# UTILIZATION OF PROBABILISTIC RISK ASSESSMENTS TO GUIDE CONCEPTUAL DESIGNS OF A REPOSITORY

L. J. Jardine
Bechtel National, Incorporated
San Francisco, California 94119

## ABSTRACT

Probabilistic risk assessment (PRA) techniques have been applied as part of the preclosure performance assessments for accident conditions conducted on the engineered systems, structures, and equipment developed during the conceptual design of a geologic repository. Performance assessments are used as a part of the systems engineering activities to aid in establishing realistic design requirements, to guide the engineering design process, and to enhance the overall safety of the design. This is accomplished through an iterative feedback approach. The approach evaluates the PRA results of the performance assessments and then, if necessary, recommends new design changes for input to the next stage of design that improve the performance objectives. If these evaluations are repeated during all phases of repository design, an optimized design which meets all performance objectives will be obtained. All design projects, particularly first-of-a-kind complex nuclear facilities, may find the performance assessment techniques outlined in this paper to be a good tool for developing optimized design concepts which satisfy the design requirements, safety goals, and the performance objectives.

## INTRODUCTION

This paper outlines the general design process used to develop a conceptual design for the surface facilities of a geologic repository, interprets the results of a preclosure performance assessment for accident conditions conducted on the conceptual design, and discusses how the results of the performance assessments can be used to formulate recommendations to change the design in subsequent design phases to enhance the repository safety and the performance objectives. This approach to the design of a complex nuclear facility is unique because the architect engineer conducted and coordinated all of these activities as part of a single design project. Some background on the relationships of systems engineering and performance assessment is also given.

## BACKGROUND: SYSTEMS ENGINEERING AND PERFORMANCE ASSESSMENTS

Systems engineering activities and performance assessment methods are being developed for geologic repositories and the waste management system. Systems engineering involves the orderly process of defining the nature, relationships, and interfaces between and within the mined geologic disposal system (MGDS), its three major subsystems (i.e., site, waste package, and repository) and the rest of the waste management system. Systems engineering activities apply to all phases of a project from an initial system requirements analysis and design criteria development through design, procurement, construction, startup, operation, maintenance, training, and client acceptance. A major portion of the systems engineering activities is front-end work in preparation for the design engineering. Systems engineering continues throughout design engineering and the remainder of the project. Systems engineering techniques are used to continuously analyze the design against project or mission objectives, system requirements, design criteria, and performance objectives and to verify the design before proceeding with the next design phase or actual construction. Many systems engineering functions, such as interface management and configuration management, continue concurrently with other project activities until the project is completed.

The major objective of the systems engineering activities is to develop a framework for the systematic and orderly control of the geologic repository development. An initial task in the systems engineering activities is the development of the generic requirements for a MGDS. These requirements are established in a top-level baseline controlled document that is used to control the technical design requirements and to ensure a reasonable degree of uniformity among the diverse design efforts required to design a repository (1) The requirements reflect and interpret applicable regulatory performance objectives, standards, DOE criteria, and mission requirements on a generic basis. The top-level document is the official basis for all system descriptions and design activities. Secondary documents are prepared by each repository project which incorporate the MGDS generic requirements as well as site-specific objectives, standards, other criteria, and federal, state and local requirements. These secondary documents define the site-specific requirements and provide the basis for developing the site-specific repository design requirements, performance criteria, interface-control requirements, design bases, and performance specifications for the various subsystems and components of the MGDS.

Performance assessments analyze the combined effects of the numerous phenomena that might affect the facilities designed for the MGDS. Preclosure performance assessments address the safety aspects of the operating repository and determine compliance with applicable performance specifications, performance objectives, and regulatory requirements. These assessment activities predict the ability of the repository design, its subsystems, and it components to meet project-specific requirements established through the systems engineering process. The generic repository system and subsystem performance objectives developed as part of the systems engineering activities comply with the regulations, standards, and

objectives of 10 CFR 60, 40 CFR 191, and 10 CFR 960. Performance assessments compare site-specific performance objectives of repository systems, subsystems, and components with calculated performance predictions.

