Bechtel Group, Inc.
Engineers-Constructors
Fifty Beale Street
San Francisco, CA 94105

Neil A. Norman, P.E.
Bechtel Fellow

October 6, 1989

Mr. Philip S. Justus, Ph.D.
Staff Geologist
U.S. Nuclear Regulatory Commission, 4H3
Washington, D.C. 20555

Dear Phil,

I enjoyed talking with you in Las Vegas. I have enclosed a paper which I presented in Japan in 1987 which discusses the strong need to see that performance assessment is an integral part of the facility design process and that the PA process is closely integrated with the design activity and not done elsewhere. I would be pleased to have your comments on my ideas.

Very truly yours,

Neil Norman

Neil A. Norman, P.E.

NAN:sb
Encl.

109-1
WM-1
NH01

1. THE USE OF PERFORMANCE ASSESSMENT IN THE DESIGN OF SPENT FUEL STORAGE AND HIGH-LEVEL WASTE REPOSITORY FACILITIES

Neil A. Norman, PE
Bechtel National, Inc.
San Francisco, California

Section 1

INTRODUCTION

The process of formal risk assessment and confidence analyses is a portion of the overall technology of systems engineering. In order to provide a clear understanding of performance assessment and confidence analyses related to high-level nuclear waste management applications, I will present a brief description of the systems engineering process and the techniques that we are applying to reduce risks.

Because of prior successful U.S. experience in the application of systems engineering techniques to large, complex, multi-participant programs, the DOE has elected to apply the systems engineering process to the U.S. High-Level Nuclear Waste Management Program.

The U.S. HLNWMP must develop an integrated system that meets the complex national and international needs for safe long-term disposal of spent fuel from over 100 commercial nuclear power reactors as well as defense HLW.[1]

The processes of risk assessment and consequence analysis can be used during facility design to permit early modifications to reduce risk. Costs for this activity are minimized by interative application for the preconceptual design phase onward.

By using the risk assessment techniques early, before the design is in great detail, a more effective performance is achieved at a lower design cost.

Section 2

THE SYSTEMS ENGINEERING PROCESS

Many detailed working documents describe specific applications for the systems engineering process, but the brief implementing circular No. A-109[2], issued by the U.S. Office of Management and Budget in 1976, provides a useful introduction and describes several steps in the process, i.e.:

- Identify alternative designs
- Perform trade-off studies (capability, schedule, cost)
- Evaluate and test alternatives
- Select a system
- Proceed with full-scale development

Implementation of this process has led to the development of training programs for U.S. Government program and procurement managers. The "Systems Engineering Management Guide" presents useful systems engineering techniques which apply equally to the HLW program. "Although programs differ in underlying requirements, there is a consistent, logical process for best accomplishing system design tasks. Figure 1-1 (graphically) illustrates the activities of the basic systems engineering process."[3] Figure 1-1 from the original appears as Figure 2-1 on the following page.

The iterative nature of the systems engineering process is shown in Figure 2-1. This process is sometimes implemented without due consideration of the necessary iterations of design development. Multiple alternatives must be available to permit design optimization. Some additional potential alternatives will be discovered in the function analysis, synthesis, and evaluation steps. When another way of satisfying mission needs or reducing risk is discovered, a change should be considered in the requirements, function analysis, or synthesis phase, and the systems engineering steps should be repeated. This iteration is especially productive early in the design or site evaluation phase because changes can be made early without major cost or schedule impacts.

