SAND2011-4093C

Security for Long-Term Storage of Used Nuclear Fuel[1]

by

Felicia A. Durán and Gregory D. Wyss
Sandia National Laboratories

James Blink
Lawrence Livermore National Laboratory

ABSTRACT

Given the uncertain future of the proposed Yucca Mountain Repository for final disposal of used light water reactor fuel, the need to store these fuels past their current regulatory certification periods has become clear. This situation presents possible regulatory and technical issues with regard to both storage safety and security. The U.S Department of Energy (DOE), Office of Nuclear Energy (NE) is engaged in a program to develop the technical bases for extending dry storage and subsequent transportation of used nuclear fuel. The DOE/NE program addressing this issue is divided into four main topical areas: Research and Development (R&D) Opportunities, Security, Transportation, and Concept Evaluations. Previous work focused on a regulatory assessment of security regulations, including those from the U.S. Nuclear Regulatory Commission and the DOE. In addition, it has been determined that the dose rates for commercial used fuel will fall below the current 100 rem/hour self-protection threshold after between 70 and 120 years of storage. Work continues on developing the technical basis for maintaining security for long-term storage of used fuel, including consideration of "barriers" characteristic of used fuel in addition to the radiation hazard that is the basis for the existing self-protection. These additional barriers relate to technical difficulty and detectability of attacks, technical difficulty of separations processes, and thermal/chemical/nuclear signatures considered in the National Academy of Sciences Spent Fuel Standard for Disposition of Excess Weapon Plutonium. In addition, figures of merit for material attractiveness over the long-term are being evaluated. Security assessments are being performed for orphan storage sites, existing operating storage sites, and possible consolidated storage concepts.

INTRODUCTION

Given the uncertain future of the proposed Yucca Mountain Repository for final disposal of used light water reactor (LWR) fuel, the tactical strategy is to store used nuclear fuel (UNF) at the utility sites in either pool or dry cask storage systems. This does present possible regulatory and technical issues with regard to both storage safety and security. This paper discusses work in progress to address UNF storage security for long-term storage. Previous work [1, 2] focused on a regulatory assessment of applicable security requirements, including regulations for the U.S. Nuclear Regulatory Commission (NRC) and directives for the U.S. Department of Energy (DOE). In addition, it has been determined that the dose rates for commercial UNF will fall below the current 100 rem/hour self-protection threshold after about 70 to 120 years.

---

[1] Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Company, for the U.S. Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000. Approved for unclassified/unlimited release.

This work is part of a larger effort to develop concepts for the implementation of a demonstration UNF storage site and to develop a technical basis for long-term storage of UNF and the associated transportation. Work continues to address issues associated with developing the technical basis for maintaining security for long-term storage of UNF. As described in the following sections, this includes consideration of other factors to extend the existing self-protection concept and assessments to evaluate the relative security risk over the long-term of different UNF storage configurations.

SELF-PROTECTION CONCEPT

Security requirements for UNF are determined in part by a determination that it is self-protecting. Within the NRC regulations in 10 CFR 73, self-protection is attributed to special nuclear material "which is not readily separable from other radioactive material and which has a total external radiation dose rate in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding." Revisiting the concept of self-protection and considering the evolution of adversary attacks will provide a basis for determining threats that should be addressed and protection strategies that should be recommended within the context of long-term storage security. In this section, the current basis for self-protection is discussed as well as additional "barriers" characteristic of UNF that are being considered to extend the concept of self-protection for long-term storage security.

Current Self-Protection Basis

LWR UNF is considered self-protecting because its large size, high thermal heat, and radioactivity make it extremely dangerous to handle. Because of self-protection, commercial UNF is not considered an attractive theft or diversion target in the NRC design basis threat [3]. The radioactivity of UNF, and therefore, its self-protection decreases over time. Previous work for this project [1, 2] extended dose rate calculations for 50 years out to 200 years and determined that for low burn-up fuels (20-35 MWd/kg), the dose rate falls below the existing 100 rem/hr threshold in approximately 70 to 120 years. This timeframe would be longer for higher burn-up fuels.

