USING QA CLASSIFICATION TO GUIDE DESIGN AND MANAGE RISK

John Lathrop
Strategic Insights
575 Los Altos Ave.
Los Altos, CA 94022
(415) 941-4950

Richard DeKlever
Raytheon Services Nevada
101 Convention Ctr Dr., Ste P280
Las Vegas, NV 89108
(702) 794-7592

Edgar H. Petrie*
Department of Energy
101 Convention Ctr. Dr., M/S 523
Las Vegas, NV 89109
(702) 794-7961

ABSTRACT

Raytheon Services Nevada has developed a classification process based on probabilistic risk assessment, using accident/impact scenarios for each system classified. Initial classification analyses were performed for the 20 systems of Package 1A of the Exploratory Studies Facility (ESF). The analyses demonstrated a solid, defensible methodological basis for classification which minimizes the use of direct engineering judgment. They provide guidance for ESF design and risk management through the identification of:

- the critical characteristics of each system that need to be controlled; and
- the parts of the information base that most need to be further developed through performance assessment or other efforts.

I. INTRODUCTION

The design of a system such as the Exploratory Studies Facility (ESF) presents a special risk management challenge. Ideally, the design of such a system should be guided by an overall, integrated probabilistic risk analysis that identifies the risks of the system and how each design feature affects that risk. Guidance from such an analysis can be used to revise the design and to select QA controls to achieve an appropriate level of risk. However in this case, different elements of the ESF system are designed separately and at different times. Parts of the system may become part of a potential repository, yet that repository has only been designed to a preliminary level.

The net effect is that, in the absence of an organizational structure to conduct an integrated probabilistic risk analysis, we must develop a means to manage risk that can be applied to a highly segmented system. Prudent, sound engineering judgment and practice are the primary means to manage that risk. Risk management judgment and practice can be in part proceduralized, supported and documented by classification, otherwise known as "determination of importance." Classification sorts the physical entities of the system into two categories: the Q-List and the Management Control List (MC-List). Things on the Q-List are subject to QA controls specified by the Quality Assurance Requirements Document (QARD).[1] Things on the MC-List are not required to have those controls, though those controls can be selected in any case.

The basis for classification is established in NUREG-1318.[2] That NUREG is interpreted for application by the Office of Civilian Radioactive Waste Management in the QARD, thence by DOE Administrative Procedure AP-6.17Q.[3] That procedure is then implemented at the participant level by a Raytheon Services Nevada (RSN) procedure entitled "Determination of Importance of Items and Activities".[4] In this paper we describe classification analyses performed by RSN on each of the twenty systems that make up Package 1A of the ESF, the initial facilities planned around the North Portal. Figure 1 presents a pictorial of the Exploratory Studies Facility, indicating the location of the North Portal. Figure 2 presents the general layout of the elements of Package 1A.

The focus of this paper is to present the results, insights and conclusions to be gained from the twenty RSN classification analyses. Eighteen of those analyses were still being reviewed and revised by the time design responsibility was transferred to the M&O organization.

*The authors would like to acknowledge the guidance and insight into many of the concepts presented in this paper from Durward I. Hulbert, TRW, Las Vegas, Nevada.

