A METHODOLOGY FOR HIGH-LEVEL WASTE SYSTEMS SAFETY ANALYSIS IN THE PRECLOSURE PHASE*

P. A. Harris, D. M. Ligon, and M. G. Stamatelatos
GA Technologies, Inc.
San Diego, California 92121

N. R. Ortiz and M. S. Chu
Sandia National Laboratories
Albuquerque, New Mexico 87185

ABSTRACT

A systematic methodology has been assembled to assess the safety of high-level waste repositories during the preclosure phase. The methodology can be used to identify and quantitatively rank structures, components, systems, and operations that are important to safety. Results from the first of the three project phases are reported, along with preliminary conclusions available to date.

INTRODUCTION

The Department of Energy (DOE) has been expending considerable effort, in recent years, developing conceptual designs for high-level waste (HLW) repositories in geologic media. The Nuclear Regulatory Commission (NRC), which is responsible for the licensing of the repositories, is involved in the review and evaluations of the conceptual designs. It is the intent of this project to provide NRC with a systematic methodology suitable for the identification and quantitative ranking of the structures, components, systems, and operations important to safety. The methodology will also help to assess compliance with the operational phase standards (10CFR60, 10CFR20, and 40CFR190) by estimating the potential releases of radionuclides to the public.

The development of a tool of this nature could use techniques from existing probabilistic risk and safety assessments. Several analyses addressing these areas for the preclosure phase are currently available, and a literature review of these studies has been performed and documented.[1] Therefore, one of the prime project objectives was to build on this existing body of information using currently available accepted techniques wherever possible.

This project has emphasized the preclosure phase of the repository to concentrate on operations involving the receipt, examination, preparation, and emplacement of commercial high-level waste. Retrieval was also examined, with the goal of characterizing the incremental risk. The option for retrieval of emplaced waste is currently required by NRC regulation (10CFR60). Retrieval must remain a valid option until such time as the NRC is satisfied as to the likely success of the isolation process. Other risk analyses have been performed to examine long-term risk following closure of the facility;[2] no examination of post-closure risk was attempted in this analysis other than the consideration of immediate and delayed retrieval.

The project has been divided into three phases: assembly and integration of existing methods, demonstration of the methodology using a sample problem and finally the complete analysis of a basalt repository. The first phase has been completed and documented.[3] The next section provides an overview of the entire project, including both completed and future tasks. The subsequent section addresses the tasks completed to date. The final section presents the conclusions available at this time.

PROJECT OVERVIEW

Characterization of risk due to facility operation requires identification of the potential accidents and their consequences. An accident scenario contains three components: the initiating event, the interaction with additional facility systems that could influence the course of that event, and the consequences that could be expected if the accident were to progress unchecked. The spectrum of all plausible accident scenarios with consequences detrimental to public health and safety define the contribution of the facility to overall societal risk. Determination of this body of accident scenarios, representation in terms of a quantifiable set of logic models, and acquisition of the data base necessary for quantification are the major tasks of the characterization of risk.

Within this framework several specific results are required. A literature review[1] was performed to assemble previous repository studies, repository design concepts, applicable probabilistic risk assessment methodology, important ranking methods, and data for initiating event frequencies, component failure rates, etc. This information was used to guide the direction for the remainder of the project.

Given a conceptual repository design, all initiating events potentially capable of causing consequences of concern to public health and safety must be identified. They must be screened on a preliminary basis to remove obviously insignificant contributors, and then developed into accident *scenarios by coupling* the interaction of all plant systems potentially capable of influencing the outcome of that initiating event. The type of logic models (e.g., event trees, fault trees) must be selected to suitably represent these accident scenarios in a numerically quantifiable form.

*This work supported by the United States Nuclear Regulatory Commission and performed at Sandia National Laboratories which is operated for the U.S. Department of Energy Under Contract Number DE-AC04-76DP00789.

Each system identified in an accident scenario as capable of influencing event outcome must then be assigned a failure probability based on the expected behavior of that system. Systems described in sufficient detail from the conceptual design can be modeled explicitly by several different techniques. Other systems (such as support systems) that are identified but not described in detail must be assigned a failure probability based on the performance of similar systems.