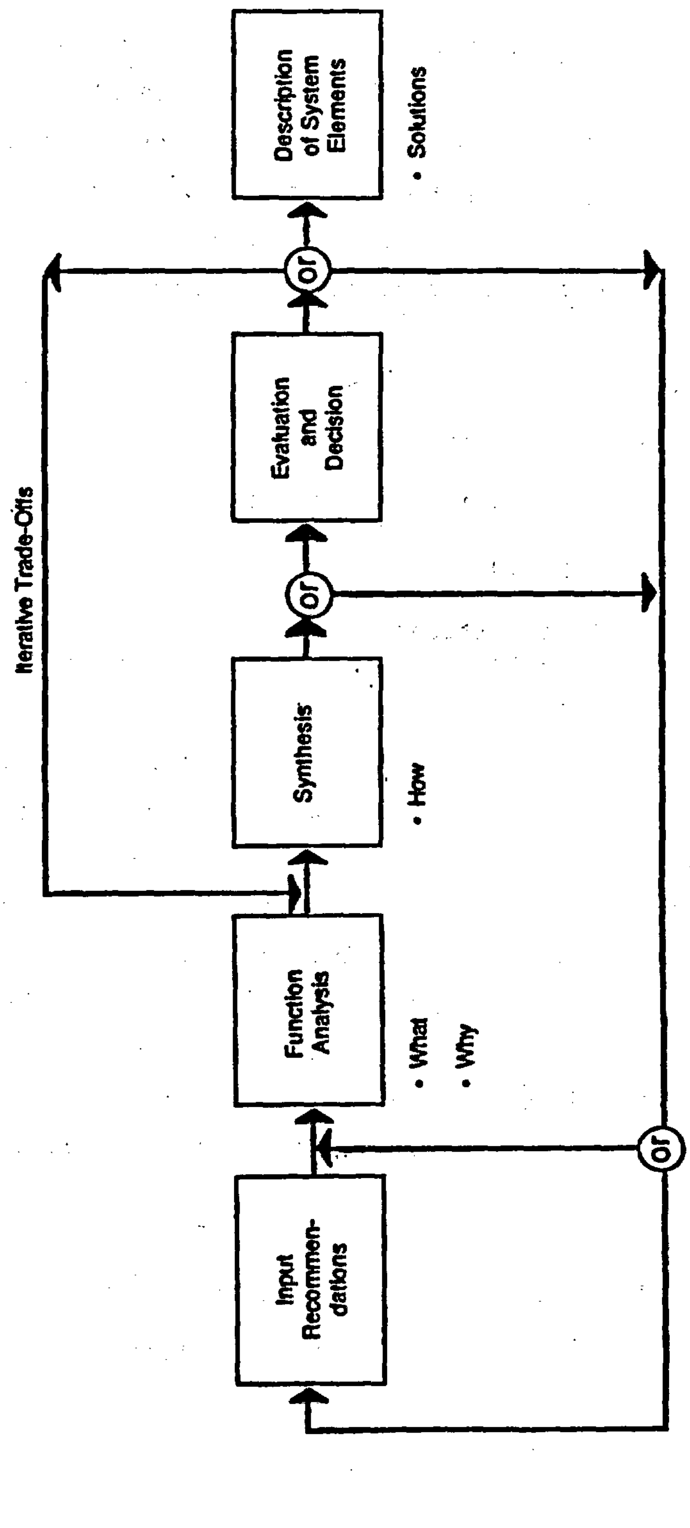


Figure 2-1 The System Engineering Process

Section 3

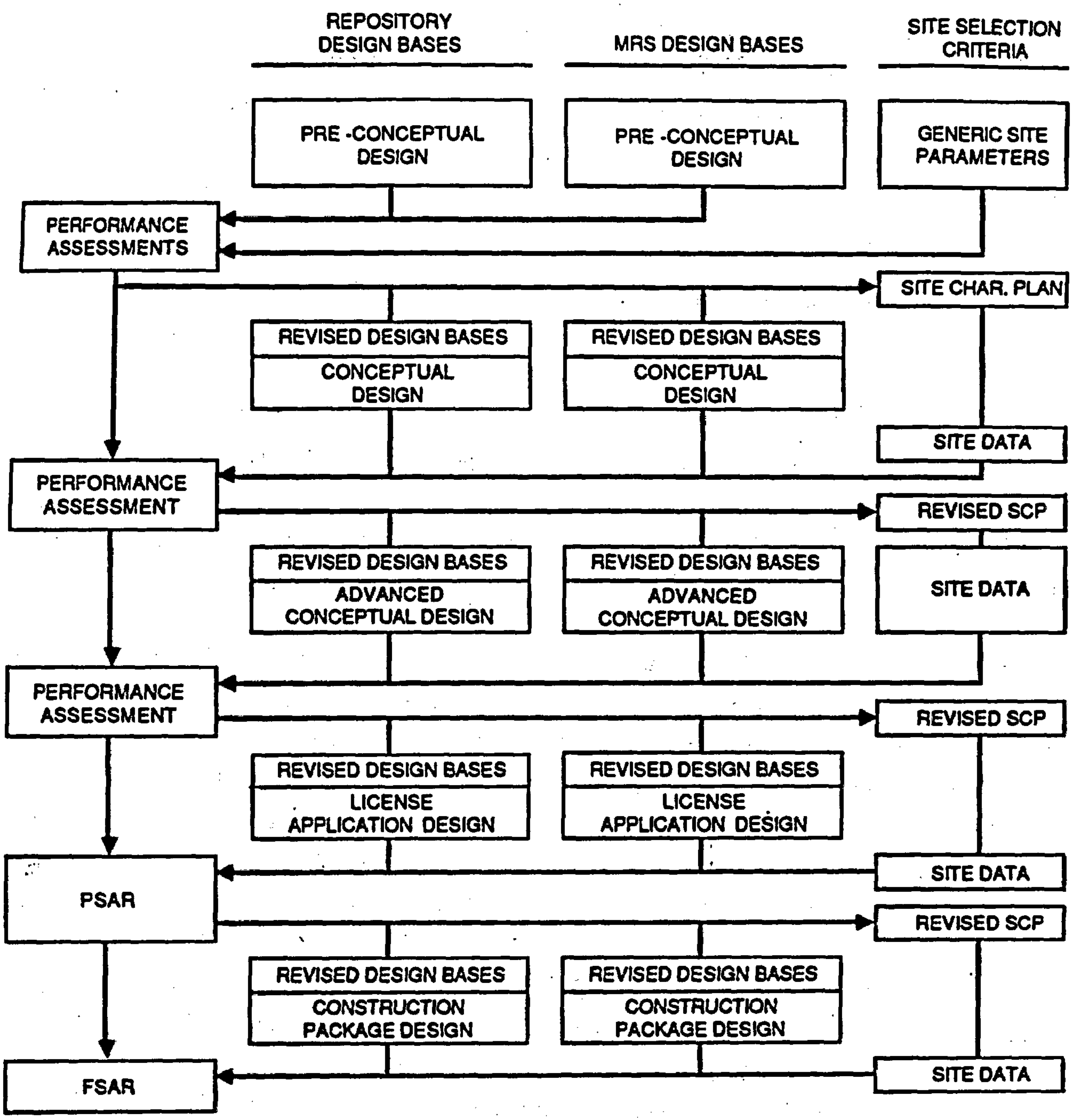
APPLICATION OF SYSTEMS ENGINEERING TO FACILITY DESIGN

We are applying the systems engineering process to our design activity at Bechtel for a number of clients. In the unique application that I will present here, system performance is used as the measure of the acceptability of a design alternative. Figure 3-1 notes high-level waste repository design basis across the top, and increasingly more detailed phases of design down the left side. Repository and monitored retrievable storage (MRS) design bases for the repository are derived from DOE interpretation of numerous regulatory documents.* Design requirements prepared from these sources, along with known or generic site parameters, are used to prepare the design bases. At the conceptual design phase, site data may be available, but are not detailed. From the bases, a performance-driven system design process can be implemented:

- Prepare design alternatives
- Assess performance
- Reevaluate alternatives and design bases and revise design to eliminate unacceptable consequences

Performing probabilistic risk assessments (PRAs) during conceptual design requires an innovative application of PRA techniques due to incomplete and soft design details at the conceptual level. In the scenario development and FMEA activites, when the engineering design team conducts these analyses, there can be direct interactions and discussions between the facility design specialists and the PRA analysts on the team. The result is a timely and iterative exchange of the often diverse concerns between the design specialists and the PRA analysts. The insights developed during these exchanges provide valuable and immediate feedback to the design specialists

