SAND2009-4737C

A SYSTEMS ENGINEERING PROCESS FOR SAFEGUARDS DESIGN[*]

Felicia A. Durán – Security Systems Analysis
Benjamin B. Cipiti – Advanced Nuclear Fuel Cycle Technologies
Sandia National Laboratories

ABSTRACT

As the world engages in a nuclear renaissance, methodologies are needed to ensure the ability to meet requirements without adding tremendous additional financial burden to new fuel cycle facilities. The objectives of these methodologies are to develop processes, methods, technologies and tools that enable the design, evaluation, and operation of future nuclear facilities that are safe, secure, efficient, cost-effective, and that support the demonstration that these facilities meet all regulatory requirements. This paper presents current work on developing a systems engineering process for safeguards design and evaluation. Different types of fuel cycle facilities will implement various safeguards technologies for nuclear material control and accountability, including measurement equipment, process monitoring, and modeling and analysis tools. The process includes the following steps: define objectives and requirements; develop the design for the safeguards system; evaluate the system design; and iterate the design for optimal effectiveness. The initial basis for the safeguards systems engineering process developed in this work is a similar systems-based process that has been applied for over 25 years for physical protection systems – the Design and Evaluation Process Outline (DEPO). The purpose of the DEPO methodology is to enable the design of an integrated system that performs the physical security system functions to detect, delay and respond to adversary attacks. The initial version of the safeguards systems engineering process follows the pattern of the DEPO methodology, and 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 initial version of the process is described. One of the goals of this process development is to provide a framework within which safeguards technologies, including measurement equipment, and modeling and analysis tools, can be implemented to design and evaluate effective safeguards systems. The strategy of patterning the safeguards process after DEPO would support efforts to integrate safeguards and physical security in the future.

INTRODUCTION

The successful deployment of new fuel cycle facilities requires methodologies to ensure the ability to cost-effectively meet requirements. These methodologies include processes, technologies and tools to demonstrate the design, evaluation, and operation of these facilities meet all regulatory requirements in a safe, secure, efficient and cost-effective manner. This paper discusses the development of a systems engineering process that provides a step-by-step methodology to design and evaluate a safeguards system. The process provides a framework within which safeguards technologies, including measurement equipment, process monitoring,

[*] 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. SAND2009-XXXXC, Unclassified/Unlimited Release.

and modeling and analysis tools, can be implemented to design and evaluate effective safeguards systems.

This paper describes the initial version of the process. Safeguards software tools that have been previously identified are linked to various steps in the process. In some cases, areas have been identified where additional or more robust modeling and analysis capabilities are needed. An example of how portions of this process are being demonstrated and plans for additional integration analyses will also be discussed.

BACKGROUND

The lack of new nuclear reactors or reprocessing plants in the U.S. over the past couple decades has prevented the development of a standardized approach to safeguards design for fuel cycle facilities. As safeguards regulations continue to evolve and the size of fuel cycle facilities increases, it becomes more challenging for new plants to meet requirements. It has become recognized that incorporation of safeguards early in the design process will drastically save costs in the long-term. With the use of nuclear energy increasing worldwide, Safeguards-by-Design[†] is a concept that has evolved in recent years through domestic efforts by the U.S. Department of Energy (DOE) as well as internationally by the International Atomic Energy Agency (IAEA) [IAEA, 2009]. The concept involves consideration throughout all phases of facility design of requirements and design features that address safeguards, as well as safety and security. Other related efforts have focused on identifying software tools that are used by safeguards professionals with the intent to develop a strategy for creating one integrated software tool for safeguards design and analysis [Parker, 2007]. Additionally, recent efforts have identified research and development efforts for advanced instrumentation and integration and control [PNNL, 2009]. These efforts all contribute to developing advanced safeguards systems for future nuclear facilities. A methodology that can be applied to determine the effectiveness of a safeguards system design will support these efforts as well.

Different types of fuel cycle facilities will implement various safeguards technologies, including material measurement equipment, process monitoring, and modeling and analysis tools. A systems engineering process provides a framework within which safeguards technologies can be integrated in a step-by-step approach to design and evaluate effective safeguards systems. The initial basis for the safeguards systems engineering process developed in this work is a similar systems-based methodology that has been applied for over 25 years for physical protection systems – the Design and Evaluation Process Outline (DEPO) [Garcia, 2008; IAEA, 1999]. The purpose of the DEPO methodology is to enable the design of an integrated system that performs the physical security system functions to detect, delay and respond to adversary attacks. The initial version of the safeguards process described here follows the pattern of the DEPO methodology, and 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

[†] INL, 2009, "Institutionalizing Safeguards-by-Design: High-Level Framework, Interim Report, Vols. 1 and 2," INL/EXT-14777, Revision 0, Idaho National Laboratory, Idaho Falls, ID.

measurements. The strategy of patterning the safeguards process after DEPO would support efforts to integrate safeguards and physical security in the future.