Other work has looked at the effects of exposure to radiation from UNF on potential adversaries [4]. The current dose rate for self-protection has been determined not to be immediately incapacitating; a much higher dose rate would be required to incapacitate an adversary within minutes. In addition, discussions about raising the dose rate for self-protection are ongoing. If the threshold dose rate is increased, then the self-protection of UNF will fall below the higher threshold at an even earlier time during storage.

Material Attractiveness

Material attractiveness is a categorization of nuclear material (type and composition) that reflects the relative ease of processing and handling required to convert that material into a nuclear explosive device. It is a metric that describes the weapons utility of processed (transformed) nuclear material, for safeguards and security purposes, in an unclassified environment. For the purposes of evaluating the proliferation resistance and physical protection requirements for nuclear fuel cycle options, a simple formula has been developed to estimate the weapons usability of special nuclear material [5 -8]. The formula is a figure of merit (FOM) that considers material quantity, heat content, and dose rate. As shown in Equation 1, the FOM is defined as

$$FOM = 1 - \log_{10}\left(\frac{M}{800} + \frac{M \bullet h}{4500} + \frac{N}{10}\left[\frac{D}{500}\right]^{\frac{1}{\log_{10} 2}}\right) \quad (1)$$

The FOM is an empirically derived formula that uses two physical parameters associated with the *product* material that is to be weaponized, i.e., the metal alloy produced in the transformation *stage* that is the starting point for the fabrication *stage*. These two parameters are the bare critical mass, M, in kg and the heat content, h, in W/kg. The third parameter in the equation is the dose rate, D, in rad/h; it could be calculated for the material *before or after transformation*, depending on what *stage* of the *proliferation pathway* is being evaluated. The term with the dose rate also includes the net weight of the item, N, in kg. The net weight for the theft *stage* would be the spent fuel assembly weight; whereas, the net weight for the fabrication *stage* is the weight of the component being handled.

The values of the constants and exponents in the FOM are designed to produce a range nominally between zero and three. FOM values less than 1.0 represent materials that are impractical for weapons utility (low or very low *Materials Attractiveness*, and *Attractiveness Levels D or E* from the DOE manual [9]). FOM values greater than 2.0 represent materials preferred for nuclear explosive fabrication (high *Materials Attractiveness*, and *Attractiveness Level B* from DOE [9]). Intermediate values between 1.0 and 2.0 are potentially usable (medium *Materials Attractiveness*, and *Attractiveness Level C* from DOE [9]).

The argument of the logarithm of the FOM is the overall *complexity* of the material. Lower *complexity* increases the FOM due to the negative sign on the logarithm, and use of a logarithm converts large differences into a more comprehensible and manageable scale. The constant term from which the logarithm is subtracted is set to 1.0 so that the FOM is 1.0 when the material *complexity* is 1.0.

The first argument of the *complexity* is the *size factor*. It is based on M, the bare critical mass of the transformed material that is required to build a nuclear explosive. In general, as M increases, the required amount of source material increases. It becomes impractical to build the device when M becomes very large. The reference point for this impracticality has historically been set at 20% ^{235}U enrichment, which has a bare critical mass of about 800 kg. At the reference point, the *size factor* is 1.0 (leading to a zero logarithm and an FOM of 1.0 for that M when the other terms are ignored). An M of 80 kg (10 times lower) would lead to an FOM of 2.0 when the other terms are ignored.

The second argument of the *complexity* is the *stability factor*. It is based on M and the heat content, h, in W/kg. The constant of 4500 W is based on radioisotope thermal generators (RTG), which use the decay heat of ^{238}Pu. An 80%:20% mixture of ^{238}Pu:^{239}Pu has M = 9.6 kg and h = 412 W/kg. At these values, the *stability factor* is 1.0, resulting in an FOM value of 1.0 for that heat content when the other terms are ignored. An 8%:92% mixture of ^{238}Pu:^{239}Pu has M = 10 kg and h = 43 W/kg (a *stability factor* 10 times lower), resulting in an FOM of 2.0 when the other terms are ignored.