The consequence of each particular accident sequence must be linked together into categories of similar risk level. Accident sequences containing similar consequence categories can be assembled into groups contributing to the same consequences category. The sequences in each category can then be treated as the contributors to that level of risk.

The tasks outlined above describe the modeling of the conceptual facility design through the development of equivalent logic models. This is a fairly straight-forward application of existing risk assessment techniques. There are several additional requirements for this analysis that are not amenable to a standard approach. The need to prioritize the contribution of systems, components, and operations to each category of risk requires some measure of importance for each component in each system and subsequently each system in each accident scenario. It has been proven that human error is a major concern in activities and operations that require human handling;[4] therefore, human interaction at both the component and system level must be included to obtain a representative picture. Finally, uncertainty in the data must be reflected in the overall estimation of risk in each category, and the sensitivity of the numerical value to different component or system values must be examined. Techniques for obtaining these results must be integrated into the structure of the risk assessment.

Completion of the logic models and preliminary numerical evaluation will be followed by consideration of common cause failures. This can alter both system failure probabilities and accident sequence frequencies by recognition that failures in some systems can cause failures in other systems previously assumed to be independent. A complete logic model of system interaction is required to identify subtle system interdependencies.

The assembly and integration of the information and selection of methods described above constitute the major accomplishments of the first phase of this project. The second phase will demonstrate the coupled methodology, using a sample problem consisting of a small subset of the accident sequences identified in the first phase. The sample problem will check the application of the assembled methods, in particular, the importance ranking scheme, on a tractable size problem. The sample problem will also illustrate the utility of prioritization for evaluation of proposed design changes. All of the features of the complete analytical technique will be used, including uncertainty, sensitivity, common cause evaluation, and contribution of human error. The small size of the problem will allow for hand checking of numerical results and rapid solution.

The third phase of the project will provide a characterization of risk for the basalt repository concept described in the "Conceptual Design Description, Nuclear Waste Repository in Basalt."[5] The entire facility will be examined using the latest design information available. A potential additional application may be considered if the NRC desires the evaluation of a design concept in alternate geologic media (i.e., bedded salt). Figure 1 provides a diagram of the overall methodology structure described above.

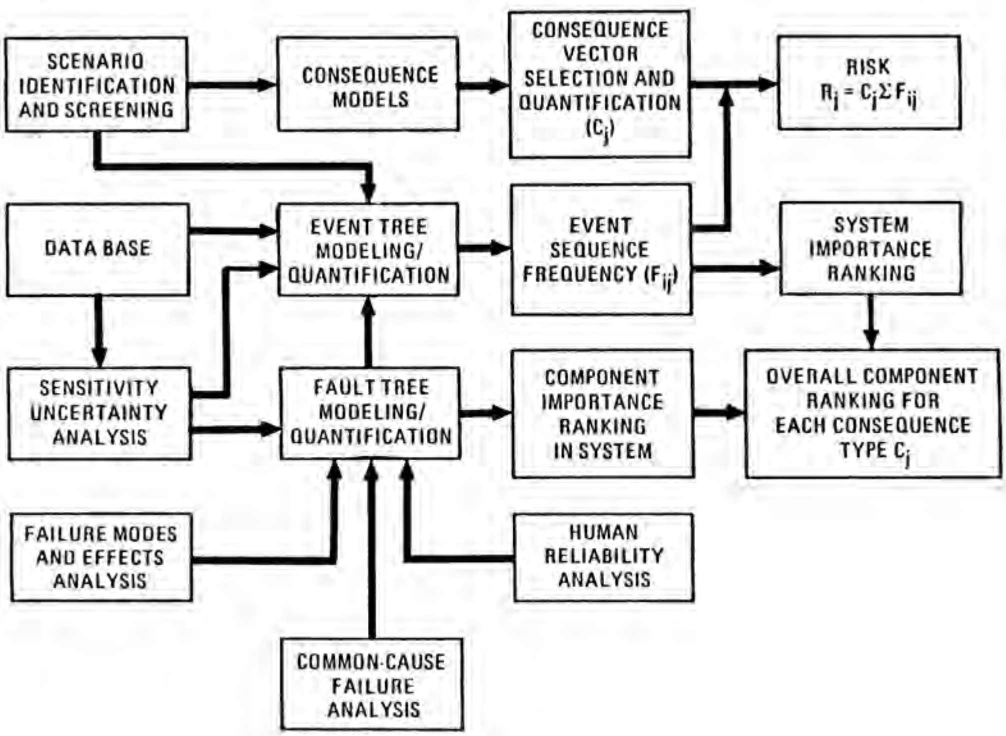

Fig. 1. Methodology for high-level preclosure safety systems analysis.

