CNWRA *A center of excellence in earth sciences and engineering*

A Division of Southwest Research Institute™
6220 Culebra Road • San Antonio, Texas, U.S.A. 78228-5166
(210) 522-5160 • Fax (210) 522-5155

September 27, 2001
Contract No. NRC–02–97–009
Account No. 20.01402.671

U.S. Nuclear Regulatory Commission
ATTN: Dr. Mysore S. Nataraja
Division of Waste Management
Two White Flint North (Mail Stop 7–C6)
Washington, DC 20555

SUBJECT: Repository Design and Thermal-Mechanical Effects Key Technical Issue Intermediate Milestone No. 20.01402.671.160, Preliminary Report on Human Reliability at Geologic Repository Operations Area Operations—Letter Report

Dear Dr. Nataraja:

Attached is the Center for Nuclear Waste Regulatory Analyses (CNWRA) document entitled "Human Reliability Analysis and Repository Preclosure Safety—An Initial Evaluation." This technical document fulfills the requirements for the subject milestone, which is due September 28, 2001.

This report evaluates the application of human reliability methods to the assessment of preclosure repository safety. This initial evaluation describes: (i) basic concepts and selected methodologies for human reliability analysis and (ii) the considerable research and guidance developed by the NRC and others in human reliability analysis and human factors. Based on this background, an approach to treating human reliability in the U.S. Nuclear Regulatory Commission/CNWRA Preclosure Safety Analysis (PCSA) Tool is articulated. The PCSA Tool will be used to review the DOE preclosure safety analysis of the proposed geologic repository operations area at Yucca Mountain.

Washington Office • Twinbrook Metro Plaza #210
12300 Twinbrook Parkway • Rockville, Maryland 20852-1606

If you have any question on this report, please contact me at (210) 522-5151 or Norman Eisenberg at (301) 384-6507.

Sincerely yours,

Asadul H. Chowdhury, Manager
Mining, Geotechnical, and
Facility Engineering

cc:
J. Greeves
J. Piccone
W. Reamer
D. DeMarco
B. Meehan
J. Linehan (w/o enclosure)
E. Whitt
N. Stablein
D. Brooks
D. Galvin
B. Jagannath
T. Ahn
D. Dancer
T. McCartin
B. Leslie
R. Johnson
P. Justus
J. Pohle
W. Patrick
CNWRA Directors
CNWRA Element Mgrs
S. Hsiung
N. Eisenberg
A. Ghosh
D. Gute
G. Ofoegbu
B. Dasgupta
R. Benke
R. Janetzke
P. Maldonado
T. Nagy (SwRI)

HUMAN RELIABILITY ANALYSIS AND REPOSITORY PRECLOSURE SAFETY—AN INITIAL EVALUATION

Prepared for

U.S. Nuclear Regulatory Commission
Contract NRC–02–97–009

Prepared by

Norman A. Eisenberg

Center for Nuclear Waste Regulatory Analyses
San Antonio, Texas

September 2001

ABSTRACT

An initial evaluation is made of the application of human reliability methods to the assessment of preclosure repository safety. In particular, the approach for incorporating human reliability analysis into the Center for Nuclear Waste Regulatory Analyses PCSA Tool is considered. Basic concepts and selected methodologies for human reliability analysis are described. The considerable research and guidance developed by the U.S. Nuclear Regulatory Commission in human reliability analysis and human factors are briefly described and evaluated for applicability to topic of preclosure repository safety. Based on this background, an approach to treating human reliability in the PCSA Tool is articulated. A few examples illustrate how such human reliability analyses might proceed. Additional conclusions and recommendations are provided.

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

FIGURES

TABLES

ACKNOWLEDGMENTS

This report was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the U.S. Nuclear Regulatory Commission (NRC) under Contract No. NRC–02–97–009. The activities reported here were performed on behalf of the NRC Office of Nuclear Material Safety and Safeguards, Division of Waste Management. The report is an independent product of the CNWRA and does not necessarily reflect the view or regulatory position of the NRC.