The development of the safeguard systems engineering process has also considered existing software tools that can be applied to implement the process. Table 1 provides a summary of previously identified safeguards software tools [Parker, 2007] and others that have been identified in this current effort. These have been linked with certain steps in the systems engineering process.

SYSTEMS ENGINEERING PROCESS

This effort has focused on developing a systems engineering *process* as a first step. This approach provides a framework within which safeguards technologies, including measurement equipment, process monitoring, and modeling and analysis tools (a safeguard analysis toolkit), can be implemented to design and evaluate effective safeguards systems. Development of the process allows for the identification of and integration of important elements of the system. Similarly, the DEPO methodology evolved from collaboration among and integration of physical protection system technologies. The DEPO methodology has continued to be widely used for the design and vulnerability analysis of physical protection systems for DOE and commercial nuclear facilities and is applied using a variety of analysis tools (a physical protection system tool box), for example ASSESS (Analytic System and Software for Evaluating Safeguards and Security) [SNL, 1992] and JCATS (Joint Conflict and Tactical Simulation) [LLNL, 1992]. Additionally, defining a process also allows for consistent application of protection principles to different facilities. Each facility is unique, even if generally performing the similar activities, so a systems engineering approach will allow flexibility in the application of safeguards tools to address local facility conditions.

The elements of the systems engineering process envisioned for safeguards design are shown in Figure 1. It should be noted that this methodology is early in the development phase, and more thorough review by others in the safeguards community will likely lead to changes. The first major step in the design for a plant or facility is to determine the safeguards objectives—this includes regulatory requirements, 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 identifying system elements to perform the detection, delay, and response functions. The final step is to analyze and evaluate the design for various risks. Based on those results, the system design is modified until a final design is agreed upon. The following sections describe each step in the process in more detail.

Determine Safeguards System Objectives

A safeguards system design begins with identifying objectives and goals. A safeguards system is concerned with the material control and accountability and the theft, diversion, and/or misuse of nuclear material. The primary function of a safeguards system typically focuses on detection of material loss or misuse. This step can be complicated by regulatory requirements that may be changing as the nuclear industry worldwide changes. This step addresses four areas: regulatory requirements, facility characterization, threat definition, and target identification.

Table 1: Summary of Safeguards Software Tools

Tool Name	Brief Description	Primary Use
AMUSE[1]	AMUSE is a steady-state model for reprocessing plant separation chemistry. It includes all aspects of the chemistry and tracking of elements and isotopes, although it currently does not include transient response. It also is not set up for evaluating materials accountancy and process monitoring measurements.	Facility/process chemistry simulation/ modeling
FACSIM[2]	Code to model true flows and inventories of all declared nuclear material and to create corresponding text files suitable for other applications.	Facility/process simulation/modeling
GEANT4[2]	A toolkit for the simulation of the passage of particles through matter.	Detector response modeling
LISSAT[2]	A suite of systems analysis tools to determine the probability of successful diversion for various scenarios; determines if IAEA timeliness goals are met and whether additional safeguards measures are needed to achieve these goals.	Safeguards/diversion analysis/risk assessment
NFCSim[2]	NFCSim is an event-driven, fully time dependent simulation code modeling the flow of materials through the nuclear fuel cycle (NFC).	Fuel-cycle/process simulation/modeling
ORIGEN, ORIGEN-ARP[2]	Internationally-used for spent fuel isotopic and radiation source analysis. Tracks time-dependent nuclide concentrations during radiation, decay and fuel reprocessing and calculates the neutron and gamma spectra in any energy group structure.	Burn-up calculations process simulation/ modeling
SEPHIS[1]	SEPHIS is an older model of separations that is able to track separation efficiencies during transients. However, it also does not include materials accountancy.	Separations/process simulation/modeling
SMES – Safeguards Measurement Evaluation System[2]	SMES stores data on assay and isotopic abundance measurements, performs outlier tests, compares the measurement results against the respective characterized values, calculates the bias and precision of the measurements using statistical methods, and prepares evaluation reports and graphs.	Assay/statistical analysis
SOLOMON	A tool for solution monitoring to locate, classify, and reconcile all key tank events.	Solution monitoring/ process simulation/ modeling
SSPM – Separations Safeguards Performance Model[1]	SSPM is an instrumentation model that tracks elements through a reprocessing plant at a high level and simulates accountancy and process monitoring measurements. It can perform mass balances and evaluate diversion scenarios. However, it does not include any modeling of the chemistry currently.	Separations/accountancy process simulation/ modeling
SYNTH – Synthetic Gamma Ray Spectrum Generator[2]	An interactive program to synthesize the results of typical gamma ray spectroscopy experiments/measurements.	Detector response modeling
VPSim[2]	Propagates individual measurement errors to estimate the error standard deviation of the inventory difference using Monte Carlo simulation to model random and systematic measurement error.	Statistical analysis