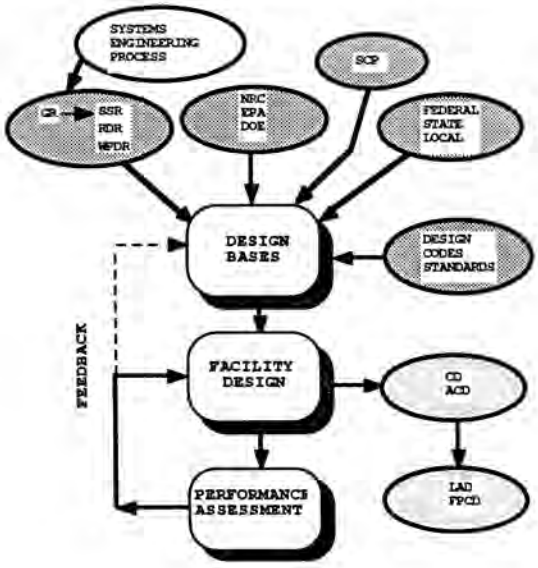
## GENERAL REPOSITORY DESIGN PROCESS

An outline of the process being used by this architect engineer to design the surface facilities of a geologic repository is illustrated in Fig. 1. It consists of four general steps:

Step 1: Establish the Design Requirements and Design Bases
Step 2: Develop a Facility Design
Step 3: Conduct a Performance Assessment of the Design
Step 4: Revise the Facility Design, if necessary, and Iterate

### Step 1:

Design bases are constructed by the architect engineer firm during the initial stages of the design project to guide the development of the facility design, as illustrated in Fig. 1. Inputs used to develop these design bases are taken from the systems engineering generic requirements (GR) documents, project site-specific requirements (SSR), site-specific repository design requirements (RDR), site-specific waste package design requirements (WPDR), the Site Characterization Plan (SCP), NRC and EPA regulatory requirements, DOE site-specific requirements, and other federal, state and local requirements, standards, and codes. Design bases include the performance objectives and establish detailed design requirements for radiological protection, nuclear safeguards, site security, radiation monitoring, fire and explosion protection, materials handling and storage, nuclear criticality, industrial and chemical safety, electrical, mechanical handling, and natural phenomena such as seismic, tornados and wind, water levels, snow loads, and ice loads. The numbers, types, complexity, and details of the design bases increase as the design stages progress.




**REPOSITORY DESIGN PROCESS**

Fig. 1. Illustration of the Iterative Feedback Process Used to Guide the Design of a Geologic Repository

### Step 2:

The development of a specific facility design is achieved by a conventional multidiscipline engineering design team. For the conceptual design stage, the design team is separated into groups such as mechanical engineering and plant design, nuclear engineering, civil, structural and architectural engineering, electrical and control systems engineering, and systems engineering. The design team develops and generates the design bases, the facility design drawings, and the outline specifications. This team also conducts special tradeoff studies required to select specific design alternatives. A conceptual design for the surface facilities of a geologic repository resulting from this process is reported in Ref. 2.

### Step 3:

After a reference facility design is established by the design team, a performance assessment of the design is conducted by the systems engineering group. The systems engineering group consists of staff from multiple engineering and scientific disciplines and reports to the same project engineer as the major design groups but functions in the design process as a separate independent analysis group. The performance assessment predicts the effects of both normal and accident operating conditions on a repository design during the time it is open for handling and emplacement of radioactive wastes. The assessment evaluates the responses of the facility design in terms of the conditions that might affect its performance, including natural events and processes, human actions, and interactions between the radioactive waste and the facility design. The calculated performance predictions and the site-specific performance objectives in the design bases are then compared.

### Step 4:

Using the comparative results of the performance assessments, the design requirements are reevaluated and the design is modified to enhance the safety and reliability and improve the performance of the initial repository design. This step constitutes an iterative feedback process. If the entire cycle is repeated for each stage of design from conceptual to final design, a systematic method exists to optimize and improve the design in the subsequent design phases.

