3/30/15

Defense in Depth for Dry Cask Storage Systems

Background:

The Nuclear Regulatory Commission (NRC) has risk-informs a variety of regulatory activities. As a part of the implementation of the proposed risk-inform regulatory framework for Spent Fuel Storage and Transportation (SFST) regulatory activities, the Agency needed to more consistently consider the concept of defense-in-depth and evaluate its proper use in the spent nuclear fuel storage regulatory program.

The term "defense-in-depth" was introduced in WASH-1250[1] as a convenient method of summarizing the "Lines of Defense", or the "Levels of Safety". WASH-1250 distinguishes three levels of safety, each with a distinct objective. This structure of defense-in-depth, together with the objectives of each level, is shown in Figure 1, which is an illustration of the application of this concept of defense-in-depth to spent fuel dry storage.

Defense-in-depth is typically defined as an approach to designing and operating nuclear facilities that prevents and mitigates accidents that have the potential to release radiation or hazardous materials. The concept calls for creating multiple independent and redundant layers of defense to compensate for uncertainties, and potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon for minimizing the risks to the public, environment, and plant personnel.

[1] WASH-1250, "The Safety of Nuclear Power Reactors (light Water-cooled) and Related Facilities," (USAEC, July 1973, LM12143A280)

Defense-in-Depth (DiD) and DiD-like Requirements and Guidance in US NRC Regulations

The United States Nuclear Regulatory Commission (US NRC) regulatory requirements (codified in Title 10, *Code of Federal Regulations* (CFR)) contain only a handful of instances that specifically mention defense-in-depth. Generally, the statement specifies that defense-in-depth concepts or practices are to be implemented, or simply, that "defense-in-depth is to be maintained."

In addition to the concept of defense-in-depth, there are US NRC regulations and guidance that contribute to safety by requiring redundancy and multiple layers of defense. The following are some examples:

Double Contingency Principle. 10 CFR 70.4, 10 CFR 70.64(a)(9), 10 CFR 72.124(a) and 72.236(c) "...at least two unlikely, independent and concurrent changes in process conditions before a criticality accident is possible."

Redundant Seals. 10 CFR 72.236 (e). "The spent fuel storage cask must be designed to provide redundant sealing of confinement systems."

Redundant utility or other services. 10 CFR 72.122 (k) (1). "Each utility service system must be designed to meet emergency conditions. The design of utility services and distribution systems that are important to safety must include redundant systems to the extent necessary to maintain, with adequate capacity, the ability to perform safety functions assuming a single failure."

Single Failure Criteria. Regulatory Guide 1.53, and 10 CFR Part 50, Appendix K. "An analysis of possible failure modes of [emergency core cooling system] ECCS equipment and of their effects on ECCS performance must be made. In carrying out the accident evaluation the combination of ECCS subsystems assumed to be operative shall be those available after the most damaging single failure of ECCS equipment has taken place."

Multiple Barriers (isolation). SECY-82-0288. "It has chosen to address this difficulty by requiring that a DOE proposal be based upon a multiple barrier approach. An engineered barrier system is required to compensate for uncertainties in predicting the performance of the geologic setting, especially during the period of high radioactivity. Similarly, because the performance of the engineered barrier system is also subject to considerable uncertainty, the geologic setting must be able to contribute significantly to isolation."

Definition of Defense in Depth for a Dry Spent Fuel Storage

Defense-in-depth has been described in a report by the US NRC, Office of Nuclear Material Safety and Safeguards (NMSS)[2] as: "a design and operational philosophy with regard to NMSS-regulated facilities that calls for multiple layers of protection to prevent and mitigate accidents. It includes the use of controls, multiple physical barriers to prevent release of radiation, redundant and diverse key safety functions, and emergency response measures." This document contains DSFM's early thinking regarding defense-in-depth for dry cask storage.

NMSS's Division of Spent Fuel Management (DSFM) is engaged in an effort to establish a framework to risk-inform regulatory decisions and activities in the area of spent nuclear fuel storage. At this time, this effort is limited to the dry storage of spent nuclear fuel from commercial power reactors under the general license provisions of 10 CFR Part 72. As part of this effort, DSFM is proposing to develop the application of the defense-in-depth philosophy to this area in order to facilitate this philosophy's explicit consideration within the risk-informed framework.