[1] These software tools were identified as part of this safeguards systems engineering process development.

[2] The information on these software tools was extracted from Parker, 2007, “Inventory of Safeguards Software,” LA-UR-07-6991, Los Alamos National Laboratory, Los Alamos, NM.

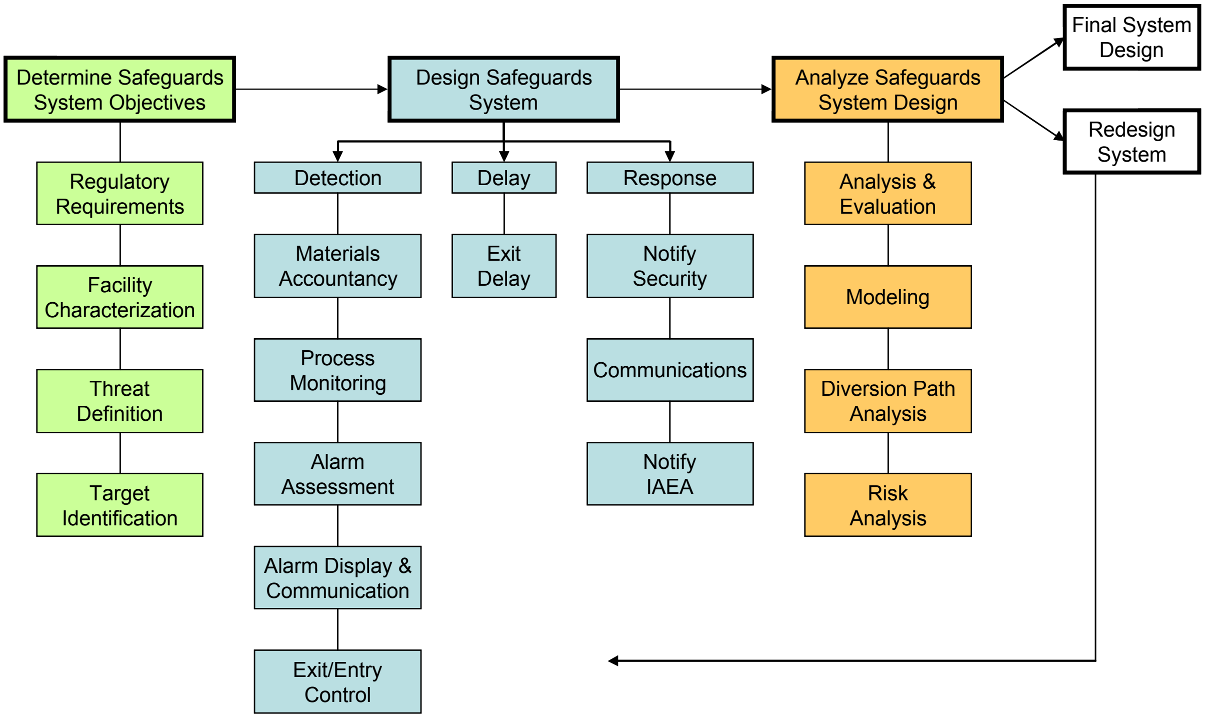

Figure 1: Systems Engineering Process for Safeguards Design

Regulatory Requirements **–** Fuel cycle facilities in the U.S. may have up to three sets of regulatory requirements to be concerned with: DOE, NRC, and IAEA requirements [Durán et al., 2008]. Commercial facilities will most likely need to satisfy NRC requirements for domestic safeguards and IAEA requirements for international safeguards. In the case of a demonstration facility, DOE requirements may be important as well. In addition to specific safeguards requirements, safety requirements, security requirements, and environmental requirements will need to be considered in the design of a safeguards system.

