



Security for Long-Term Storage of Used Nuclear Fuel

Presented at the
MPACT Working Group Meeting
September 14-15, 2011 • Gaithersburg MD

by

Felicia A. Durán – Sandia National Laboratories
Contact: ☎ (505) 844-4495 💻 faduran@sandia.gov



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Approved for Unclassified/Unlimited Release.



Sandia National Laboratories

Used Fuel Disposition Campaign

■ U.S. Department of Energy Office of Nuclear Energy

- Fuel Cycle Technologies Program

■ Used Fuel Disposition Campaign

- Identify alternatives and conduct scientific research and technology development to enable storage, transportation and disposal of used nuclear fuel and wastes generated by existing and future nuclear fuel cycles

■ Used Fuel Storage and Transportation

- R&D Opportunities
- Security
- Concepts Evaluation
- Transportation



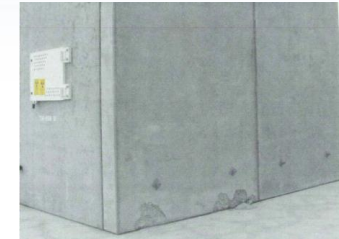
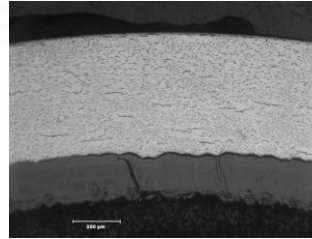
TN Metal Dry Storage Casks.

(http://www.energy.gov/images/Onsite_Dry_Cask_Storage.jpg)

Storage and Transportation Work Packages

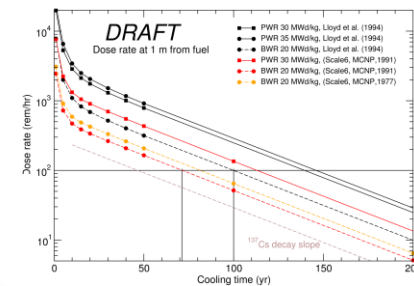
■ Storage R&D Investigations

- Data gap analyses
- Plan to address gaps
- Development of technical basis



■ Security

- Regulatory assessment
- Issues relevant to long-term storage
- Security assessment to address issues



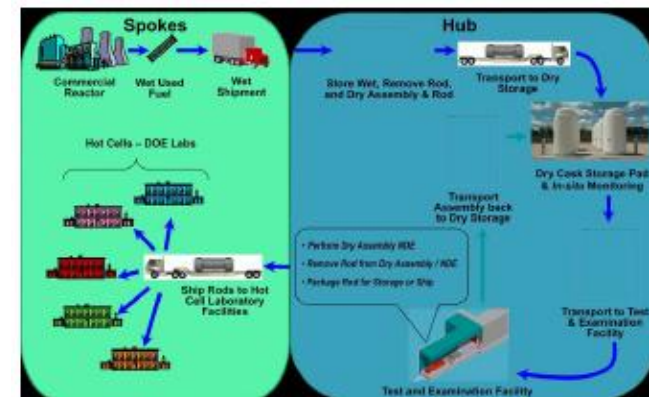
■ Transportation

- High burnup fuels
- Transportation of all fuels after storage



■ Conceptual Evaluation

- Scenarios for development of technical basis
- Systems framework for decision-making
- Capabilities for Test and Validation Complex



Sandia National Laboratories



Used Fuel Storage Security Objectives

■ Objectives

- To identify and evaluate security issues related to extended storage of used nuclear fuel and the associated transportation after extended storage
- Support overall objectives for Storage and Transportation to develop technical bases for extended storage

■ Work Activities

- Address technical and regulatory issues
 - ◆ Self-protection threshold
 - ◆ Security impacts of orphan sites
 - ◆ Long-term engineered protection strategies and institutional controls
- Perform assessments to evaluate security
- Provide recommendations to maintain security

■ Used Fuel Storage Security Team

- Multi-Lab team – Idaho National Laboratory, Lawrence Livermore National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, Sandia National Laboratories, Savannah River National Laboratory