The preclosure performance objectives outlined in Step 3 for the repository system can be achieved through a variety of designs. Determining whether the performance objectives for a specific design will be met is a process of iteration between design and performance assessment as outlined in Fig. 1. The iterative design process involves incorporating initial design requirements and performance objectives from many sources into the design bases prepared by the architect engineer and then developing a specific facility system design. Next, performance assessments are conducted by the architect engineer to identify operating scenarios and to assess whether the facility design will achieve the specified performance objectives for both normal and accident conditions. If the objectives are not met, new design alternatives are proposed based on the data base and technical insights generated by the performance assessments.

Once design changes are established, modifications are made in the initial facility design to satisfy any new design requirements. The performance assessment is then repeated to verify that the design modifications allow the performance objectives to be achieved. Each iteration of design and performance assessment uses increasingly more detailed site-specific and design-specific information as the design stages advance toward completion. In a few instances during the initial design stages, it is conceivable that some parts of the initial design bases may merit revision. This is indicated by the dashed line in Fig. 1. However, no changes to the original performance objectives are made. This iterative feedback process ultimately results in the final and optimized design with performance requirements allocated to the individual components of the repository system design.

The ability to apply this design approach to all stages of the repository design is dependent upon the time allocated to complete each of the steps in the iterative process. This process has been successfully applied during the conceptual design stage of a geologic repository to enhance the safety of the initial facility design (2,3,4). Methods for applying these principles to the subsequent advanced conceptual design (ACD), license application design (LAD), and final procurement and construction design (FPCD) stages of geologic repositories will be developed based on the successful application of these principles during the conceptual design stage.

## STAGES OF REPOSITORY DESIGN

The DOE has separated the design of geologic repositories into four stages (5). The four stages can be compared to the two phases of conventional facility design: the conceptual design phase and the Title I and Title II design phases. These relationships may be summarized as follows:

Phase One: Conceptual Design

- Stage 1: Conceptual Design for Site Characterization Plans
- Stage 2: Advanced Conceptual Design

Phase Two: Title I and Title II Design

- Stage 3: License Application Design
- Stage 4: Final Procurement and Construction Design

The initial conceptual design concentrates on the surface and subsurface systems, structures, emplacement, and component designs that require site characterization data. The design provides information to ensure that the site characterization data collection plans relative to the repository design are adequately covered in the specific site characterization activities (5). The advanced conceptual design starts after the repository conceptual design reports supporting the Site Characterization Plan are completed. This design stage is used to refine the initial site specific design requirements, criteria, and concepts that will be made final in the next stages of the repository design (5).

After the advanced conceptual design reports are completed, the license application design (LAD) portion of the Title I (preliminary design) and Title II (final design) design phases are started. The DOE has decided that the design of systems, structures, components, excavations, and necessary engineered barriers should be substantially complete at the time the license application for the repository is submitted to the NRC in order to establish and demonstrate compliance with the performance objectives of 10 CFR 60. The LAD design phase will therefore resolve any remaining design and licensing issues identified and assessed in the two earlier conceptual design stages. Sufficient design information is developed to demonstrate compliance with the design requirements and performance objectives of 10 CFR 60, which is required for the repository license application. A safety analysis report as specified in 10 CFR 60 is prepared. To allow emphasis on the safety systems during the LAD design phase, the design of non-licensing related auxiliary support systems will be developed during the LAD design stage only to the extent necessary to ensure adequate cost estimates, schedules, planning, and their proper functions. All three repository sites being characterized will prepare LAD designs (5).

## PRECLOSURE PERFORMANCE ASSESSMENTS FOR ACCIDENT CONDITIONS

The preclosure performance assessment for accident conditions conducted by the systems engineering group as Steps 3 and 4 of the general repository design process used a probabilistic risk assessment (PRA) approach. The approach can be divided into four primary parts:

- o systems modeling and analyses
- o radioactive release analyses
- o consequences analyses
- o regulatory compliance assessment

The systems modeling includes scenario development and screening to establish possible future occurrences that might affect a specific repository design, assigns probabilities to them, and determines which occurrences merit detailed consideration as part of the formal performance assessment. Radioactive release analyses involve the development of source terms and radionuclide releases from accident scenarios requiring consequence analyses. Consequence analyses calculate the offsite doses that might arise from the scenarios of interest. The regulatory compliance assessment evaluates the results of the systems modeling analyses, release analyses, and the consequence analyses to determine whether the repository design is in compliance with the NRC, EPA, DOE performance objectives, and all other requirements. This approach for accident conditions is based on probabilistic risk assessment techniques.