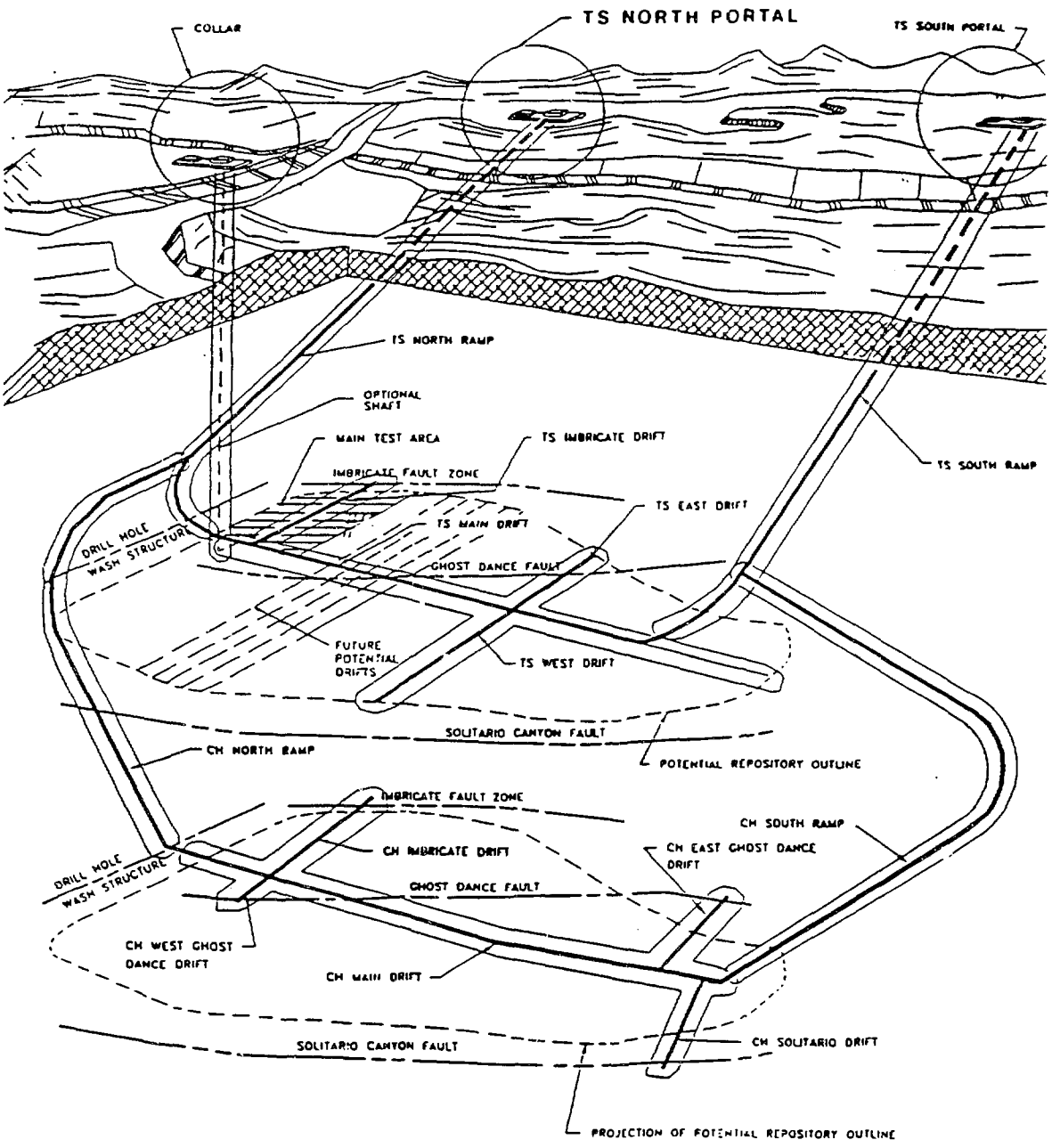

Figure 1 - Pictorial of the Exploratory Studies Facility at Yucca Mountain.