*10CFR60, 10CFR72, 40CRF191; Department of Transportation acceptable routes and transportation impacts; and state, tribal, and local regulations



NOMENCLATURE	
SCP	SITE CHARACTERIZATION PLAN
PSAR	PRELIM. SAFETY ANALYSIS REPORT
FSAR	FINAL SAFETY ANALYSIS REPORT

Figure 3-1 U.S. HIGH -LEVEL WASTE MANAGEMENT PROGRAM - PERFORMANCE DRIVEN HIGH -LEVEL WASTE MANAGEMENT CRITERIA

and PRA analysts for improving and enhancing facility designs. This enhancement of facility design can be accomplished with minimal cost and schedule impacts when it is initiated at the conceptual level.

The performance assessment process can be described in five steps:

- o Systems modeling and analyses
- o Radioactive release analyses
- o Dose consequence analyses
- o Regulatory compliance assessment
- o Modify model or requirements and repeat the process

These key steps in the performance assessment and consequence analysis process require different types of skills.

Since the foundation of modern probability theory by Pascal and Fermat in the 17th century, analysts have strived to apply the classical numerical processes to the scenario development as well as to the analytical process. In monetary risk applications, Cramer and Bernoulli(4) hypothesized a "utility" of wealth function, which attempted to explain why two individuals would accept different monetary risks based on their relative wealth. In a recent paper, Machina(5) has explained the application of the "utility" model to other than monetary risks. In studies, so-called "risk averse" and "risk preferring" individuals have been found to change their preference given subsequent choices. The results have led to an apparent inability of the classical numerical processes to define behavior when complex human motivations and differing levels of knowledge exist. The development of scenarios for failures of systems, structures, and components can include considerations of human behavior, perceptions, politial motivations, etc., which make the scenario development not presently amenable to a pure mathematical solution. Table 3-1 provides a 1983 IAEA list of potential phenomena which could provide initiating events for failure scenarios. This first step in the analysis process must, depending on the scenario complexity, often be developed from a deterministic rather than a probabilistic approach.

Table 3-1

IAEA LIST OF PHENOMENA POTENTIALLY RELEVANT
TO SCENARIOS FOR WASTE REPOSITORIES

Natural Processes and Events

Climatic change
Hydrology change
Sea-level change
Denudation
Stream erosion
Glacial erosion
Flooding
Sedimentation
Diagenesis
Diapirism
Faulting/seismicity
Geochemical changes
Fluid interactions
- o Groundwater flow
- o Dissolution
- o Brine pockets

Uplift/subsidence
- o Orogenic
- o Epeirogenic
- o Isostatic

Undetected features
- o Faults, shear zones
- o Breccia pipes
- o Lava tubes
- o Intrusive dikes
- o Gas or brine pockets

Magmatic activity
- o Intrusive
- o Extrusive

Meteorite

Human Activities

Faulty design
- o Shaft seal failure
- o Exploration borehole seal failure

Faulty operation
- o Faulty waste emplacement

Transport agent introduction
- o Irrigation
- o Reservoirs
- o Intentional artificial groundwater recharge or withdrawal
- o Chemical liquid waste disposal

Large-scale alteration of hydrology

Undetected past intrusion
- o Undiscovered boreholes
- o Mine shafts

Inadvertent future intrusion
- o Exploratory drilling
- o Archaeological exhumation
- o Resource mining (mineral, water, hydrocarbon, geothermal, salt, etc.)

