear Materials Management 48th Annual Meeting*, Institute of Nuclear Materials Management (2007).
36. Darby, J.L., Horak, K., LaChance, J.L., Tolk, K., and Whitehead, D., 2007. "Framework for Integrating Safety Operations, Security, and Safeguards in the Design and Operation of Nuclear Facilities," SAND 2007-6429, Sandia National Laboratories, Albuquerque, NM.
37. "South Texas Project Probabilistic Safety Assessment," PLG-0675, Houston Lighting and Power Company, Houston, TX (May 1989).
38. H. A. Bennett, "The EASI Approach to Physical Security Evaluation," SAND76-0500, Sandia National Laboratories, (1977).
39. 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
P.O. Box 1663
Los Alamos, NM 87545

1 Frank Goldner
NE-54/Germantown Building
U.S. Department of Energy
1000 Independence Ave., S.W.
Washington, DC 20585-1290

1	0736	John Kelly, 6770
1	0747	Ken Sorenson, 6774
2	0747	Ben Cipiti, 6774
1	1202	Rebecca Horton, 5640
1	0759	Betty Biringer, 6411
1	0757	John L. Darby, 6414
2	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	1374	Peter Merkle, 6723
1	1371	Keith Tolk, 6720
1	0899	Technical Library, 9536 (1 electronic copy)


Sandia National Laboratories