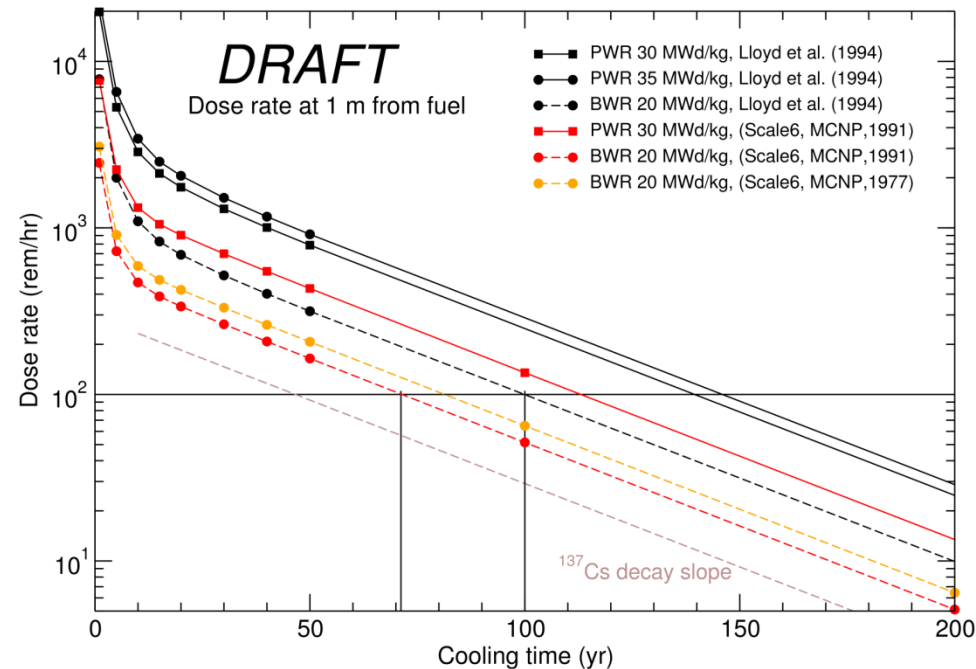
Self-Protection for Used Fuel

■ Most commercial used nuclear fuel (UNF) is considered self-protecting

- High radioactivity makes it extremely dangerous to handle – current dose rate threshold is 100 rem/hour at 3 feet

■ Issues with self-protection for extended storage

- Radioactivity decreases with time due to decay; at some point (70-120 yrs) dose rate for UNF falls below the 100 rem/hr threshold
- Designation of “self-protecting” affects security requirements associated with storage and handling of UNF
- Possible increase in threshold limit – dose rate for UNF will fall below threshold even earlier in time
- Does UNF become a credible theft target?
- Are different protection strategies required?



**FY2010 Results - Dose Rates for
PWR/BWR Low Burn-up Fuels**



Sandia National Laboratories



Re-evaluating Self-Protection for Used Fuel

■ Additional self-protection assessment activities

- Review RW-859 Database (includes assembly-specific information for ~163,000 discharged PWR & BWR assemblies through 2002 with projected data through 2014)
- “Aging Study” – prepared for Argonne National Laboratory

■ Spent Fuel Standard

- Overlap with self-protection
- Considers other characteristics of spent fuel as a basis for disposition options of excess weapons plutonium
 - ♦ Radiological, physical, chemical and nuclear properties
 - ♦ Intrinsic barriers and threat characterization
- Performance measures developed for screening criteria of disposition options



Security Assessment Methodology

- **Based on risk-based cost/benefit method for prioritizing security investment options**
 - Variables for security risk are highly interdependent
- **Rather than using a traditional method that relies on highly uncertain probability of attack, the method uses approaches to describe the difficulty for an adversary to successfully prepare and execute an attack that can produce a given level of consequences**
 - Difficulty of attack is a characteristic of the target
 - Allows comparison and prioritization across multiple targets or facilities across an enterprise
 - ◆ Comparison of used fuel storage facilities relative to other targets
 - ◆ Consideration of factors that change over time frame of extended storage
 - ◆ Basis for developing recommended protection strategies for extended storage



Adversary Decision Criteria

- Approach examines adversary criteria for selecting which attack scenario to pursue, including:

Adversary's Decision Criterion	How we make an attack less likely
"Could I do it if I wanted to?" <i>(Is success likelihood high?)</i>	Make attack scenario more difficult
"Would I do it if I could?" <i>(Worthy investment of resources?)</i> <i>(Does it violate my doctrine?)</i>	Make attack scenario more difficult or reduce potential consequences
"Are the expected consequences high enough?"	Reduce the potential or expected consequences of the scenario

- The benefits of a security investment can be inferred from two metrics:
 - How much harder has the scenario become for an adversary?
 - How much have expected consequences been reduced?

Considerations for Estimating Attack Scenario Difficulty

Attack Preparation

- **Outsider attack participants**
 - Number of engaged participants
 - Training and expertise required
- **Insider attack participants**
 - Number and coordination
 - Level of physical and cyber access required, sensitivity, vs. security controls
- **Organizational support structure**
 - Size, capabilities and commitment
 - Training facilities, R&D, safe haven, intelligence and OPSEC capabilities...
- **Availability of required tools**
 - Rarity, signatures for intelligence or law enforcement, training signatures...

Attack Execution

- **Ingenuity & inventiveness**
- **Situational understanding**
 - Observability and transience of vulnerabilities
- **Stealth & covertness**
- **Dedication & commitment of participants**
 - Risk to both outsiders and insiders includes personal risk, willingness to die, etc.
 - Risk to the “cause” or support base
- **Operational complexity/flexibility**
 - Precision coordination of disparate tasks
 - Multi-modal attack (cyber+physical+???)

Example characteristics used to establish levels of difficulty for each dimension:

Scenario difficulty is a property of the target.
It estimates how capable the adversary must be to have a successful attack.