A PRA provides techniques for integrating the diverse aspects of design and operation that assesses the risks and develops an information base for analyzing both site-specific design requirements and generic issues. Probabilistic risk assessment has been a rapidly developing field in the past decade, particularly with regard to nuclear reactor safety which was introduced in the Reactor Safety Study, Wash-1400 (6). In general, a PRA (1) identifies and delineates the combinations of events that, if they occur, will lead to a severe accident or some other undesired event, (2) estimates the probability of occurrence for each combination and (3) estimates the consequences (3,4,7). This is basically the approach outlined in Step 3, above, for the performance assessments of a repository design.

The emphasis in PRAs for reactors has been on identifying internal failure modes leading to serious consequences, mainly core melts, and recently also on low probability but rapidly developing accidents that bypass the reactor containment structure (7).

The major advantage of a PRA is that it can integrate in a uniform method all the relevant information, including system designs, operating practices, operating histories, component reliabilities, emergency actions and potential environmental and health effects. The PRA is good for identifying weak points in the system design. The PRA's limitation is that not every element in the assessment is developed to the same level of detail. We believe the PRA is an excellent systems engineering analytical tool that can be effectively applied during the conceptual design of complex nuclear projects.

## INTERPRETATION OF PRA RESULTS AND FEEDBACK PROCESS ILLUSTRATIONS

Two specific examples are discussed that illustrate how the PRA preclosure performance assessment for accident conditions has been used to guide the design process by specifying design alternatives to improve the overall safety of the repository. Many of the same principles can be applied to performance assessments for preclosure normal operating conditions and postclosure periods; however, this is beyond the scope of this paper. Recommendations of possible changes to the facility design during the next ACD phase of the repository design are discussed to demonstrate how the iterative feedback process can be implemented. Similar evaluations are being performed for other accident scenarios identified in the complete performance assessment (3,4).

Figure 2 summarizes the thirteen most dominant accident scenarios identified in a complete PRA performance assessment of a repository conceptual design (3,4). Dominant scenarios are defined here as those occurring with a probability greater than $10^{-9}$ per year and resulting in an offsite dose consequence greater than 50 mrem. Figure 2 shows that no scenarios result in offsite dose consequences that exceed 1.1 rem. These scenarios are conservatively estimated to occur with probabilities smaller than $10^{-6}$ per year or less. For such probabilities, these scenarios are considered incredible and can be justified as not part of the repository design bases. Details of these PRA analyses, the specific repository conceptual design, and a complete description of accident scenarios are given elsewhere (3,4).

The scenarios in the packaging hot cell of the main waste handling building result in threefold greater dose consequences than the others indicated in Fig. 2 and, as such, represent a greater risk than the others. These scenarios all involve a potential drop within the packaging hot cell of a container of spent fuel prior to its being sealed. The scenarios are based on an initial facility conceptual design developed for a Site Characterization Plan (2,3,4). In this conceptual design consolidated spent fuel is loaded in the containers in the horizontal position. The unsealed container is then rotated and moved with an overhead crane device to the vertical position for the container closure operations. The discovery during the performance

