SAND2011-4907C

Proceedings of the ASME 2011 14th International Conference on Environmental Remediation and Radioactive Waste Management
ICEM2011
September 25-29, 2011, Reims, France

ICEM2011-59380

SECURITY ISSUES FOR LONG-TERM STORAGE OF USED FUEL

Felicia A. Durán, Ph.D.
Sandia National Laboratories
Albuquerque, NM, United States

Gregory D. Wyss, Ph.D.
Sandia National Laboratories
Albuquerque, NM, United States

Calvin D. Jaeger
Sandia National Laboratories
Albuquerque, NM, United States

ABSTRACT

With 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 (UNF). 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. This paper will discuss work to address security issues for long-term storage of UNF. The timeframe for long-term management of UNF is currently defined to be on the order of 100 years. This timeframe presents possible regulatory and technical issues with regard to both storage safety and security. Issues associated with maintaining security for very long-term storage are being identified and addressed. An assessment has been performed of security regulations, including those from the U.S. Nuclear Regulatory Commission and the DOE, for impacts over the longer timeframe. The characterization of UNF as "self-protecting" affects the security requirements associated with storage and handling of this material; however, this characteristic changes over time. It has been determined that the dose rates for commercial UNF 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 UNF, including consideration of "barriers" characteristic of UNF 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, and nuclear signatures considered in the National Academy of Sciences Spent Fuel Standard for Disposition of Excess Weapon Plutonium. In addition, security assessments are being performed for "orphan" storage sites, existing operating storage sites, and possible consolidated storage concepts. This work will evaluate the security risk of UNF storage configurations 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.

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 of UNF. This paper discusses work in progress to address UNF storage security for long-term storage. Previous work [1, 2] focused on

This manuscript has been authored by Sandia Corporation under Contract No. DE-AC04-94AL85000 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

 Copyright © 2011 by ASME

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.

This work is part of a larger effort to develop concepts for a test and verification facility to develop the experimental data to support the 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 evaluations of self-protection of used fuel and relative security risk for UNF storage configurations over the time frame of extended storage.

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 address the issue of how self-protection characteristics changes over the period of long-term storage.

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]. However, 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/hour threshold in approximately 70 to 120 years.

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.

Spent Fuel Standard

In addition to the radiation hazard, additional "intrinsic barriers" characteristic of UNF are being considered as a possible basis for addressing the current self-protection concept. These characteristics are part of the spent fuel standard (SFS), a concept developed by the Committee on International Security and Arms Control (CISAC), National Academy of Sciences (NAS) in its study of options for achieving long-term disposition of the excess plutonium from nuclear weapon dismantlement. In 1994, the NAS first introduced the concept of the SFS 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" [5]. Of concern was the accessibility of the material to nation states with or without reprocessing capabilities as well as nation states or sub-national groups without nuclear programs. The NAS also identified several factors affecting the usefulness of commercial spent fuel, including the intense radioactivity of fission products, the need for chemical separation, the isotopic composition of the plutonium, and acquisition of spent fuel. Further clarification was provided by the NAS in its 1995 report [6] that the rationale for the SFS is that the bulk, composition, and radiation pose appreciable barriers to theft or diversion and that the SFS describes a condition in which weapons plutonium has become roughly as difficult to acquire, process, and use in nuclear weapons as it would be to use plutonium in commercial spent fuel.

In developing performance measures for plutonium disposition [7], the SFS was considered with respect to the form of the final disposition state of the material and how this influences security and safeguards requirement. Again, the characteristics that were considered included radiological (the primary basis for current self-protection), physical, chemical, and nuclear characteristics. The radiological properties address the dose level associated with burn-up and time age of the fuel. 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, along with material form, radiation barriers, ease of separation, and ease of use in a nuclear device. The nuclear properties address the isotopic content of plutonium.