PROGRESS TO DATE

A detailed examination of material flow through a facility described in the basalt repository conceptual design was performed to determine the plausible accidents (initiating events) that could occur for all expected facility operations. Process flow diagrams specifying all individual operations required in every major facility area were developed.

Initiating events were subjected to an initial screening process used in a previous NRC study[6] for early elimination of insignificant contributors. An additional screening criterion was used from the draft EPA standard suggesting a lower credible occurrence frequency of 1.0E-08/year.[7] Initiating events surviving this screening process were developed into accident scenarios.

The combination of event and fault tree methodology was selected for construction of logic models to represent the spectrum of potential accidents. Event trees were used to simulate the interaction of various systems that could influence the outcome of an initiating event. Fault trees were used to model each individual system where sufficient information was available. Portions of fault trees from previous analyses[6,8,9] were incorporated where, system and function were similar. Additional detail identifying the contribution of human error was added to the trees.

Initially, several different consequence types were considered, including public radiological exposure, personnel radiological exposure, personnel non-radiological injury, loss of repository availability, financial impact, and compromise of long term repository performance. After identification of accident sequences contributing to each category only public and personnel radiological consequence categories were pursued, due to the limited time available before repository review by the NRC must commence. Several different consequence models for the initial release, transport, and movement into the open environment were identified. An existing method was modified to quantify the probable source term given drop of a spent fuel handling cask. Coupling of the accident sequences to the consequence types was performed by examining the immediate consequence (i.e., cask drop) to determine if the subsequent release and transport path posed a hazard to the public or to the operating personnel.

The potential for disruption of several systems in the facility and possible radiological release by natural and induced external events (earthquake, fire) was also considered. The vulnerability of each initiating event and intermediate event (system interaction) to disruption/damage by the external event was examined. Where this possibility existed, another accident sequence was created, specifying the external event as the accident initiator and identifying potentially degraded intermediate events.

Assembly of the logic models provided 100 accident sequences in consequence category 1 (public radiological exposure) for emplacement and 67 sequences in category 1 from retrieval considerations. One hundred and seven accident sequences were identified for category 2 (personnel radiological exposure) for emplacement and 58 sequences from retrieval. Sequences were determined for other consequence categories but all further attention was focused solely on radiological consequences.

Several importance measures[10] were evaluated for use in ranking risk contributors. The Fussel-Vesely measure was chosen as the best technique for consideration of not only dominant single contributors but also lower probability contributors that occur more than once.

Mining activities were examined to provide an estimate of initiating events that could be expected due to the repository environment and to better characterize equipment reliability. A mining consultant (Engineers International) was retained to provide additional expertise and locate the required data more rapidly.

The data required for logic model quantification can be divided into initiating event frequencies, component/system failure rates, and human error rates for tasks of varying complexity and stress level. Sources of initiating and external event frequency data include previous repository studies for waste process specific events, transportation accident statistics for switchyard, transporter, and other transportation related events; warehousing and shipping accident statistics for events addressing lifting and movement of heavy objects; and siting studies conducted for the environmental history of the intended repository site.

Primary component data sources will be the Nuclear Plant Reliability Data System (NPRDS)[11] and the Government Industry Data Exchange Program (GIDEP).[12] These two sources contain accumulated data histories for almost any conceivable component, including sample size and variance required for uncertainty calculations.

Human error rates can be estimated from the approach of Swain and Guttman developed at Sandia National Laboratories.[4] These error rate calculations will suffice for operations identified at both the individual system and system interaction levels.