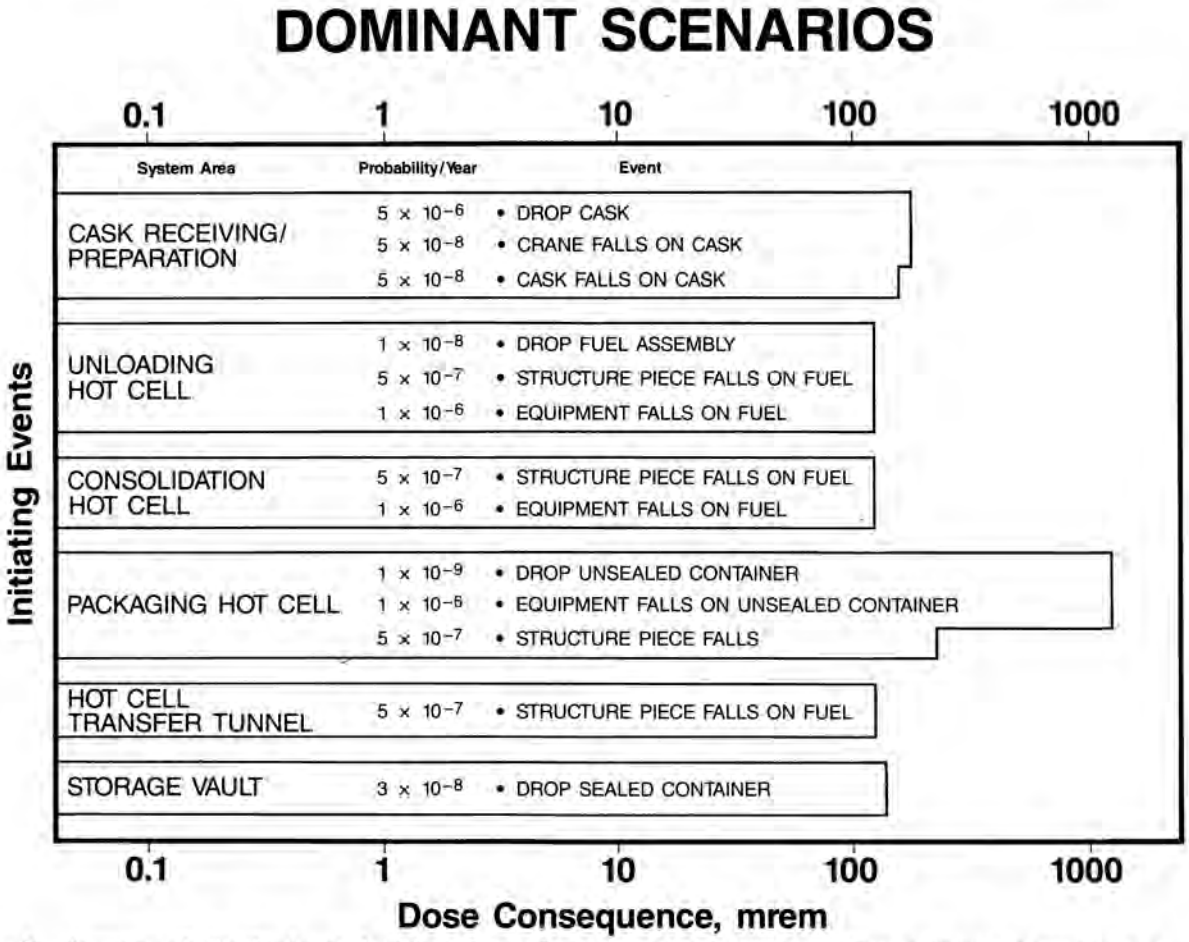



Fig. 2. Summary of the Dominant Accident Scenarios in the Main Waste Handling Building Identified in a Preclosure PRA Performance Assessment of the Surface Facilities a Geologic Repository (3,4)

assessment that the unsealed container requires handling operations is a key design issue that merits further evaluation.

These dominant scenarios in the packaging hot cell can be eliminated by design modifications from the initial facility design in various ways: for example, (1) by performing the container closures before any rotation of the unsealed containers, (2) by reducing the possible drop heights of the unsealed containers, or (3) by designing the hot cell equipment or the structure to lower even further the probability of occurrences of the postulated failure during a seismic design basis event. To enhance the safety of the facility design and to obtain an improved performance assessment response, the design modification alternatives outlined above are being evaluated and recommendations are being formulated for changes for the next stage of repository design -- the advanced conceptual design stage. Some consideration must be given to cost benefit ratios while the design alternatives are evaluated. When finalized, the specific recommendations resulting from the performance assessment for changes to the initial design requirements will constitute the feedback process illustrated in Fig. 1.