The third argument of the *complexity* is the *acquisition factor*. It is based on the acute dose rate, D, in rad/h. The dose rate used to evaluate the FOM should be consistent with the material at the *stage* of the *proliferation pathway* being considered. For the fabrication *stage*, it is the product material, whereas for the theft *stage* for an orphaned surface storage site, it is the spent nuclear fuel assembly. The dose rate is that at 1 m from the material, with no intervening shielding. The constant of 500 rad/hr is equivalent to 5000 rad/hr at a more realistic working distance of 30 cm for the fabrication *stage*. (For the theft *stage* in an orphaned surface storage site, we may need to change the constant to a higher value based on working with heavy equipment and being farther away from the material.) Nominally, 5000 rad results in 100% incapacitation within one hour and 50% incapacitation within 30 minutes. For D = 500 rad/hr, the dose rate multiplicative contribution to the *acquisition factor* is 1.0, resulting in an FOM value of 1.0 when the other terms are ignored. The exponent is designed to change the dose rate contribution by 10x (or the single-term FOM by 1.0) when the dose rate changes by 2 times. For example, a dose rate of 250 rad/hr results in a single-term FOM of 2.0.

The *acquisition factor* is modified to account for the net weight, N, of the item in kg. The heavier or larger the item, the more difficult it is to steal or divert. A 10x change in net weight results in a change in FOM by one unit. For example, the single-term FOM is zero in the fabrication stage for a net weight of 100 kg and a dose rate of 500 rad/h. If the item is very small, or the net weight is not known, one can evaluate Equation 1 using N = M/5. A net weight constant of 10 kg is appropriate for the fabrication *stage*, but we may need to change the reference values of both the dose rate and the net weight for the theft *stage* at an orphaned surface storage site.

Material Attractiveness for Used Fuel Self-protection

Nuclear weapons experts at both Los Alamos National Laboratory and Lawrence Livermore National Laboratory reviewed the FOM. While it was determined that there are a number of smaller factors that are not captured, it was agreed that the FOM adequately captures the dominant factors in an unclassified format.

The FOM represents an important part of the overall proliferation and security risks that are posed by various materials and processes in the nuclear fuel cycle. To contextualize the FOM, it overlaps strongly with one of the six proliferation resistance measures (Fissile Material Type) identified in the Proliferation Resistance and Physical Protection (PR&PP) methodology [10], and it overlaps strongly with the material attractiveness criteria which are a key part of the DOE graded safeguards table [9]. Therefore, in the case of proliferation resistance, five other factors need to be considered (technical difficulty, cost, time, detection probability, and detection resource efficiency). In the case of physical protection, there are two other factors that need to be considered (material quantity and security category).

The material attractiveness FOM can be modified for the particular situation of a UNF storage facility, for each of three potential *adversary objectives* (*on-site radionuclide dispersion*, theft of material for *later radionuclide dispersion*, and theft of material for *later processing and fabrication into a nuclear explosive*). For example, King [7] aggregates the FOM in the nuclear explosives fabrication *stage* with the number of significant quantities (SQs) of material available for theft in the two nuclear systems he compared (a fusion-fission hybrid system deep-burning plutonium in the subcritical blanket and a pressurized water reactor (PWR) burning mixed oxide fuel. King multiplies the FOM by a function that has a value of 1.0 for SQs above about 1.5 and that has a value of 0.0 for SQs below about 0.5. This enabled the King study to show that, after seven years of deep-burn irradiation time, the fusion-fission system is impractical to an adversary seeking to divert material for *later processing and fabrication into a nuclear explosive*.

The FOM can provide a measure of how material attractiveness changes over the period of long-term storage of UNF. Bathke's FOM calculations for hypothetical theft of commercial PWR used fuel indicate PWR assemblies (30, 45, and 60 MWD/kg burn-ups) become attractive (FOM >1) 95-125 years after discharge, and highly attractive (FOM >2) 125-170 years after discharge [8]. The development of a modified FOM for the particular situation of a UNF surface storage facility will consider potential adversary objectives, difficulty of attack, and other characteristics of the storage system evaluate how material attractiveness will change over the timeframe of long-term storage.