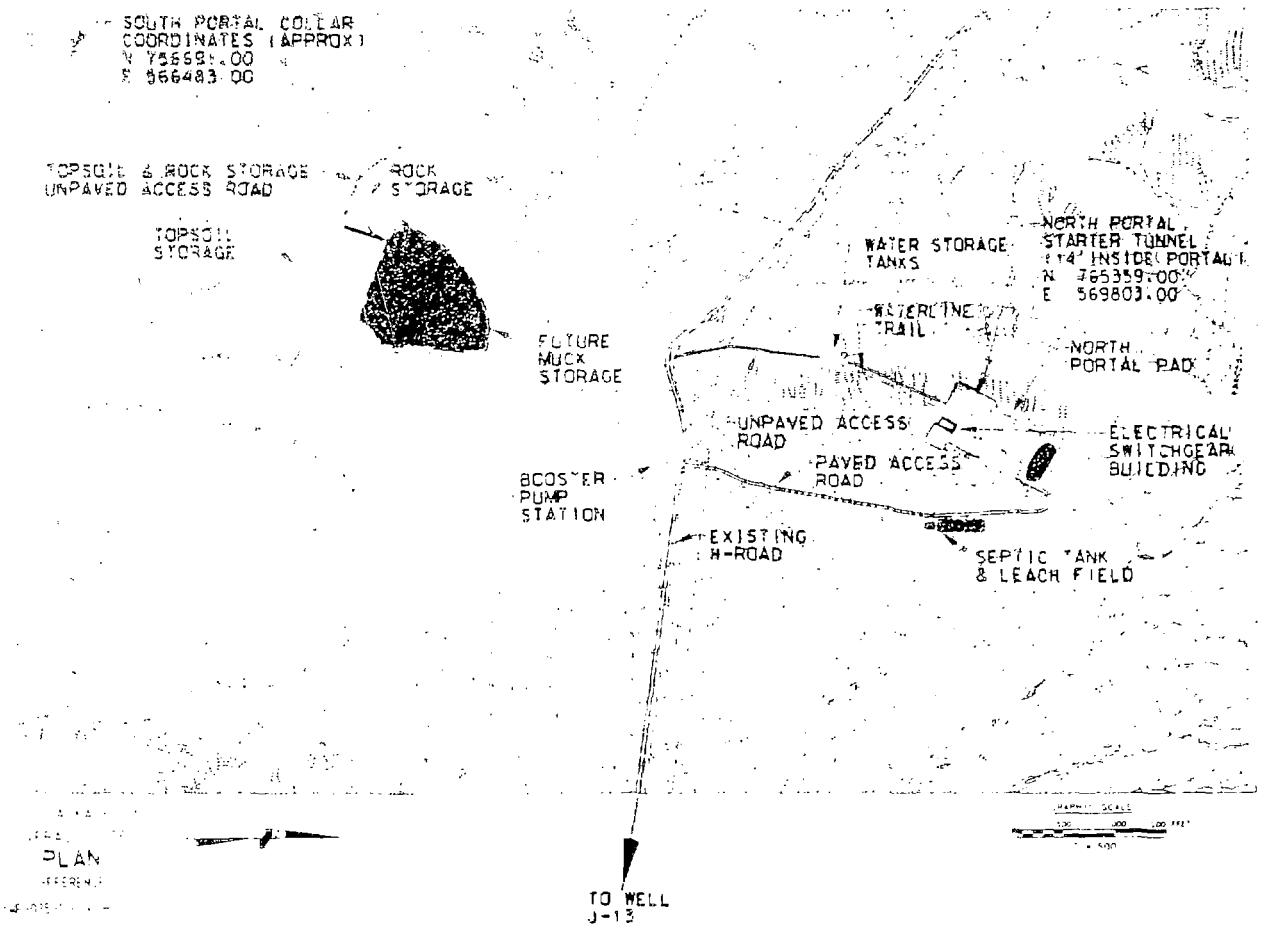

Figure 2 - Elements of ESF Package 1A

The corresponding eighteen classifications will be completed by the M&O.

The analyses had two immediate goals:

- to classify items and activities; and
- to guide selection of QA controls, a program that follows classification.

But there was another, broader purpose for performing these analyses: to answer the question "Can classification analyses applied separately to separate elements in a system perform system-wide risk management functions?" Those functions are to guide revision of the design and selection of QA controls to achieve an appropriate level of risk.

II. DESCRIPTION OF THE ANALYSES

Because we were the first ones to perform a classification for Yucca Mountain designed items, we had to develop a QA-approved procedure. In doing so, it was necessary to develop an expansion of the process outlined in AP-6.17Q to include:

- classification of ESF systems that will not be part of the potential repository, and so are not "items" and cannot be on the Yucca Mountain Project Q-List in the terminology of AP-6.17Q. In the RSN classification terminology, we call those systems "equipment" and classify them as being on the "EQ-List" or on the "EMC-List."
- classification of activities. Activities are not "items" and so cannot be on the Q-List in the terminology of AP-6.17Q. The procedure classifies activities that otherwise fulfill requirements for being on the Q-List, or impact Q or EQ systems, as "Special Activities" to be put on the "SA-List." Those activities

are identified in related specifications, which are design output documents. As such, classification of Special Activities is a derivative classification. That is, strictly speaking, a Special Activity does not have an inherent "importance," but derives its importance from the system it affects.