Although they result in only twofold greater dose consequences than most other scenarios, the next most dominant scenarios in Fig. 2 occur in the cask receiving and preparation area of the main waste handling building (2,3,4) These can be evaluated to determine if the inherent safety of the design can be improved by a change in the facility design. These scenarios all involve the potential drop of a shipping cask that exceeds 30 feet. The initial facility layout provides a cask preparation laydown area that is at an elevation 25 feet below the grade of the truck and rail cask handling area (2) These accident scenarios can be eliminated by (1) designing the casks to withstand such drops, (2) providing a facility design that does not have the 25-foot elevation difference, or (3) installing cask drop mitigation design features. Specific recommendations for changes in the facility design are currently being evaluated and formulated for the next design stage. In arriving at a specific recommended design alternative, the evaluation process must include a consideration of the effects and the interdependence of the multitude of system components and other design requirements.

## CONCLUSIONS

Typically, detailed safety analyses and performance assessments are conducted late in the design process in parallel with the Title I (preliminary) and Title II (final) design phases of facilities. If either of these establish unacceptable results for the facility, design changes must be made. Depending on the complexity and specific stage of a project's design and construction, these changes generally have a large impact on project cost and schedule. However, if design changes or modifications are identified in performance assessments during the conceptual design stage, the changes are only made on limited quantities of paper rather than with concrete. Thus, they can be implemented with virtually no impact on cost and schedule. This is the most important incentive for applying performance assessments early and continuously to the design process as the facility design is being developed.

Conducting performance assessments of accident conditions during the conceptual design required an innovative application of PRA techniques because of the incomplete, soft, and varying levels of design details. Because the architect engineer's system engineering design team conducted these performance assessments, direct interactions and discussions took place between the repository designers and the PRA analysts. This resulted in a timely, clear, and iterative exchange of the often diverse concerns between the designers and the PRA analysts. The insights developed during these exchanges provided invaluable and immediate feedback to both the designers and the PRA analysts, producing improved facility designs that satisfy design requirements and performance objectives of the NRC, DOE, EPA as well as other regulatory and contracting organizations. This enhancement of the facility design's safety was accomplished with minimal cost and schedule impacts because it was initiated at the conceptual design stage. The two specific examples of the potential cask drop and the potential unsealed container drop discussed above demonstrate how this performance assessment process is being effectively implemented in complex design projects.

When performance assessments and PRA analyses are done by organizations or individuals physically separated from the repository design team, time delays occur due to communication and documentation requirements. These time delays may impact the completion schedule for the PRA analysts and can result in the analysts not obtaining and utilizing current facility design details. These factors generate additional obstacles to the efficient and timely implementation of design modifications and of the provision of direct feedback to the facility designers. These obstacles were removed in the conceptual design of the repository because the PRA analysts were physically located with the design team. The assessments were done as a fully coordinated effort within the same design organization and as part of the actual design process.

By using the performance assessment PRA techniques, the facility risks for accident conditions can be quantified in a consistent manner starting at the conceptual design stage. In principle, the same techniques can be continued through all subsequent stages of project design and development. Additional innovative methods and approaches for applying PRA techniques will require development in the subsequent stages of repository design due to the more complex design details and fast moving production schedules that occur as the design progresses toward completion. Comparisons of the PRA results determine which operations and design concepts appear to be the greater risks and which are the major contributors to risk. These analyses and comparisons provide a sound data base that can be used by various decision makers in the design process to initiate design modifications that reduce the facility risks and improve the safety of the operating facility. This can be achieved using the iterative feedback design process illustrated in Fig. 1.

## REFERENCES

1. U.S. Department of Energy, "Generic Requirements for a Mined Geologic Disposal System," DOE/NE/44301-1, September 1984.

2. H. R. MacDougall, Compiler "Draft-Site Characterization Plan Conceptual Design Report," SAND84-2641, November 1986.

3. L. J. Jardine, C. W. Ma, R. C. Sit and R. Donahue, "Preliminary Preclosure Safety Analysis for a Prospective Yucca Mountain Repository," Proceedings of Waste Management '87, March 1987.

4. H. R. MacDougall, Compiler "Draft-Site Characterization Plan Conceptual Design Report," SAND84-2641, "Appendix F - Preclosure Radiation Safety Analysis Study", November 1986.

5. U.S. Department of Energy, "Mission Plan for the Civilian Radioactive Waste Management Program," DOE/RW-0005, June 1985.

6. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, (NUREG-75/014), October 1975.

7. Office of Nuclear Regulatory Research, USRC, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, January 1983.