Risk managers can then ask, “Are the easiest attacks difficult enough to deter the adversaries we are concerned about?”

Laboratories

Example Scenario: 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.

Level (Score) [1, 2, 3, 4, 5 → 1, 3, 9, 27, 81]

Attack Planning & Preparation	Participants	2 (3)	Several (~2-5); Small team
	Training	2 (3)	Self-taught; Open source info; No professional foundation; Practice not required for critical tasks
	Support	1 (1)	Minimal; Few if any support personnel / collaborators; No intelligence support; Preparations easily concealed—no need for cover; Open source info
	Tools	2 (3)	Legal availability controlled, limited to special purpose uses; Typical of criminal enterprises
	# of Insiders	1 (1)	None
	Insider Access	1 (1)	None
	Ingenuity	1 (1)	Very predictable, straightforward approach; Easily conceivable by knowledgeable public; Defenses likely to be well prepared / trained against
Attack Execution	Situational Understanding	1 (1)	Minimal; Requires little recognition or utilization of exploitable conditions; Exploitable vulnerabilities are persistent and predictable, with evident signatures
	Stealth & Covertness	1 (1)	Minimal
	Outsider Commitment	2 (3)	Persistent remote exposure or participants, limited direct exposure to less-than-lethal conditions; Little risk of casualties, but significant risk of participant attribution
	Insider Commitment	1 (1)	None
	Complexity	1 (1)	Single avenue of attack with simple tasks; Unimodal tasks; If multi-modal attack, modalities are sequential, temporally decoupled
	Flexibility	1 (1)	Singular binary course of action; No contingency planning; Little tactical adjustment
Aggregated Score		-- (21)	Score for each level is 3x that of the next lower level in this example.



Implementation for Used Fuel Storage Security

■ Discussions by Security Team

- Regulatory context for security at commercial used fuel storage sites
- Overview of site configuration and cask characteristics
- Self-protection – Changes over extended storage
- Risk-Based Cost-Benefit Security Assessment Methods

■ Implementation Steps

- Identify consequences of concern
- Identify attack scenarios for each consequence
- Develop a description of the scenario and what the adversary will require for success
- Develop preliminary difficulty scores
- Develop strategies to estimate consequences



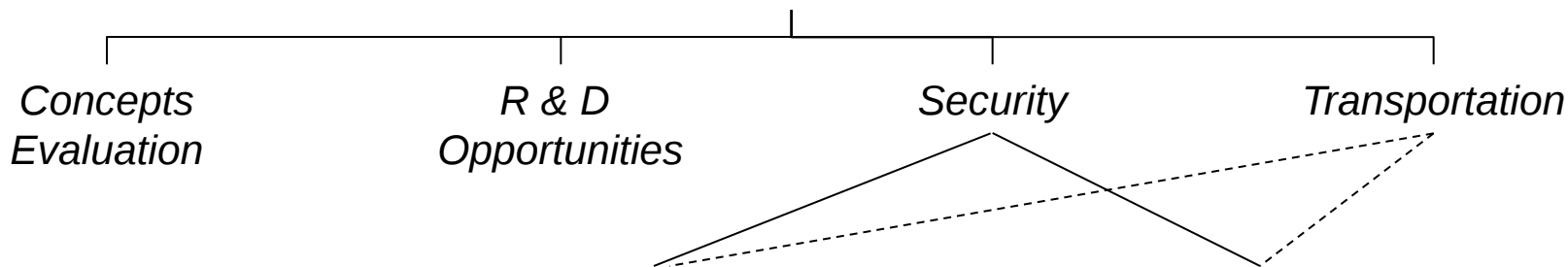


Implementation for Used Fuel Storage Security

- **Development of baseline scenarios for a generic “orphan” site based on current conditions**
 - Radiological sabotage threat for surface storage at decommissioned reactor (no additional fuel to be received)
 - Scoring for Attack Difficulty – Preparation and Execution
- **Further assessment efforts**
 - Discussion of changes in conditions over time
 - ◆ Used fuel characteristics (dose rate, other)
 - ◆ Evolution of attack characteristics
 - ◆ Other storage system conditions
 - Assessment for baseline scenario change over time
 - ◆ 50 years, 100 years, 100+ years
 - Assessment for other storage configurations and transportation
 - ◆ At-reactor ISFSI, consolidated storage site

Summary of Used Fuel Storage Security Efforts

USED FUEL STORAGE Technical Bases



	Radiological Sabotage	Theft
Current	Established protection requirements for irradiated fuel – external dose >100 rem/hr at 3 ft	Not considered a credible threat in NRC Design Basis Threat
VLTS	Fuel will fall below <100 rem/hr in 70 to 120 years (longer for high burn-up fuel)	
Issues	Regulatory gap?	Credible threat?
FY2011 Efforts	Security risk of used fuel storage relative to other targets – Recommendations for orphan sites Recommended protections strategies – below self-protection threshold, long-term institutional control	