Intentional intrusion
- o War
- o Sabotage
- o Waste recovery

Climate control

Waste and Repository Effects

Thermal effects
- o Differential elastic response
- o Nonelastic response
- o Fluid pressure, density, viscosity changes
- o Fluid migration

Mechanical effects
- o Canister movement
- o Local fracturing

Chemical effects
- o Corrosion
- o Waste package - rock interactions
- o Gas generation
- o Geochemical alterations

Radiological effects
- o Material property changes
- o Radiolysis
- o Decay-product gas generation
- o Nuclear criticality

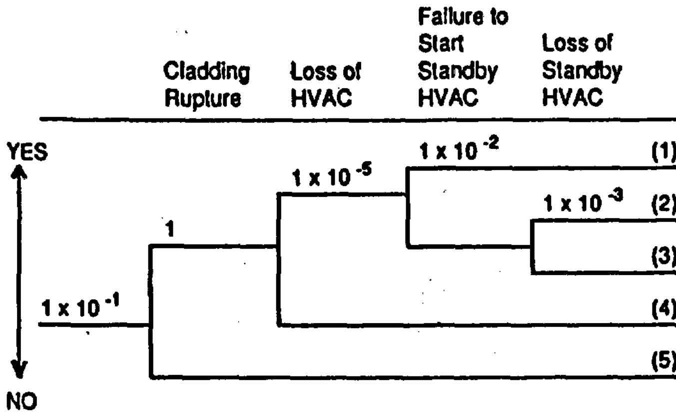
The Delphi Process[6] brings diverse and experienced specialists together to develop the failure scenario and to "judgmentally" assign failure probabilities to the processes and events leading to a health consequence.

If the failure scenario and failure modes and effects analyses are performed by the skilled PRA analysts instead the highly experienced design specialists, the risks and consequences may be classically and correctly presented but with erroneous results because of false or overly conservative initial assumptions.

If PRA analyses are done by organizations or individuals physically separated from the facility design team, time delays and misunderstandings due to communication and documentation requirements occur. Time delays and misunderstandings can result in the analyses not utilizing current facility design details, leading to obsolete or incorrect conclusions. The result is a greater impact on risk of failure, project cost, and schedule than if the PRA and consequence analyses were done as a coordinated effort within the same organization and as part of the actual design process.

Preliminary site-specific and facility design-specific preclosure radiological safety analyses have been performed for high-level waste repository cases using a reference conceptual design. A Delphi Process approach was used to develop accident scenarios and system, structure, or component failure probabilities, which could result in offsite releases of radioactive materials. For these scenarios, numerical dose consequences for the maximum exposure to an individual located offsite and the numerical frequencies or probabilities of occurrence were estimated. The models developed in the PRA analyses can be used to provide sound, systematic and rational bases for evaluating alternative design changes and for identifying R&D needs to support licensing activities. Figure 3-2 shows a sample event tree developed by Bechtel using this process. The development and use of these methods is discussed in more detail in Reference 6.

By using the models, the facility risks can be quantified relatively and in a consistent manner starting at the conceptual design level and continuing through all future phases of design development. Analyses of the results determine



Sequence	Probability (Year⁻¹)	Dose (mrem) Kr85	Particulates GAP	Particulates Pulv.	Total
(1)	1(-8)	7.4(-2)	4.1(+1)	6.3(+1)	1.1(+2)
(2)	1(-9)	7.4(-2)	4.1(+1)	6.3(+1)	1.1(+2)
(3)	1(-6)	7.4(-2)	4.1(-3)	1.4(-1)	2.2(-1)
(4)	1(-1)	7.4(-2)	4.1(-3)	1.2(-1)	2.2(-1)
(5)	0.0	0.0	0.0	0.0	0.0

Figure 3-2 Event Tree for the Crane Dropping a Fuel Assembly in the Unloading Hot Cell

which risks appear to be greater and what scenarios are the major contributors to risk. These analyses and information provide a sound data base to be used by various decision makers. These enable the designer to direct attention to the items that contribute most to the facility risks and safety consequences.

Figures 3-3 and 3-4 provide simplified logic diagrams for a preclosure and a postclosure incident.

It is vital to the process to use the most realistic value for each site or design parameter, not an assumed conservative value. Use of conservative values for performance analyses will compound conservatism on conservatism and result in an erroneous answer. The use of sensitivity analyses after the initial calculation of performance will be meaningless if the performance result has been made erroneous by conservative assumptions.