Key Safety Functions

The key safety functions that need to be maintained in dry spent fuel storage operations are:

1) Nuclear sub-criticality - required by 10 CFR 72.124 and 72.236(c) that controls be established to prevent a criticality event.
2) Prevention of radiation exposure exceeding regulatory limits - As stated in 72.104(a) establish dose limits for the public for normal operations and anticipated occurrences; 72.106(b) for accidents, including natural phenomena events.
3) Prevention of release of radioactive materials exceeding regulatory limits of 10 CFR 72.104(a) and 72.106(b).

The combined dose of direct radiation from the storage and from releases must also not exceed the regulatory limits.

Phases of Operation

Dry spent fuel storage operations can be divided into three phases. The first phase is the loading and transfer phase. This includes the steps in loading of spent fuel elements into a spent fuel dry storage cask or a canister in the spent fuel pool, the removal from the spent fuel pool, and movement of the cask to the preparations area. Loading also includes the activities performed at the preparation area such as draining, drying, pressurization with inert gas, and sealing. After all preparation are completed, the cask is move to outside of the containment. If multipurpose canisters are deployed as a part of the dry storage system (DSS), there would

---

[2] Risk-Informed Decisionmaking for Nuclear Material and Waste Applications, Rev. 1, Feb. 2008. ML080720238

also be a transfer step where the canister is unloaded from the transfer cask into a storage cask. The final step in first phase is transferring the storage cask to a predetermined location in a concrete vault, or on the independent spent fuel storage installation (ISFSI) pad.

The second phase is the storage phase. The purpose of this phase is to safely store the dry spent fuel until it can be transport to a final disposal site. Storage phase can last for decades[3], and during this period the storage cask is exposed to natural events and possible man-induced events.

The third phase encompasses removal of a spent fuel storage cask from the ISFSI and storage overpack either for loading into a transportation overpack in preparation of shipping offsite, or for returning back into a spent fuel handling facility. The storage cask may need to be returned for various reasons. This operation may include transfer and unloading steps that are the reverse of those in the first phase. Such operations have been done, as in the case of a Peach Bottom cask when the outer closure seal failed. Safety concerns spans over all three phases of the dry spent fuel storage operation.

Levels of Defense-in-Depth

The concept of defense-in-depth (DiD) as applied to dry storage safety must address the previously identified three safety functions. The safety objective for each safety function is listed. There are the three levels of defense defined: prevention, mitigation, and emergency actions. Examples of elements of protection within each level are presented in Figure 1. These levels are described below.

First level

The objective of the first level is to prevent abnormal operation and failures. This includes multiple components of protection to prevent nuclear criticality accidents and to prevent increased direct radiation exposure and release of radioactive materials. This includes minimizing the likelihood of occurrence of events (i.e., abnormal operations, failures, natural phenomena and accidents). These components include engineered physical barriers and cask design features, site features (including modifications to the site), and personnel actions or operations.

For a DSS, the components in the first level specify the design, analyses, siting and construction of the DSS. These include hardware (e.g., cask SSCs), siting, modifications made to the site, and tests conducted to verify the quality of the DSS fabrication. The components also include routine and scheduled monitoring and maintenance, licensee corrective action programs, and testing performed in the course of preparing material for storage. It also includes

[3] Casks used under general license provisions have so far been certified for 20 years of storage though the rule allows for certification for up to 40 years. The certificate may be renewed for up to an additional 40 years before requiring an additional renewal by the NRC.

site boundary monitoring, dose measurements during loading and transfer, and inspections required for certificate renewal and aging management programs.

Second Level
The objective of the second level is to address expected and unexpected events where the first level's components of protection are not able to adequately maintain one or multiple safety functions of the DSS. This scenario may result from a component(s) in the first level of defense-in-depth not performing as intended or being overwhelmed. Depending on the circumstance, the failure of the first level of defense-in-depth may be gradual or rapid. An example of a second level component of protection would be the addition of temporary shielding to prevent radiation from a DSS exceeding the regulatory limit following an off-normal event or accident (for example, the dropping of a transfer cask causing damage to the transfer cask's neutron shield shell and loss of the liquid neutron shielding).