The author thanks Dr. Biswajit Dasgupta and Dr. Asad Chowdhury, CNWRA, for their help guidance, expertise, and cooperation in developing this report. The author also thanks Dr. Julius J. Persensky and Dr. Nathan Siu, NRC, for kindly agreeing to meet on the subject of this report; they provided many helpful suggestions, that have been incorporated for a better report. The author also acknowledges the substantial assistance of A. Ramos and J. Gonzalez, CNWRA, for their expertise and effort in placing this report in the approved format, thereby conforming to the latest standards. The author gratefully acknowledges B. Sagar for technical support, the programmatic review of W. Patrick, and the editorial review of J. Pryor.

QUALITY OF DATA, ANALYSES, AND CODE DEVELOPMENT

DATA: No CNWRA-generated original data are contained in this report.

ANALYSES AND CODES: No analysis codes or analyses were used in this report.

1 INTRODUCTION

Numerous probabilistic risk assessment studies have shown that human errors can be important contributors to the risk associated with the operations of nuclear facilities. By analogy, human error may also be a significant factor in the safety of operations of the proposed repository at Yucca Mountain. The goal of this investigation is to (i) identify and evaluate a variety of human reliability analysis tools that can be used in repository risk, reliability, and safety analyses; (ii) suggest which human reliability analysis tools might be most appropriate for repository analyses at the current stage of project development; (iii) explore on a preliminary basis how such tools might be incorporated, in part or whole, into the PCSA Tool developed by the Center for Nuclear Waste Regulatory Analyses (CNWRA); and (iv) identify technical, informational, and regulatory issues that arise from the consideration of human reliability analysis in the context of repository preclosure safety. Special attention is devoted to the methods and approaches developed, employed, or endorsed by the U.S. Nuclear Regulatory Commission (NRC).

This report is organized according to the following outline. Chapter 2 describes the fundamentals of human reliability analysis and discusses selected methodologies in some detail. Chapter 3 lists important contributions developed by NRC in human reliability assessment and human factors engineering applied to nuclear safety; an evaluation is made of the significance of especially applicable elements of this body of work. Chapter 4 discusses various contexts of applying human reliability analysis to preclosure safety evaluation and evaluates the influence of these contexts on the choice and application of human reliability analysis methods for use in the PCSA Tool. Chapter 5 articulates an approach to be used with the PCSA Tool and illustrates its application to some examples of repository operations; examples are used because the lack of information on repository operations prevents even a preliminary analysis. Chapter 6 provides conclusions and recommendations, including recommendations for future work. Chapter 7 contains a list of references.

2 FUNDAMENTALS OF HUMAN RELIABILITY ANALYSIS

2.1 Definition of Human Reliability, Human Reliability Analysis, and Other Terms

Human reliability analysis is the study of how human performance affects the reliability of systems in which humans determine, in whole or in part, the performance of the system. Human reliability analysis is usually part of a risk assessment in which other, nonhuman components and subsystems are also modeled. Human reliability analysis may be either qualitative or quantitative. Like other types of risk analysis methods, a quantitative human reliability analysis is generally preceded by a qualitative human reliability analysis for the same system.

Swain and Guttmann (1983) provide the following general definitions:

> Human error—failure to (i) perform the task correctly, (ii) within time limits, or (iii) performance of some extraneous activity that can degrade the system
>
> Human reliability—the probability that a person (i) correctly performs some system-required activity in the required time period (if time is a limiting factor) and (ii) performs no extraneous activity that can degrade the system

Note that the definition of human reliability has a quantitative nature. Human errors are regarded as the outgrowth of an unfavorable combination of the work situation and the humans in it. A human error then becomes some output by a human, that affects system performance and that is outside the tolerances established by the system requirements in which the human is working. Human errors include unintentional errors and intentional errors. Unintended errors are fully unintended when committed and may not even be recognized; intended errors result when a human intentionally commits an error, but the human's belief is that the act is superior to alternatives and will benefit the performance of the system. It is generally considered that malevolent acts are beyond the scope of human reliability analysis, since malevolent acts are intentional attempts to cause harm. There are a variety of measures used to protect against or limit the effects of malevolent acts, such as limiting access to special nuclear material (10 CFR Part 11) and physical protection of nuclear facilities and material (10 CFR Part 73). Analytical methods, other than human reliability analysis, such as threat analysis, support these protective measures.