- specification of two types of "critical characteristics:"
  - critical characteristic(s) of a Q or EQ system: responsible for it being on the Q-List or EQ-List, and therefore subject to QARD controls; and
  - critical characteristic(s) of an MC or EMC system: could, if changed, cause the system to be placed on the Q-List or EQ-List, and therefore should be monitored to make sure they are not changed in that way.
- specification of suggested efforts which may enable a reduction in risk or change in classification, such as a design change to reduce a potential contamination risk, or seismic hazard research to see if a particular scenario is too unlikely to warrant concern.

These expansions are designed to make the best use of the information gained by conducting the classification analysis.

The classification analysis specified in AP-6.17Q calls for the identification of accident scenarios. It effectively also calls for the identification of impact scenarios, i.e., scenarios with consequences due to normal operations, not failures, such as infiltration from a sewage leach field. AP-6.17Q sets thresholds on the probability and consequence of an accident scenario such that, if both are met, the scenario is a "Q scenario." In our approach, if the scenario would be Q, except that it does not involve systems that could be part of a potential repository, and so does not involve "items" as defined in AP-6.17Q, we classify it as an "EQ scenario." If an item or activity is a significant element in a Q or EQ scenario, i.e., if it or its failure would:

- lead to a consequence exceeding the Q/EQ threshold, or
- cause the loss of the mitigation function of essential consequence-mitigating items, or
- initiate an event sequence resulting in a Q consequence if mitigating features are not considered,

then it is classified as:

- Q if it is an "item" (i.e., an element that would become part of a potential repository),
- EQ if it is "equipment" (i.e., an element that would not become part of a potential repository), or
- SA (for "special activity") if it is a Q-related activity.

AP-6.17Q specifies two types of Q Items:

- Items Important to Safety (ITS), relied upon to prevent or mitigate a ≥.5 rem dose to the boundary of the unrestricted area during the preclosure phase; and
- Items Important to Waste Isolation (ITWI), relied upon to meet the postclosure performance objectives of 10 CFR 60, Subpart E.[5]

We expanded the ITWI definitions of AP-6.17Q to deal with accident scenarios having ITWI consequences, and to reflect findings of our classification analyses. The expansions were largely a result of applying the analysis to the ESF (as opposed to a potential repository), which involved several cases where the impacts had to do with characterization, not actual isolation performance.

For clarity, we divided the concept of ITWI into two categories: Important to Isolation Performance (ITIP), for impacts where the actual ability to isolate wastes could be affected; and Important to Site Characterization (ITSC), for impacts which alter site characterization data, and so impair the ability to evaluate performance, which in turn impairs the ability to meet postclosure performance objectives. That is, ITSC impacts do not necessarily affect actual performance, but do affect our knowledge of that performance, and so affect our ability to meet postclosure performance objectives.

We found that there were accident scenarios associated with both ITIP and ITSC impacts. For an ITIP example, some accidents could cause water flows down faults or drifts that could possibly alter isolation performance. For an ITSC example, underground pipes could leak and alter site characterization data, and so possibly impair the ability to evaluate performance, which in turn could impair ability to meet postclosure performance objectives. We set probability and consequence thresholds for ITIP and ITSC accident and impact scenarios. Those thresholds are specified in Reference 4.

We found and resolved two key concerns with applying AP-6.17Q to classifying Package 1A systems:

Concern 1: Classifying elements by where they could be located, as opposed to where they are located in the current design.

The water storage tanks for Package 1A are located such that any leaks or catastrophic spills would not send water into any known faults or close to the portal. Therefore, in their current location the tanks would not be involved in any EQ scenarios and so would be classified EMC. Yet they could be relocated in such a

way that spills could flow down faults or into the portal, possibly causing Q consequences, and so would, if relocated in that way, be reclassified onto the EQ-List. There is a desire to classify elements by where they could be located (as opposed to where they are located in the current design), based on two lines of thought:

1. Where an element location can make the difference between being classified EQ or EMC, location can be considered a mitigating feature (See Concern 2 below). AP-6.17Q specifies that a mitigating feature cannot be taken into account in classification.
2. There is a desire to use the EQ-List to track EMC items and flag characteristics of those items, when changes in those characteristics could make the item EQ. The EQ-List is to be used, by this reasoning, as a way to apply special change controls to engineered mitigating features.