Facility Characterization **–** The facility purpose and general layout will be required to provide the context for more detailed safeguards system design. Different types of fuel cycle operations will have different facilities characteristics, most specifically with regard to process and operations. Characteristics such as schedule and procedures for operations and use of employees, among other should be considered.

Threat Definition **–** The threat definition may be one of the most difficult parts of the design as many different threats exist, and adversary capabilities are constantly evolving. These threats in general are focused on material removal or misuse of material and are examined in diversion scenario analysis. The adversary could be a state or non-state actor. Motivations, knowledge, equipment, training, and the number of adversaries are all factors to consider. In contrast to the DEPO methodology for physical protection, threat definition for safeguards would not include sabotage.

Target Identification – Target identification would involve generating a list of items, flow streams, or process areas to be protected. This list includes location, size, and characteristics of the material. Previous work has proposed the use of material assurance indicators (MAI) which consider these material characteristics as well as when the material is last handled [Dawson and Hester, 2006]. Safeguards software tools that may be used in this step include ORIGEN and CINDER to calculate the source term and SYNTH and GEANT to determine radiation signatures.

Design Safeguards System

Once the facility is characterized, targets and threats are identified, and the regulatory requirements are determined, the initial safeguards design can begin. The safeguards system design focuses on addressing basic system functions. Similar to the DEPO methodology, this initial version of the process identifies safeguards system functions as detection, delay, and response. As part of this step in the process, it is important to identify and characterize the type of safeguards tools and equipment that would be used to perform the required system functions of detection, delay, and response. The need exists to develop performance testing of the types of equipment that could be part of an overall safeguards system design and to use the results of such testing to create a data base of performance metrics for the different type of safeguards equipment. This will be a key effort in advancing the use of this type of systems engineering process.

<u>Detection</u> – Safeguards systems center around materials accountancy and process monitoring measurements. These measurements form the basis for detecting any loss of the material being protected. However, detection also includes alarms, alarm assessment, and communication.

Materials Accountancy – Materials accountancy includes destructive analysis of analytical samples from tanks, item accounting, mass balances, and non-destructive measurements. Depending on the facility, accountancy may have separate systems for domestic safeguards and international verification. In some cases, process monitoring measurements are used in conjunction with analytical samples to calculate mass balances. Safeguards software tools that may be used in this step include: MCNPX for the design of instrumentation and detector response; SSPM for identifying gaps in accountability and virtually testing new concepts; and SMES for evaluating measurements using statistical methods.

Process Monitoring – Increasingly, process monitoring may be used more often for materials accountancy as systems becomes more integrated. Process monitoring measurements include non-nuclear measurements like flow, mass, volume, density, temperature, and cold chemical monitoring. Safeguards software tools that may be used in this step include: SEPHIS, AMUSE, MayTag, and PULCO for separations modeling; SOLMON for solution monitoring; and SPM for evaluating the integration of process monitoring with accountancy.

Alarm Assessment – If a diversion, loss, or misuse of material occurs, it must be reported before any action can be taken. Alarm assessment may include lower limits of detection in the overall mass balance and the detectability of diversion scenarios. If an alarm is triggered, a method must be in place to recognize false positives. Codes that may be used in this step include: SPM for examining diversion scenarios and detectability.

Alarm Display and Communication – The final area of detection is that the alarm must be reported or communicated to the party of interest. Reporting may be to the plant operators or to the IAEA.

Delay – Delay is typically used for the design of physical protection systems, but it also has value here and can play a role in the second step of safeguards design. In addition to more traditional delay measures common in physical security systems, delay can occur because the adversary may need to wait for an opportune facility configuration to complete theft or diversion steps [Durán and Wyss, 2008].

Exit Delay – Safeguards is only concerned with exit delay. The plant can be designed to make it difficult or time-consuming to get material out in the event of a diversion. The goal is to give the plant operators or IAEA enough time to respond if an event is detected.

Response – Response for the design of safeguards systems may be a more limited effort since it can integrate with the physical security system. This is a key area where integration of safeguards and security should be pursued, but may be complicated by the differences between domestic safeguards and international safeguards. The ultimate response may be based on physical security (e.g., arrest the one stealing materials) or on political actions (e.g., United Nations or IAEA sanctions against a state diversion of materials).

Notify Security – If a diversion event occurs and the alarm is assessed to be real, security must be notified. It will be up to the security plan to determine the necessary response force. The threats identified for safeguards should be incorporated in the DEPO process for physical protection to prepare the response force for a number of likely events.