With data from the above sources, uncertainty analysis can be performed using direct distribution sampling to provide a true estimate of top event (e.g., release of radioactive material to the public) uncertainty. A simple perturbation method was selected as adequate for performing sensitivity analysis given the complete logic models.

CONCLUSIONS

The first phase of this project was primarily devoted to gathering, sorting, and assembling information appropriate for a safety assessment of the preclosure operation of a HLW repository in basalt. Additional effort was expended to obtain methods for importance ranking, uncertainty/sensitivity analysis, and human error rate estimation that complemented the chosen logic structure and was consistent with available information.

Although only a preliminary analysis was performed in the first phase, enough detail from logic model development is now available to focus on several key areas of the basalt repository conceptual design. For example, the conceptual design calls only for standby exhaust filtration from the underground areas. Filters would be placed in exhaust fan trains only upon receipt of air activity alarms from underground monitors. Active switching of large fans and opening and closing of louvers that rely on long instrumentation leads is a potential problem. Further air circulation concerns arise from the redundant power available to exhaust systems but apparently not to air supply systems. Although the electrical distribution system is not delineated in sufficient detail to verify this, the available description does not address backup power to the supply units, and this should be tracked carefully as design matures.

Several accident sequences were identified as potentially capable of influencing long term repository performance. Handling accidents capable of denting or puncturing the storage canisters that might occur during transport to the underground emplacement area could go undetected without additional instrumentation or procedural precautions. Several automated operations involving moving the canister with hydraulic equipment, without direct visual contact either during or after movement, could allow dented or punctured canisters to be emplaced unknowingly. This could compromise the long term repository performance due to accelerated canister degradation.

The above examples are just some of the preliminary results obtained from completion of the first project phase. With the additional information available and the ability to quantitatively prioritize concerns, the NRC should have an analytical tool available to track repository design throughout the development phase to insure that the public health and safety are protected.

REFERENCES

1. D. M. Ligon, V. Hwa, and P. A. Harris, "Literature Review of Studies Related to the Safe and Permanent Disposal of Nuclear Wastes," GA-A17653, GA Technologies, Inc. (1984).

2. R. M. Cranwell, N. R. Ortiz, and G. E. Runkle, "A Methodology for Assessing the Risk from the Disposal of High-Level Radioactive Wastes in Deep Geologic Formations," SAND83-0465C, Sandia National Laboratories (1983).

3. P. A. Harris, D. M. Ligon, and M. G. Stamatelatos, "High-Level Waste Preclosure Systems Safety Analysis, Phase I Final Report," GA-A17670, GA Technologies, Inc. (to be published).

4. A. D. Swain and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations," NUREG/CR-1278, SAND80-0200, Sandia National Laboratories (1983).

5. J. M. Davis, "Conceptual System Design Description, Nuclear Waste Repository in Basalt," BWI-SD-005, 3 vols. Rockwell Hanford Operations (1983).

6. R. E. Pepping, et al, "Risk Analysis Methodology for Spent Fuel Repositories in Bedded Salt: Reference Repository Definition and Contributions from Handling Activities," NUREG/CR-1931, SAND81-0219, Sandia National Laboratories (1981)

7. "Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level And Transuramic Radioactive Wastes, Environmental Protection Agency 40CFR191," Federal Register, Vol. 47, No. 250 (1982).

8. "National Waste Terminal Storage Repository for Storing Reprocessing Wastes in a Dome Salt Formation, Conceptual Design Study No. 2, Accident Analysis," EY-77-C-05-5367, Stearns-Roger Engineering Company (1978).

9. "Preliminary Information Report for a Conceptual Reference Repository in a Deep Geologic Formation, Part 1 - Safety Analysis, Chapters 5 and 6," ONWI-121, Bechtel Group, Inc. (1981).

10. H. E. Lambert, "Fault Tree Analysis for Decision Making in Systems Analysis," UCRL-51829, Lawrence Livermore Laboratory (1975).

11. NPRDS, "Nuclear Plant Reliability Data System 1980 Annual Reports of Commulative System and Component Reliability," NUREG/CR-2232, Southwest Research Institute (1981).

12. Government Industry Data Exchange Program (GIDEP), Vol. 6 (1984).