Spent Fuel Standard

In addition to the radiation hazard, additional "barriers" characteristic of UNF are being considered as a possible basis for extending the current self-protection concept. These characteristics are part of the spent fuel standard described by the NAS in its study of options for achieving long-term disposition of the excess plutonium from nuclear weapon dismantlement. The NAS describes the spent fuel standard as a basis for disposition options that "make plutonium roughly as inaccessible for weapons use as the much larger and growing quantity of plutonium that exists in spent fuel from commercial reactors" [11]. The spent fuel standard is defined by three characteristics that include radiological properties (the basis for current self-protection) along with physical properties and chemical properties, that influence security requirements [12]. The physical properties address the large, bulky size of UNF assemblies and storage casks that can facilitate material accounting and theft detection as well as present a significant challenge to an adversary attempting theft of the material. The chemical properties address the extent of processing required to convert nuclear materials to a nuclear explosive device – also considered as an element of material attractiveness, along with material form, radiation barriers, ease of separation, and ease of use in a nuclear device.

Revisiting Self-Protection for Long-Term Storage

Revisiting the self-protection of UNF for long-term storage raises several significant questions. What are the quantities of UNF that will fall below the different self-protection thresholds and at what points in time does this occur? Is UNF a credible theft target over the period of long-term storage? Are different protection strategies required, and if so, what are they?

Current efforts on this project are working to address these issues. The DOE-RW-859 data base includes assembly-specific information for discharged commercial fuel assemblies through 2002 with projections through 2014. An assessment of the data base information will be conducted to determine the self-protection status of the fuel inventory for the purposes of informing the storage security activities and evaluating implications of changes to the self-protection threshold. The current self-protection basis, the FOM for material attractiveness, and spent fuel standard overlap some in their consideration of factors for security of long-term storage of UNF. All three consider the radiological hazard. The current self-protection basis considers the chemical properties (not readily separable) and, implicitly, the physical size and of UNF. The spent fuel standard addresses the material processing aspect of material attractiveness, where as the FOM does not. Work will continue to address these issues to evaluate how they might change over the timeframe of long-term storage and to support a more comprehensive technical basis that considers all these factors and that can serve as a basis to develop recommended protection strategies for long-term storage security.

SECURITY ASSESSMENT FOR LONG-TERM STORAGE

Any assessment of security over a very long timeframe is a challenge. For this effort, a risk/cost benefit methodology [13] is being implemented to evaluate the security risk of UNF storage configurations relative to other possible targets. Rather than using a traditional security assessment method that relies on a highly uncertain probability of attack, the risk/cost benefit method uses approaches to describe the difficulty for an adversary to successfully plan and execute an attack that can produce a desired level of consequences. Having the basis to compare the security risk of UNF storage sites relative to other possible targets enables recommendations for appropriate protection strategies at these sites commensurate with the security risk. Protection strategies then can be developed to either increase an adversary's difficulty of attack or reduce potential consequences, or both.

This method for security risk assessment hinges on developing a metric for simply characterizing targets in terms of the overall difficulty for the generalized set of disparate potential adversaries to conduct successful attacks. While it is easy for an analyst to describe the difficulties inherent in a specific attack scenario, these difficulties are hard to express as a single metric – either qualitative or quantitative – because of the large number of disparate factors that may cause difficulty to an attacker. The following sections describe a system of metrics designed to describe and summarize the levels of difficulty that adversaries would face in successfully executing attack scenarios.

General Characteristics of the Proposed Method

The proposed approach starts by identifying a scenario that would offer an adversary a reasonable expectation of success[2] against the target(s) under consideration, i.e., a scenario for which the conditional likelihood that the attack by this threat will be successful exceeds a threshold established for this purpose. Such scenarios can be developed by any number of currently available means that are commonly used by the security analysis and vulnerability assessment community. Specific to each scenario, either explicitly or implicitly, are the resources (personnel, materiel, and knowledge) that an adversary would need to have, and the manner in which they would need to be employed, in order for the adversary to have a reasonable likelihood of success when executing the scenario against the target(s) under consideration.