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

Copyright © 2011 by ASME

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. A software tool has been developed to perform an interactive evaluation of the self-protection status of used fuel on a power plant-specific or national level. The tool utilizes a user input screening level, a multi-parameter fit of calculated radiation dose values, and the DOE RW-859 used fuel inventory data, which includes assembly-specific information for discharged commercial fuel assemblies through 2002 with projections through 2014. The tool will be able to identify at-risk inventory and provide data on power plant specific and overall at-risk inventory. Sensitivity studies have been performed to identify which parameters to use in the multi-parameter fit. The fit parameters include variation of assembly initial uranium loading, final discharge burn-up, and final discharge date. The initial uranium loading is included because it can vary significantly with fuel assembly design. The initial uranium loading in BWR and PWR fuel assemblies has varied between 130 and 200 kgU/assembly and 220 to 490 kgU/assembly, respectively. For a given assembly burn-up value, the radiation dose is approximately proportional to initial uranium loading. The sensitivity of dose to initial ^{235}U enrichment has also been investigated, but is not expected to be significant. An assessment of the data base information has been 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.

In addition, previous work for the SFS is being considered for addressing the issue of UNF self-protection. An approach was developed to evaluate the compliance of disposition approaches with the SFS. This approach considered the intrinsic barriers of the final plutonium forms and their importance against three types of proliferation threats, including host-nation, theft by a nation state, and theft for sub-national group. This approach will be revisited by the UNF security team to evaluate the importance of the identified barriers for long-term storage of used fuel.

The current self-protection basis and the SFS overlap some in their consideration of factors for security of long-term storage of UNF. Both consider the radiological hazard. The current self-protection basis considers the chemical properties (not readily separable) and, implicitly, the physical size of UNF. It is evident from the previous and current work on this project that over the period of long-term storage, the current basis for self-protection applies for only a portion of the expected period for long-term storage of UNF. Work will continue to address these issues to evaluate implications of changes over the period 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. The security assessment needs to consider protection provided by a storage container (cask) as well as the facility protection measures and to address identified security issues for long-term storage, including the following:

- Do security protection requirements and strategies change for different concepts or for a commercial versus government site?
- How do we address identified security issues?
  - Differences in requirements for a commercial site versus a government site, including categorization of materials, roll up, threat and level of protection measures
  - Definition and evolution of the adversary capabilities over the longer timeframe
  - Gaps in current requirements and the need to develop new requirements to address the gaps
  - Applicability of the concept of self-protection for used fuel
  - Risk of “orphan” storage sites at decommissioned reactors
  - Protection strategies that consider the viability of long-term institutional control
- How can we improve overall system integration?
  - Facility protection measures integrated with aspects of cask/fuel design that contribute to security
  - Integration of operational activities (monitoring and institutional control)
  - Integration issues for different concepts
  - Identification of “intrinsically secure” system features of storage options – beneficial security characteristics that are inherent options and can be leveraged to enhance security with minimal or no additional cost

For this effort, a risk/cost benefit methodology [8] 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.

Copyright © 2011 by ASME

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 and presents several examples.

General Characteristics of the Proposed Method

The proposed approach starts by identifying a scenario that would offer an adversary a reasonable expectation of success[1] 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 been developed so that they can be considered as roughly independent dimensions of generally equivalent importance.

[1] 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 defined 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: Number 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.

Copyright © 2011 by ASME

- *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: Number 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.

Calculating Difficulty of an Attack Scenario

The Preparation and Execution success factors are represented in 13 dimensions, as describe in the previous sections. Five discrete levels of difficulty have been defined for each success factor dimension. The levels of difficulty have been calibrated so that a particular level for one dimension roughly correlates to an equivalent level of difficulty for any other dimension. Levels of difficulty generally correlate with the size of the portion of the spectrum of 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. Guidelines have been 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.

A numerical value is associated with each of the five levels of difficulty. Because the dimensions are roughly independent and span the most significant challenges that are key to adversary success, the metric for overall difficulty of that scenario for the target(s) under consideration could be calculated as the length of the vector described by the values

Copyright © 2011 by ASME

along each of the phase's dimensions (an L_2 norm). Aggregation methods that apply nonlinear weights to the levels of difficulty within a dimension have also been tested with encouraging results. A dimension's values could also be weighted to reflect that dimension's relative general significance to adversary success, although research to date has not indicated a rationale for other than uniform weighting.