These components of protection can also respond to gradual failures of the first level of Defense-in-depth. For example, a DSS is designed, analyzed, and constructed to resist known material degradation mechanism at the time; but over time the confinement may be challenged by newly identified mechanisms. In this example, components of protection could include performing a repair on the DSS.

Third Level
The objective of the third level is to implement emergency actions to protect the public and on-site personal if the first two levels of defense fail. As stated in the NRC policy statement, "Safety Goals for the Operation of Nuclear Power Plants" (51 FR 30028; August 4, 1986), emergency preparedness is a "defense-in-depth" measure. This additional level of defense relies on having an emergency plan for the ISFSI (dry storage operations) so emergency response measures can be taken.

The components in emergency plans include notifications and protective responses. The plan cover the possible radiation exposures expected to occur and the short and long term protective actions, when under the highly unlikely conditions where the first and second levels of defense have failed. The emergency plans provide actions to minimize doses for a "spectrum" of events that could impact site workers, and potentially produce offsite doses in excess of those allowed by the NRC regulations and the U.S. Environmental Protection Agency protective action guides.

Summary

Defense-in-depth is a philosophy that involves multiple, independent levels of defense that may include multiple independent and/or redundant components of protection to ensure the safety of an activity. The key concept is that no single level or component of defense is relied upon to assure safety. This philosophy has a long history in the regulation of nuclear activities. DSFM is proposing a working concept of how defense-in-depth can be applied to dry storage of commercial power reactor spent fuel under the general license provisions of 10 CFR Part 72. The purpose of this effort is to better ensure explicit and consistent consideration of this philosophy as part of a risk-informed framework for regulatory decisions in this regulated area. This strategy will be assessed and modified as warranted as the risk framework is defined and implemented.

Figure 1: Three Levels of Defense-in-Depth for Dry Storage[4]

Safety Objectives	First Level - Prevention	Second Level - Mitigation	Third Level Emergency Actions
Protection Against Nuclear Criticality During Storage	• Double contingency principle (10 CFR 72.124(a)) - Cask/canister confinement (barrier to water intrusion) - Neutron Absorbers (Poisons) with fuel burn-up credit in criticality analysis • Aging Management Programs for fuel, neutron absorber, and cask/canister confinement. (NUREG-1927)	• Perform remedial actions - Relocate DSS to reduce external factor - Repackaging - Re-evaluate potential for criticality - Repair DSS	• Site Emergency Plan - Accident detection/assessment - Notification - Protective Response (protect workers and public)
Protection Against Radiation Exposure Exceeding Regulatory Limit During Storage	• Radiation shield overpack/storage module/transfer cask/cask • Siting (controlled area, 72.104 and 72.106(b)) • Radiation/environmental monitoring • Monitoring and maintenance	• Accident Assessment • Add (temporary) additional shielding • Repackaging	• Site Emergency Plan - Accident detection/assessment - Notification - Protective Response (protect workers and public)
Protection Against Release of Radioactive Material During Storage	• Cask/canister Confinement (barrier to material release) • Fuel Cladding - Canister inspection (NUREG-1927) • Radiation Monitoring/environmental monitoring	• Accident Assessment • Repair confinement boundary • Reanalysis and/or repackage	• Site Emergency Plan - Accident detection/assessment - Notification - Protective Response (protect workers and public) -

[4] The scope is confined to dry storage of commercial power reactor spent fuel under the general license provisions of 10 CFR Part 72.

Stakeholders (e.g., industry, members of the public, Department of Energy, etc.) will be engaged throughout the process to ensure their perspectives are factored into the process.

Approved:

Mark Lombard, Director Division of Spent Fuel Management	7/29/15 Date
Anthony Hsia, Deputy Director Division of Spent Fuel Management	5/11/15 Date
Meraj Rahimi, Branch Chief Criticality, Shielding & Risk Assessment Branch	4/27/2015 Date
Donald Chung, Risk Analyst Criticality, Shielding & Risk Assessment Branch	4-27-2015 Date
Michel Call, Nuclear Engineer Criticality, Shielding & Risk Assessment Branch	04/27/15 Date