Communications – Communications includes the probability of reporting an alarm to the response force and the time required to report and then act on it. A great deal of interplay may exist between detection, delay, and response to ensure that threats are dealt with while the event can still be stopped.

Notify IAEA – International safeguards includes response to IAEA. In this case the international response will be much different, and may require additional inspections or international support to stop operations. This response will depend to a large degree on international agreements in place.

Analyze Safeguards System Design

The final step of the process is to analyze the design and then go back to make changes as needed until the design meets the desired performance objectives. A uniform set of models or tools could provide the most benefit to this part of the process; many of the current models are dated, too narrow-focused, or need additional development. Consolidation of existing codes could be considered to create much more robust tools for the design and evaluation of the system.

Analysis and Evaluation - The purpose of analyzing and testing is to determine how effective the components work together to address the identified threats. Again, this determination would be based on performance data developed for different safeguards equipment. These analyses are done on a plant-wide basis since diversion pathways must cross the plant boundary.

Modeling – Modeling includes accountancy, process monitoring, diversion scenarios, and detectability of events. Tools do currently exist, but all have limitations that may be addressed by combining or consolidating capabilities into one uniform tool. Safeguards software tools that may be used in this step include SEPHIS and AMUSE for separations modeling; SSPM, SMES, and VPSim for evaluating accountancy and process monitoring design; and NFCSim and FacSim for fuel cycle and plant simulation.

Diversion Path Analysis – An infinite number of diversion scenarios are possible, but only a small number may be probable. Diversion path analysis is a difficult step because it depends somewhat on the imagination of those involved in the design. Part of this analysis includes probability of occurrence and response of the systems. Safeguards software tools that may be used in this step include LISSAT and SPM for modeling various diversion events.

Risk Analysis – Analysis of security risk is also considered for physical protection, but risk for safeguards is not as well defined. Past work has examined the used of risk metrics to provide a measure of effectiveness for the system [Durán and Wyss, 2008; Darby et al., 2006; Wyss et al., 2008]. The Generation IV International Forum has developed the proliferation resistance and physical protection methodology that may apply [PRPP, 2006]. A probability model for the calculation of diversion risk and advanced transparency has been generated for monitoring reactor facilities [Cleary et al., 2008]. All of this past work could be incorporated into this area, but it is clearly an area that requires more work and integration.

MODEL CONSOLIDATION

Many of the steps in the safeguards systems engineering process do not require or include software tools. In many areas the software tools listed are models that can be used to support the design or evaluation activity. Proper engineering design does not rely completely on models, but rather uses people to make sure the design meets the desired objectives. Models are simply tools to make the work more tractable, efficient, and cost-effective. One over-arching model to cover the entire process may not be recommended, and even if possible, would likely require a tremendous amount of investment to accomplish. We expect that within this framework, additional tools may be identified or developed, then integrated for implementing process steps.

In this effort, we have focused on one area in the process that could benefit from model consolidation. In this case, the analysis and evaluation step has a number of disparate software tools that have the potential to come together to form a more useful tool. Integration of these tools would be a modest and achievable effort, and the final product could still be a simple tool that could run on a desktop computer. Specific software tools that could be combined include the following: AMUSE, SEPHIS, SSPM, FACSIM, LISSAT and SMES. These codes bring different capabilities to the table, and others may be identified in this project that could be important to include, but no one alone can accomplish the full job of safeguards system design and evaluation. As a first step, it would be useful to consolidate some of these codes and models into one tool for evaluating safeguards system effectiveness.

Oak Ridge National Laboratory (ORNL) and SNL have proposed plans to incorporate the SEPHIS model into the SSPM model [Cipiti et al., 2008] to generate a more robust tool. The SSPM integrates material accountancy and process monitoring; SEPHIS would add separations chemistry. In related work, a methodology that incorporates material control and accountability functions within a physical protection system is being investigated as an approach for integrating safeguards and security, and has demonstrated promising performance improvements [Durán and Wyss, 2008]. Integration of these models and methodologies can be tested and demonstrated, and if successful, could provide a platform for integrating other models and methodologies to develop a more robust reprocessing plant safeguards model for determining system effectiveness.