The sensitivity analysis process can be briefly described:

- After performance risks have been calculated, select a new (higher or lower) value for a single parameter, such as seismic ground motion value.
- Redo the performance calculation to determine the sensitivity to the variable parameter.
- Repeat for multiple values of parameters of interest.
- If the change does not affect the performance unacceptably, then the level of accuracy for the parameter need not be determined with great accuracy.
- Unacceptable risks resulting from a changed parameter will show the need for either more accurate definition of the parameter or design change to mitigate the fault leading to the risk.

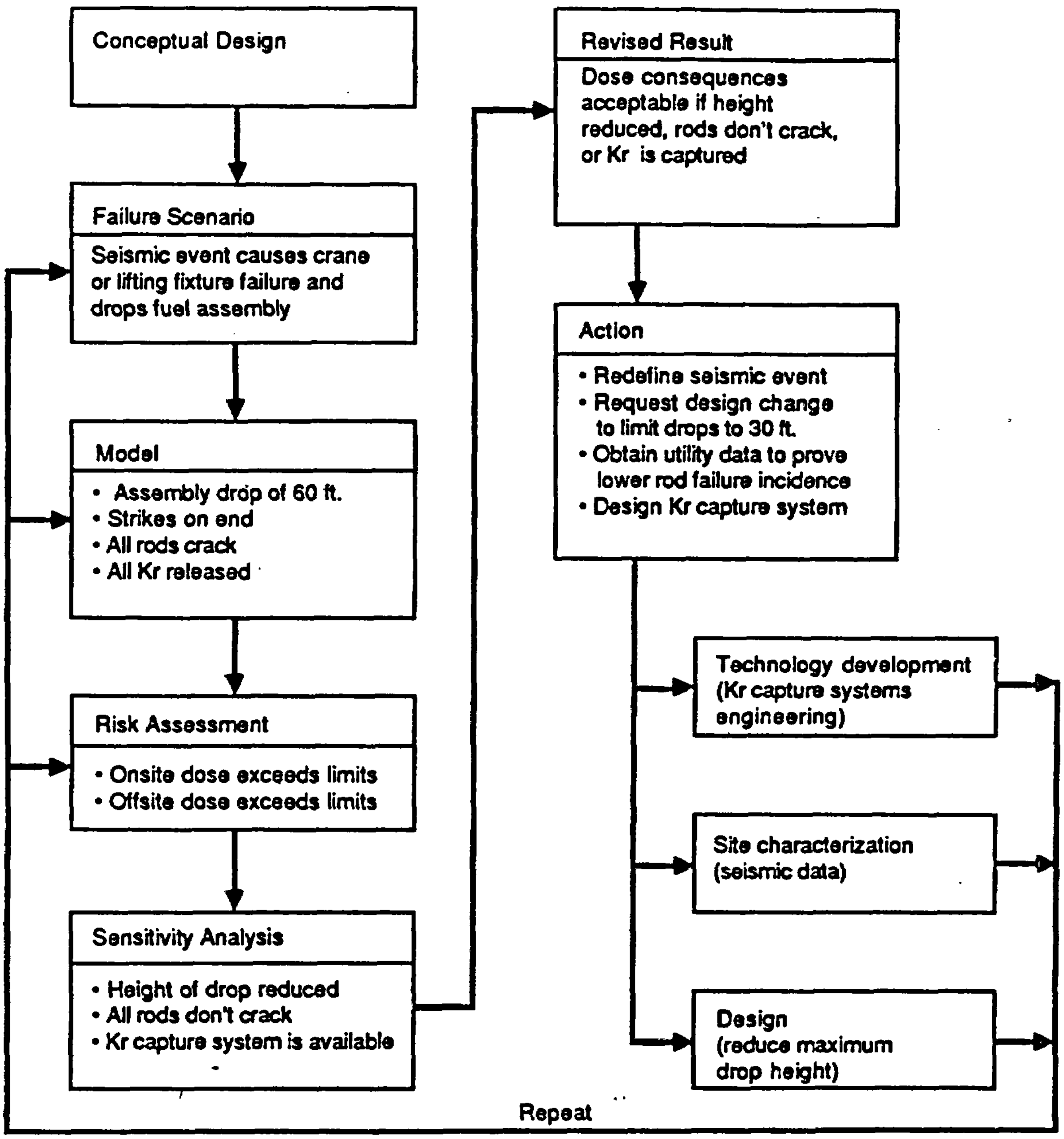


Figure 3-3 Performance Assessment Scenario: Preclosure Incident

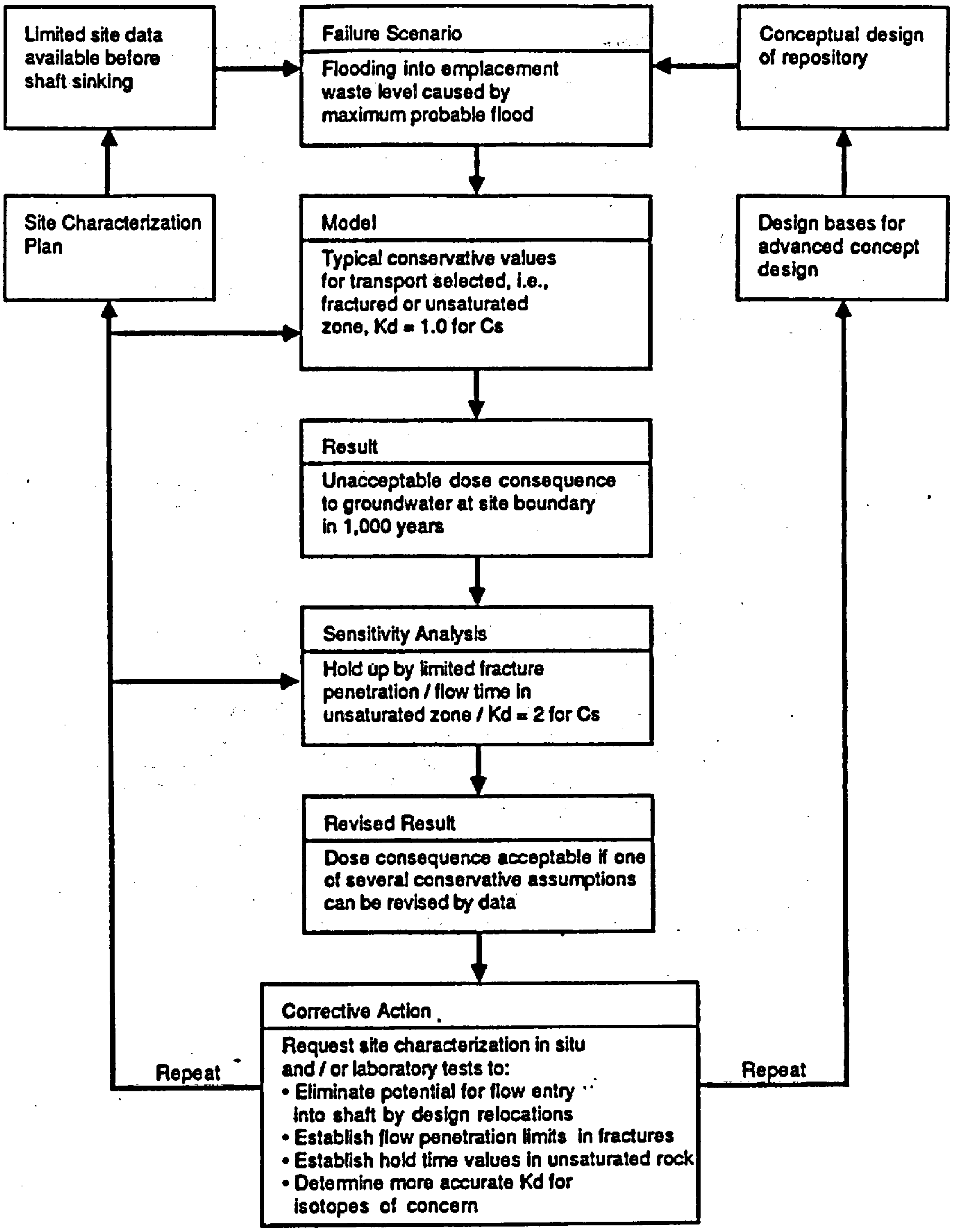


Figure 3-4 Performance Assessment Scenario: Postclosure Incident

A PRA methodology from the U.S. Nuclear Regulatory Commission (NRC)[7] was used for the recent Bechtel analyses. Use of the integrated design and risk assessment team was unique and highly successful.