We accounted for this by including "relocation scenarios" in the analysis. That is, in addition to accident scenarios involving elements where they are currently located, where called for, relocation scenarios are used to analyze the risk involved if particular elements are located in worst-case locations. In the above example, then, the classification analysis of the tanks included an EQ relocation scenario with the tanks above the portal. Therefore the tanks are EQ.

Concern 2: The combination of a broad definition of mitigating features and not being able to account for the effects of those features in classification.

As already mentioned, AP-6.17Q specifies that the probability- or consequence-reducing effects of a mitigating feature cannot be accounted for in determining whether or not a scenario is Q or EQ. That is, scenarios must be evaluated as if all mitigating features have no effect. We adopted a broad definition of mitigating feature: any engineered feature that has an effect of reducing the probability or consequence of a classification accident/impact scenario. We accounted for this by including "redesign scenarios" in the analysis. That is, in addition to accident scenarios that assume the element being classified is built as currently designed, where called for, redesign scenarios are used to analyze the risk involved if the element is redesigned such that all mitigating features have no effect.

One effect of this definition of mitigating feature can be most clearly presented with an example. Two features in Package 1A work together to prevent precipitation from entering the portal: The pad (the excavated, filled and graded base for ESF facilities and operations at the North Portal) slopes downward away from the portal, and the floor of the starter tunnel has a vertical curve that keeps that slope going upward until well inside the tunnel. By our definitions, the pad slope and tunnel vertical curve are mitigating features. Therefore we cannot classify systems based upon the mitigating functions of those features, and we have to suppose, in a redesign scenario, that the pad could be sloped the wrong way and the vertical curve could be redesigned out of existence, resulting in the pad funneling stormwater into the access drift. Therefore while in any ordinary probabilistic analysis there may not be a credible scenario involving precipitation water entering the access drift, in this case by our definitions and procedures the scenario is Q (not EQ, since the floor vertical curve may become a part of a potential repository). The intent of this logic is to flag design features that could be important so that they can be appropriately controlled. In this case that means that the pad slope and floor vertical curve will be subject to QARD controls.

The combination of not being able to account for the effects of mitigating features in classification, and the broad definition of those features, results in an analysis that may in some cases be dominated by deterministic effects. In the above example, it might be sensible to assign some probability to the pad being accidentally sloped the wrong way, and another probability to the floor vertical curve being changed. We would then analyze the scenario to see if its probability and consequence both exceeded Q thresholds, and classify accordingly. But with the definitions and procedures used here, the pad slope and vertical curve both effectively get set into worst-case configurations with a 100% probability. This could lead to classification analyses flagging many elements as Q or EQ which in fact generate no significant risk other than the potential for an in-process construction change.

III. RESULTS

Classification analyses were performed by RSN on each of the twenty systems that comprise Package 1A of the ESF design. As explained before, eighteen of the classifications will be completed by the M&O. As of December 1992, of the twenty systems, according to the RSN analyses thirteen of them were EMC, five EQ and two Q. Of the thirteen EMC systems:

Ten had as worst consequences the interruption of utilities to other parts of the ESF. Questions posed to participants established that interruption of utilities is not ITS, ITIP or ITSC. Those ten were six electrical systems, surface buildings (architecture), surface facility fire protection, access roads and heating/ventilation/air conditioning.

Surface building plumbing involved interruption of utilities and water leakage, but any leaks large enough to be significant would be readily detected and handled.

One electrical system involved interruption of utilities and possible oil leaks from transformers, but again, any leaks large enough to be significant would be readily detected and handled.

The topsoil storage area simply had no scenarios with any significant consequences.

Of the five EQ systems :

The water distribution system had tank and off-pad pipe relocations which could result in spills and leaks entering known faults or the portal, or leaks leading to unknown alteration of site characterization data. The critical characteristics of the tanks and off-pad pipes are their locations. Pipes buried within the pad could leak, possibly leading to unknown alteration of site characterization data. The critical characteristic of the under-pad pipes is the potential for undetected leaks.

The sewer system under-pad pipes share the same risks as the water distribution system under-pad pipes. The sewer pipe from the pad to the leach field could also have undetected leaks leading to unknown alteration of site characterization data. Its critical characteristics are location and potential for undetected leaks. Leachate from the leach field could alter data, if the field is located badly, so its critical characteristic is location.