Considerations of the difficulty for an adversary to mount this scenario are partitioned into the two essential phases of adversary efforts for any attack scenario - Preparation and Execution. Since adversary success in the scenario requires successful completion of both phases, they are viewed with comparable significance. The primary factors that are generally key to adversary success in each phase of attack have been identified through discussions with subject matter experts, review of various ranking schemes for adversaries or threats or scenarios, and analysis of a diverse set of specific scenarios. Since a metric is required that characterizes the relative difficulty of successfully (inducing and) exploiting target vulnerabilities, scenario success factors are expressed in terms of their manifestation at the interface between target and threat. For example, while level of funding can be important to adversary success, this is manifested at the target in other factors, such as quality and size of the toolkit used in the scenario. These factors have developed so that they can be considered as roughly independent dimensions of generally equivalent importance.

---

[2] For most attack scenarios, "success" means inducing a specific consequence of the adversary's choosing from the target.

In addition to reflecting key factors for scenario success, the required metric must also reflect the relative level of difficulty for adversaries to be successful in the scenario against the target(s) under consideration. To do this, five discrete levels of difficulty have been defined for each success factor dimension. Guidelines are being developed for analysts to consistently assign the appropriate levels to each success factor dimension in order to reflect the relative difficulty that an adversary would encounter to successfully achieve or acquire the characteristics required in that dimension for the scenario to succeed. It is important to note that this process does not assign adversaries to a particular level, nor imply that all dimensions of a scenario are at the same level. Rather, the process dissects a successful scenario into the minimum levels of difficulty associated with each of the key factors that generally underlie adversary success. Since the scenario is specific to the target(s) under consideration, this process characterizes targets in terms of the levels of adversary difficulty to recognize, induce, and exploit vulnerabilities that enable scenario success.

The levels of difficulty for the dimensions have been calibrated so that a particular level for one dimension roughly correlates to an equivalent level of difficulty for any other dimension. In general, the levels of difficulty correlate with the size of the portion of the spectrum of generalized potential adversaries that could reasonably expect to achieve or acquire the associated level characteristics. Level 1 characteristics are easily accessible or achievable by the general population, while Level 5 characteristics would typically be accessible or achievable only by elite forces or state-supported operations. Different levels of difficulty are distinguished by different levels of costs, quality of leadership, law enforcement or intelligence signatures, time to achieve, availability, ingenuity, and/or sophistication.

Dimensions of Success for Attack Preparation

The dominant challenges for adversaries in the Preparation phase of efforts are in developing, acquiring, and preparing the resources – personnel, materiel, and knowledge – required for the scenario without being detected or interdicted by authorities. The dominant resource attributes that are keys to scenario success, and the primary considerations that differentiate levels of difficulty for the adversary to succeed, are:

- *Active Outsiders: # of Fully Engaged Participants* reflects the difficulty an adversary faces to successfully muster and prepare team(s) without alerting authorities, which increases with the number of participants.
- *Active Outsiders: Training & Expertise of Fully Engaged Participants* reflects the depth and diversity of expertise required of participants, and by the rehearsal required for tasks.
- *Support Structure: Size, Complexity, and Commitment* reflects the contributions required of a support base during attack preparation, e.g., intelligence, safe haven, training or staging facilities, finances, scientific or technological R&D, and manufacturing. Difficulty varies with the extent, diversity, and quality of contributions required, and the degree of engagement and awareness of purpose for these contributions.
- *Tools: Availability* reflects the difficulty associated with acquiring the tools required to successfully execute a scenario. Tools can include weapons, transportation, breaching equipment, electronics, fixtures, armor, disguise, etc. The levels of difficulty are distinguished by factors that influence their availability: rarity, law enforcement / intelligence signatures associated with their acquisition or staging, and level of controls in place to protect against illicit usage.

- *Insiders: # of Contributors* is one of three dimensions (key factors for adversary success) associated with contributions from insiders. Difficulty varies with the necessity for insider contributions, the number of contributors required, and the necessity of collaboration among multiple insiders.
- *Insiders: Security Controls on Contributors* reflects how contributions required from insiders that have greater levels of access to security-sensitive features are generally more difficult for adversaries to confidently acquire due to the security controls in place to mitigate the potential for such occurrences.