Examples of Initial Application of Scenario Difficulty

The method described above produces a metric for characterizing *targets* (in particular, the response function of target vulnerabilities to threats), and *not* for characterizing threats, adversaries, or scenarios decoupled from specific targets. Because of the qualitative and discrete nature of the assessments, and the diversity of attributes underlying the metric's value, the values are most appropriately interpreted as indicating cohorts of scenarios of similar levels of difficulty required for adversary success in achieving a given level of consequence against the target(s) under consideration. A set of similarly valued conditions (scenario-target pairs) can be considered as a cohort of attack scenarios of comparable difficulty, with differences in values providing a reasonable basis for rank-ordering by level of difficulty. Since the scale for metric values is non-linear, one should not place undo emphasis on ratios of values between cohorts.

Confidence in the dimensions, levels of difficulty, and metric has been reinforced through reviews by subject matter experts, comparisons with other methods for rating threats and scenarios, and by exercising the process for a diverse set of scenarios and targets with a broad range of potential consequences. More than a dozen scenarios have been evaluated that include physical assaults against high-security, high-consequence facilities; the use of vehicle-borne improvised explosive devices against both mobile targets and government buildings; pathogenic attacks against food chain targets; and cyber attacks against sensitive databases. In each case, a detailed scenario was presented to the project team by a knowledgeable subject matter expert who worked with the project team to ensure that the important features of the attack scenario were appropriately captured in the scoring. These interactions helped the project team refine the dimension and level definitions, which underwent revisions during this process.

While the details of these scenarios are sensitive (and in some cases classified), brief descriptions are provided for three scenarios to illustrate how the method is applied and how aggregated results can be compared.

Scenario 1: Oklahoma City Bombing. This scenario reflects the difficulty that was likely encountered by the participants in the plot to bomb the Murrah Federal Building in Oklahoma City. This scenario represents a low level of difficulty, with all preparation and execution factors rated as either Level 1 or Level 2.

Scenario 2: Cyber Theft of Personal Information. A group wishes to steal personal information from an enterprise that is believed to have constructed reasonable cyber defenses. Perpetrators are able to discern the individuals who are responsible for maintaining the cyber defenses, and to send them "spear pfishing" emails that lead the individuals to activate specially crafted malware. The adversaries are able to use this initial access as a foothold from which they escalate privileges and ultimately steal information at will from the enterprise. This scenario was ranked as having a moderate level of difficulty. Most preparation activities were Level 1, although Level 3 was selected for training to represent the need to obtain specialized computer science skills in preparation for the attack. Most execution activities were Level 2, but the high level of stealth and covertness required to execute the attack successfully was placed at Level 3.

Scenario 3: Sabotage at a High-Security Temporary Facility. In this scenario, a high-value item is being stored in a temporary and remote high-security location. The scenario requires the adversary to pre-emplace themselves "under the noses" of the defenders, and to execute a precisely coordinated attack among multiple teams in a relatively unpredictable environment due to randomness that is inherent in the security plans. An insider is required to provide information but not to assist directly in the attack itself. The level of difficulty for this scenario was ranked as high because almost all aspects of the preparation and execution were rated as Level 3 or Level 4.

These examples demonstrate how analysts can assess and rank the difficulty of attack scenarios. While these scenarios were ranked as low, moderate, and high difficulty, respectively, these scenarios did not exercise the full range of the difficulty metric because the low-difficulty scenario did not consist solely of Level 1 attack characteristics, and the high-difficulty scenario did not use even a single Level 5 attack characteristic. Thus, we believe that this system of metrics can be useful for ranking the relative difficulty of a large majority of attacks for purposes of risk management.

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

Copyright © 2011 by ASME

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 and attractiveness; and characteristics of the attack scenario) that would change the baseline scenario at a future time. Additional assessments will be performed for other UNF storage 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. Work has been presented to evaluate and address the issue of the current self-protection basis. A risk/cost benefit methodology is being implemented to evaluate the security risk of used fuel storage facilities relative to other targets. The expected outcome of this work is 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.

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 Idaho National Laboratory, Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories, and Savannah River National Laboratory.

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. SAND2011-4907C, 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. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, p. 34, National Academy Press, Washington, DC (1994).
6. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, National Academy Press, Washington, DC (1995).
7. 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).
8. 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).

Copyright © 2011 by ASME