The pad slope could interact with two Q systems, the stormwater diversion system and the starter tunnel (floor vertical curve), in effect to send stormwater down the access drift. That is, if the stormwater system capacity can be exceeded, spilling water onto the pad, and the pad slope away from the portal is insufficient to carry that water away quickly enough to keep it from overtopping the crest of the floor vertical curve, stormwater can go down the access drift. The critical characteristic of the pad, then, is its slope.

The only scenarios involving tunnel boring machines (TBMs) involved lubricant, coolant and hydraulic leaks and spills. Spills like that could be ITIP, and if the TBMs are used in heater emplacement or instrumentation drifts, they could be ITSC. The critical characteristics of the TBM are its locations of operation and its potential to be a source of foreign material spills and leaks.

The rock storage area could be a source of foreign materials introduced into the rock during excavation, then leached out of the rock during storage. A liner is included in the current design as a mitigating measure. The critical characteristic of the rock storage area is its potential to produce foreign material leachate.

Two systems could become part of a potential repository, and so have the possibility to be classified Q (as opposed to EQ). In fact, both were Q:

The starter tunnel / portal system was Q under each of two distinct lines of reasoning:

1. It is one of the ESF permanent items selected by the program to be delineated as part of the potential repository. These items must be designed to potential repository standards, to the extent known at the time of design. This is expanded to mean that those engineered features that could play a part in the design of the potential repository must be controlled in the design, construction and operation such that the repository designer can determine the capability of the facility, and have the records to demonstrate that capability. Thus features such as design to withstand the selected seismic environment are considered to be mitigating features and treated accordingly.
2. Important aspects of calculations of the risk involved with this system cannot be known with adequate confidence at this time, and so are designated as "indeterminate." For example:
   - There is no adequate data base at this time from which to get the probability of various seismic events that could initiate important accident scenarios;
   - We do not now know the level of armoring protecting the waste canister, and so cannot predict what canister breaches are possible for different seismically-induced events;
   - Nor do we know the radiological source term to use in assessing the consequences of any such canister breach.

   Clearly, in cases where such crucial elements are indeterminate, and plausible data sets can be posited that would lead to a Q classification, the system should be classified Q at least until the data base can be expanded enough to provide a more confident assessment of possible impacts.

The stormwater system was Q under the first line of reasoning presented above for the starter tunnel / portal system, and because of its role, in combination with other elements, in preventing or sending stormwater down the access drift, as explained under Concern 2 above.

One of the most interesting results of our work is its demonstration that a sound classification analysis can provide several useful results other than classification. While classification is useful for providing guidance for selection of controls, the analysis is also useful for discovering risk problems and developing recommended actions to improve risk management. To those ends, the findings of the analyses can be summarized:

Sources of risk discovered by the analyses:
- undetected leaks from pipes (water distribution and sewer) under the pad;
- undetected leaks from the sewer line from the pad to the leach field; and
- location conflicts between the sewer off-pad pipe, leach field, and testing.

Characteristics that have classification significance and so should be tracked with special controls:
- locations of the water storage tanks and associated off-pad pipes;
- locations of the off-pad sewer pipe and leach field;
- capacity of stormwater diversion off the pad;
- pad slope;
- foreign liquids and materials, their spills and cleanup; and
- starter tunnel floor vertical curve.

Recommended efforts to expand the information base used for classification:
- identify and certify, or commission, a seismic hazard data base, then use it to analyze rockfall hazards; and
- call for a determination of how 10 CFR 60.133(e,f) applies to the starter tunnel / portal system, given determinations from Sandia National Laboratory (SNL) and Los Alamos National Laboratory (LANL) that impacts on that system are not ITWI. That section of code specifies "Openings in the underground facility shall be designed to reduce the potential for deleterious rock movement or fracturing of overlying or surrounding rock;" and "The design of the underground facility shall incorporate excavation methods that will limit the potential for creating a preferential pathway for groundwater to contact the waste packages or radionuclide migration to the accessible environment."

Recommended mitigating features to be considered (other than special tracking):
- use of neutron sources and sensors to monitor migration of water around the pad and leach field;
- tagging of non-potable water;
- lining of pipe channels for pipes buried within the pad and sloping them, with perforated pipe to collect fluids from small leaks; and
- conflict mapping between testing activities, piping and the leach field.