In the longer term, codes like ORIGEN or CINDER could be integrated to increase the accuracy of elemental and isotopic tracking. As a first step, these codes can be used to generate a library of different source terms. Later, direct code coupling could be evaluated to track the decay of material in the plant in time and the effect of mixing re-work streams with new fuel. Codes like MCNPX could be considered for modeling detector geometry. SYNTH or GEANT could integrated to include gamma spectra of the various streams. But this longer term integration would be much more time intensive and would require more analysis to determine potential benefits.

CONCLUSION

The design of safeguards systems requires a more formal methodology to support significant expansion of nuclear energy. A systems engineering process can provide a framework within which different technologies can be implemented to design and evaluate effective safeguards systems. Implementing such a process early in the design process can save costs in the design, construction, and operation of a facility. Modeling tools play an important role at certain steps in the process, and many existing safeguards software tools can be applied to implement the process. Consolidation of these tools for analysis and evaluation of safeguards systems is desirable, but this effort should be focused to demonstrate integration to achieve process implementation for a moderate cost and in a reasonable amount of time.

We have developed an initial version of a systems engineering process to provide a framework for the design and evaluation of effective safeguards systems. Within this framework, we are working to consolidate existing safeguards software tools and other methodologies to develop and demonstrate a more robust tool for safeguards modeling and analysis.

ACKNOWLEDGEMENTS

This work was performed as part of the U.S. DOE Office of Nonproliferation and International Security, International Cooperation Program (NA-242) Safeguards Modeling and Simulations Expert Group.

REFERENCES

Cipiti, B.B., and Ricker, N.L., 2008. "Advancing the State of the Art in Materials Accountancy through Safeguards Performance Modeling," SAND2008-5100, Sandia National Laboratories, Albuquerque, NM.

Cleary, V.D., Inoue, N., Irie, T., Katsumura, S., Kitabata, T., McFadden, K., Mendez, C.M., Rochau, G.E., and Suzuki, M., 2008, "Advanced Transparency Framework Phase II Report: Demonstration and Proof-of-Concept," Sandia National Laboratories, Albuquerque, NM.

Darby, J., J. Phelan, G.B. Varnado, and G. Wyss, 2006. "Cyber-Physical Security Assessment Methodology (CPSAM)," in *TRANSACTIONS*, Vol. 95, pp. 82-83, American Nuclear Society, LaGrange Park, IL.

Dawson, P.G., and P. Hester, 2006. "Real-Time Effectiveness Approach to Protecting Nuclear Materials," in *Proceedings of the Institute for Nuclear Materials Management 47th Annual Meeting*, Institute for Nuclear Materials Management, Deerfield, IL.

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

Durán, F.A., Sorenson, K., Yoshimura, R., McConnell P., Cochran, J.R., Walker, S.A., Silva, C.J., Badwan, F.M., Ireland, J., Dallman, J., McConnell, S., Geddes, R., McMullin, C., Cappucci, A., and Jones, D., 2008. "Consolidated Fuel Treatment Center Regulatory Framework Assessment, Rev. 1," GNEP-CFTC-SAFH-MI-DV-2008-000287, Advance Fuel Cycle Initiative, U.S. Department of Energy, Washington, DC.

Garcia, M. L., 2008. *The Design and Evaluation of Physical Protection Systems*, Second Edition, Boston: Butterworth-Heinemann.

IAEA, 1999. "The Physical Protection of Nuclear Materials and Nuclear Facilities," IAEA-INFCIRC/225/Rev. 4 (Corrected), International Atomic Energy Agency, Vienna.

IAEA, 2009. "Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards," SGCP-CCA, Report #STR-360, International Atomic Energy Agency, Vienna.

LLNL, 1992. "JCATS Algorithm User's Guide," UCRL-SM-213123, Lawrence Livermore National Laboratory, Livermore, CA.

Parker, Robert, 2007. "Inventory of Safeguards Software," LA-UR-07-6991, Los Alamos National Laboratory, Los Alamos, NM.

PNNL, 2008. "AFCI Safeguards Enhancement Study: Technology Development Roadmap," PNNL-18099, Pacific Northwest National Laboratory, Richland, WA.

PRPP, 2006. "Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems," Revision 5, GIV/PRPPWG/2006/005, Generation IV International Forum.

SNL, 1992. "Analytic System and Software for Evaluating Safeguards and Security - User's Manual," Sandia National Laboratories, Albuquerque, NM.

Wyss, G., Pless, D., Rhea, R., Silva, C., Kaplan, P., Aguilar, R., and Conrad, S., 2009. "Total Risk Assessment Methodology," SAND2009-0178, Sandia National Laboratories, Albuquerque, NM.