The site characterization portion of the U.S. program is very extensive. Hundreds of scientists and engineers are required for the collection and analysis of data. But, which data are required? The process just described will function equally well to optimize the site characterization process by performing the following steps:

- Prepare a Site Characterization Plan.
- Implement the conceptual phase and collect data.
- Use the site data along with the conceptual design in a PRA or deterministic performance analysis to determine risks or consequences of the selected design alternate on the selected site.
- Perform multiple sensitivity analyses for key site data values to determine how significantly performance is affected by uncertainties in specific site data parameters.
- Review the site characterization plan to focus on the collection of the sensitive site parameters during the succeeding phase of site characterization and eliminate data collection for parameters where the existing level of detail is adequate to demonstrate the system performance.

Such an integrated systems approach in the site characterization process will also reduce overall system risk as well as cost.

Section 4

CONCLUSION

The system integration process is an iterative one. The optimization of each subsystem in any system will not equate to the optimization of the total system. If the overall system management controls are permitted to accept alternative solution evaluations for subsystems, the technical result will approach closer to an optimum for the overall system. Repository site selection criteria and design bases in the U.S. are controlled by the EPA criteria of 40CFR191, the NWPA of 1982, the NRC regulation procedure of 10CFR60 for the repository and 10CFR72 for the MRS, plus others. There are, however, significant latitudes permitted in the design bases developed from these laws. Utility and transportation components operate under other codes including 10CFR50, 10CFR71, 10CFR20, 49CFR173, and 49CFR178. These, too, permit some implementing latitude. As site selection and characterization proceeds and MRS and repository designs become better defined, it is necessary that the site data and design configuration be assessed at each design level and changes be made in the subsystems to optimize the overall system and reduce risk.

By integrating the performance assessment discipline into the design team, we have significantly facilitated the feedback process both in terms of time and dollars. This closely integrated process also reduces the rejection rate of new ideas because the ideas for corrective action are created within the design team. The result, within the systems engineering process, should be a safer facility. This integration concept can be extended to the site characterization process as well.

Such early and repeated performance assessments will not only permit improvements of the design, or site characterization plans, but will also provide recommendation for changes or standardization of utility fuel management practices, cask design, transportation practices, and higher level system requirements which will improve the overall high-level waste management performance. When it can be shown that overall final disposal safety can be improved by utility or transportation actions, storage or transportation cost allowances may be allocated to utilities or transportation companies to make the changes. This close examination of the overall system performance and corrective feedback between system components will be necessary to provide an optimum and an operable system.

REFERENCES

1. Nuclear Waste Policy Act of 1982, 42USC10101, Public Law 97-425.

2. Executive Office of the President, Office of Management and Budget, Washington, DC., Circular No. A-109, April 5, 1976.

3. Defense Systems Management College, "Systems Engineering Management Guide," Second Edition, December, 1986.

4. G. Cramer, correspondence to N. Bernoulli (1728), and D. Bernoulli, Comment Acad. Sci. Imp. Petropolitanae 5, 175 (1738) [English translations Econometrica 22, 23 (1954)].

5. M. L. Machina, U.C. San Diego, "Decision-Making in the Presence of Risk," Science, May 1, 1987, Article No. 537.

6. B. Ross, Disposal Safety Inc., "Radioactive Waste Management and the Nuclear Fuel Cycle," March 1986, Scenarios in Performance Assessment of High Level Waste Repositories.

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

8. L. Jardine, "Utilization of Probabilistic Risk Assessment to Guide Conceptual Designs of a Repository," Proceedings Waste Management 87, Vol. II, Pg. 27, University of Arizona, Tucson.