IV. CONCLUSIONS

The classification process developed by Raytheon Services Nevada (RSN) and applied to the 20 initial ESF design Package 1A systems resulted in Classification Analysis reports that were approved by the RSN Technical Review Board and completed a Technical-Management Review with participation from DOE, the M&O, SNL and LANL. Of the two classifications that were completed before design responsibility was transferred to the M&O, both were accepted by the Yucca Mountain Project Assessment Team and recognized as being defensible for subsequent licensing purposes. In addition, the classification analyses achieved the other two goals listed in the introduction. They:
- provided guidance for selection of QA controls, in particular by specifying the characteristics that make each element Q, EQ, MC or EMC; and
- demonstrated that classification analyses applied separately to separate elements in a system can perform system-wide risk management functions.

Classifications were influenced by several factors:
- consideration of impacts on thermal, mechanical, geochemical and hydrologic conditions or properties at the site;
- accident-impact scenarios developed for specific systems or activities; and
- performance assessment evaluations by other participants.

Two concerns were identified:

Concern 1: Classifying elements by where they could be located, as opposed to where they are located on the current design.

One effect of this approach is that the Q- and EQ-Lists could become quite long. With an imaginative analyst, perhaps almost every element of Package 1A could be on the Q- or EQ-List. This has the danger of "diluting" the focus of attention on the elements of the system that are truly important to safety. Yet if the controls imposed by this logic are limited to location controls, the net effect could be reasonable risk management.

Concern 2: The combination of a broad definition of mitigating features and not being able to account for the effects of those features in classification.

This approach produces an effectively deterministic, worst-case analysis that may have undesirable effects for risk management. Probabilistic risk analysis normally relies on the discipline of probability math to protect it from fantastic accident scenarios and results determined by the imagination of the analyst. Once a procedure is adopted that allows deterministic thinking, a creative analyst could perhaps put almost all elements of any design package on the Q/EQ-List. This could be a more serious problem than the location controls discussed under Concern 1 above, since the controls here would not be limited to location. It could significantly "dilute" the effect of the Q/EQ-List to focus attention on the truly important elements of a system. It could also open up the analysis to licensing cross-examination that could include fanciful scenarios unlimited by probability considerations, making those scenarios difficult to anticipate or defend against. That could impair the ability to establish regulatory compliance, in a way that has little to do with actual risk.

Concern 2 could be mitigated by performing bounding analyses. For example, an analysis could calculate the minimum amount of foreign material or water that it would take to cause any measurable impact on repository performance. That threshold could then be used to dismiss scenarios where the threshold could not credibly be exceeded. Bounding analyses are currently planned to support the potential license application.

There are four more general conclusions:

1. A review of the results section indicates that in many cases, a Q or EQ classification can be a result of the broad definition of mitigating features, the treatment of those features, and aspects of the information base, not the actual, physical risk of the system being classified.

2. Benefits of this classification analysis are not limited to the classification itself, but, as with any good probabilistic risk assessment, include guidance for design and risk management through the identification of:
   - the critical characteristics that need to be controlled; and
   - the parts of the information base that most need to be further developed through performance assessment efforts.

3. We have developed and demonstrated a solid methodological basis for classification, which minimizes the use of direct engineering judgment. Where there were data gaps, they were spanned with conservative assumptions. The net result is a classification procedure that is more defensible than one where direct engineering judgment plays a more prominent role.

4. The classification analyses described here should be regarded as conservative analyses providing a sound basis for proceeding with design, construction and operation of the ESF, while minimizing the potential for adverse impacts on the site and on the potential repository.

REFERENCES

[1]DOE/RW-0214 Rev.4, "Office of Civilian Radioactive Waste Management Quality Assurance Requirements Document."

[2]NUREG-1318, "Technical Position on Items and Activities in the High-Level Waste Geologic Repository Program Subject to Quality Assurance Requirements."

[3]AP-6.17Q Rev.1, "Classification of Items Important to Safety and Waste Isolation."

[4]PP-02-06, "Determination of Importance of Items and Activities," Project Quality Procedure, Raytheon Services Nevada, Las Vegas, Nevada.

[5]10 CFR 60, "Disposal of High-Level Radioactive Wastes in Geologic Repositories."

DISCLAIMER