Dimensions of Success for Attack Execution

The manner in which adversaries employ their resources during attack execution can also be critically important to their ability to succeed. The dominant success factor dimensions for attack execution, and the primary considerations that differentiate levels of difficulty for the adversary to succeed, are:

- *Ingenuity / Inventiveness* reflects the degree to which an adversary must be creative or ingenious in order to discover and/or induce, and exploit the vulnerabilities required for a successful attack. Low levels are associated with simple, straightforward attacks that can be conceived easily by most adversaries, while high levels are associated with attacks that reflect unique, imaginative approaches that are more likely to surprise and befuddle even very well prepared defenses.
- *Situational Understanding & Exploitation* reflects the level of acuity required by the adversary to recognize the occurrence of exploitable conditions and the flexibility required to leverage those opportunities. Levels of difficulty are differentiated by the transience, unpredictability and observability of vulnerabilities upon which success of the scenario depends.
- *Stealth & Covertness* reflects the degree to which scenario success depends upon the concealment or masking of attack execution activities in order to delay the point of initial detection and recognition by authorities. Levels of difficulty are differentiated by the existence, duration and multiplicity of undetected adversary operations that must be conducted within the observational purview of authorities.
- *Outsiders: Dedication / Persistence / Commitmen*t reflects the significance of consequences at risk for the attackers, their support base, and/or their cause, the persistence of their risk exposure, and the degree of adversary certainty of those consequences.
- *Insiders: Degree of Engagement & Risk* reflects the equivalent significance, persistence, and certainty of risk exposure required of insiders contributing to the attack.
- *Operational Composition / Complexity* accounts for the required number, modalities, and orchestration of separate avenues of adversary attack execution operations. Modalities refer to the nature of vulnerabilities and exploitation operations required for the scenario: e.g., physical, cyber, procedural, etc.

Implementation for Used Fuel Storage Security

The security team for this effort has implemented the risk/cost benefit methodology for a preliminary assessment of UNF storage security. The following steps were used in the implementation:

1. Identify consequences of concern
2. Identify attack scenarios for each consequence
3. Develop a description of the scenario and what the adversary will require for success
4. Develop preliminary difficulty scores
5. Develop strategies to estimate consequences

Several baseline scenarios were developed for a radiological sabotage threat under current day conditions at a generic “orphan site” – an independent spent fuel storage installation (ISFSI) licensed under 10 CFR 72 where reactor operations have ceased and only dry cask storage occurs with no additional casks to be stored. These baseline scenarios were scored with respect to difficulty of attack preparation and execution. Further assessments have considered factors (characteristics of the fuel, including self-protection, attractiveness; and characteristics of the attack scenario) that would change the baseline scenario at a future time. Additional assessments will be performed for other ISFSI configurations including existing operating storage sites and possible consolidated storage concepts, as well as for transportation scenarios.

CONCLUSIONS

This paper has described work in progress to address issues associated with developing the technical basis for maintaining security for long-term storage of UNF. The expected outcome of this work is an evaluation of the security risk of UNF storage configurations relative to other possible targets and the development of a basis to identify possible protection strategies for different long-term storage concepts, including recommendations for security design features and operational activities for long-term monitoring and institutional control. This work will evaluate the security risk of used fuel storage configurations and transportation relative to other possible targets and provide the basis to identify possible protection strategies for different long-term storage concepts, including recommendations for security design features and operational activities for long-term monitoring and institutional control.

ACKNOWLEDGMENTS

This work is being performed for the DOE Office of Nuclear Energy Fuel Cycle Technologies Program by a team from several DOE National Laboratories, including Pacific Northwest National Laboratory, Idaho National Laboratory, Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, Sandia National Laboratories, and Savannah River National Laboratory.

Sandia National Laboratories is a multi-program laboratory managed operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Company, for the U.S. Department of Energy’s National Nuclear Security Administration under Contract DE-AC04-94AL85000. Approved for unclassified/unlimited release.

REFERENCES

1. F. A. Durán, A. G. Garrett, and S. L. Garrett, “Used Fuel Storage Security – Final 2010 Report,” prepared for the U.S. Department of Energy, Fuel Cycle Technologies Used Fuel Disposition Campaign (2010).
2. F. A. Durán, A. G. Garrett, and S. L. Garrett, “Used Fuel Storage Security,” in *Proc. of the Institute of Nuclear Materials Management 51st Annual Meeting*, Baltimore, Maryland, July 11-15, 2010, Institute of Nuclear Materials Management (2010) (CD-ROM).

3. U.S. Nuclear Regulatory Commission, "Final Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements," SECY-06-0219, U.S. Nuclear Regulatory Commission (2006).
4. C. W. Coates, B.L. Broadhead, A.M. Krichinsky, R.W. Leggett, M.B. Emmett, and J.B. Hines, "Radiation Effects on Personnel Capability and a Summary of Dose Levels for Spent Research Reactor Fuels," ORNL/TM-2005/261, Oak Ridge National Laboratory (2005).
5. C. G. Bathke, R. K. Wallace, J. R. Ireland, M. W. Johnson, K. R. Hase, G. D. Jarvinen, B. B. Ebbinghaus, B. W. Sleaford, B. A. Collins, M. Robel, K. S. Smith, A. W. Prichard, and B. W. Smith, "An Assessment of Attractiveness of Material Associated with a MOX Fuel Cycle from a Safeguards Perspective," in *Proc. of the Institute of Nuclear Materials Management 50th Annual Meeting*, Tucson, Arizona, July 12-16, 2009, Institute of Nuclear Materials Management (2009) (CD-ROM).
6. Sleaford, B. W., B. A. Collins, B. B. Egginghaus, C. G. Bathke, A. W. Prichard, R. K. Wallace, B. W. Smith, K. R. Hase, K. S. Bradley, M. Robel, G. D. Jarvinen, J. R. Ireland, and M.W. Johnson, "Nuclear Material Attractiveness: An Assessment of Material from PWHR's in a Closed Thorium Fuel Cycle," *ENC 2010*, Barcelona, Spain (2010).
7. King, W. E., "The Application of a Figure of Merit for Nuclear Explosive Utility as a Metric for Material Attractiveness in a Nuclear Material Theft Scenario," *Nuclear Engineering and Design*, 240, pp. 3699-3707 (2010).
8. C. G. Bathke, P. G Edelmann, B. B. Ebbinghaus, B. W. Sleaford, B. A. Collins, K. R. Hase, M. Robel, A. W. Prichard, and B. W. Smith, "Nuclear Material Attractiveness: An Assessment of Used-Fuel Assemblies," presented at The 13th International High Level Radioactive Waste Management Conference, Albuquerque NM, April 10-14 (2010).
9. U.S. Department of Energy, 2006. "Material Control and Accountability," DOE M 470.4-6, Chg 1, U.S. Department of Energy, Washington DC (2006).
10. U.S. Department of Energy, "Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, Revision 5," November 30, 2006. (www.gen-4.org/Technology/horizontal/PRPPEM.pdf) (2006).
11. National Academy Of Sciences, *Management and Disposition of Excess Weapons Plutonium,* p. 34, National Academy Press, Washington, DC (1994).
12. C. D. Jaeger, R. W. Moya, R. A. Duggan, K. M. Tolk, D.A. Rutherford, B. Fearey, J. Markin, B. Erkkila, D. Close, D. Wilkey, L. Moore and S. Strait, "Safeguards and Security Issues for the U.S. Fissile Materials Disposition Program," in *Proc. of the Fifth Intl. Conference on Radioactive Waste Management and Environmental Remediation*, Berlin, Germany, September 4-7, 1995, American Society of Mechanical Engineers (1995).
13. G. D. Wyss, J. F. Clem, J. L. Darby, K. Dunphy-Guzman, J. P. Hinton, and K. W. Mitchiner, "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," in *Proc. of the IEEE 44th Intl. Carnahan Conference on Security Technology,* San Jose, California, IEEE (2010) (CD-ROM).