Sandia National Laboratories (2001) defines human reliability analysis as follows:

> Human reliability analysis is the method by which the probability of a system-required human action, task, or job will be completed successfully within the required time period and that no extraneous human actions detrimental to system performance will be performed. Results of human reliability analysis are often used as inputs to probabilistic risk assessments, which analyze the reliability of entire systems by decomposing the system into its constituent components, including hardware, software, and human operators.

Some other definitions important for discussions of human reliability include the following (NRC, 1996):

> Basic human error probability—Basic human error probability is the probability that an error will occur when a task is performed or that a required task will not be performed. These probabilities are compiled from studies of human performance and, in aggregate, provide a database for human error probabilities based on the performance of a variety of task categories.
>
> Performance-shaping factors—Peformance-shaping factors are environmental, personal, or task-oriented factors that influence the probability of human error. These factors are quantified and are used to obtain a human error rate applicable to a particular set of circumstances. This is accomplished by modifying the basic human error probabilities obtained for generic circumstances.
>
> Skill-based behavior—Performance of a routine sequence of activities in a familiar work environment based on learned skills that are accessed subconsciously, once the request for the sequence has been understood. The sequence of actions takes place without conscious control and is manifest as a continuous, automatic, and integral behavior pattern.
>
> Rule-based behavior—Performance of a routine sequence of activities in a familiar work environment based on a memorized rule learned from previous experience or based on a written procedure. Rule-based behavior requires more conscious effort than skill-based behavior.
>
> Knowledge-based behavior—Performance of a nonroutine sequence of activities or performance of a routine sequence of activities in an unfamiliar work environment requiring cognition and conscious thought. Knowledge-based behavior takes place when the know-how learned from previous instances is not present or when written procedures are not applicable. This requires thought at a higher conceptual level in which performance is goal controlled and knowledge based.

In the context of probabilistic safety assessment (NRC, 1994), human errors may be placed in the following two broad categories:

(i) Those committed during normal operations (pre-initiator or routine errors)

(ii) Those committed during accidents (post-initiator or dynamic errors)

This categorization provides a natural structure and entry point for human reliability analysis into preclosure safety analysis and the **Pre**C**l**osure **S**afety **A**nalysis software tool. Simply put, human error may either (i) provide additional initiating events for accident or upset conditions or (ii) degrade the system response to an accident initiated by mechanical failure, external events, or another human error.

2.2 Human Reliability Analysis Methodologies and Approaches

Human reliability analysis methodologies are complex assemblages of models, databases, techniques, and approaches. As such, it is difficult to define clear, consistent, and disjoint categories in which to classify human reliability analysis methodologies. Nevertheless, a clear dichotomy results from the two major classifications of human error:

Type 1—Human errors that initiate an event or degrade system performance, given otherwise normal operating conditions

Type 2—Human errors that degrade system performance given that an accident or other off-normal event has been initiated

A large number of methods have been developed that address Type 1 human errors, by studying human performance during normal operations and estimating, by a variety of methods, what the human error rate is for different categories of tasks. For example, actuarial data obtained from studies of human performance are used to estimate error rates in categories such as Selects a Wrong Command or Control, or Omits a Task or Step; the error rates thus obtained are modified further to account for factors that shape performance such as Degree of Experience or Stress Level. Type 2 human errors are harder to estimate, because the error rate depends significantly on how well the humans involved understand the situation and are able to think through and perform appropriate responses correctly. Because the errors and error rates in this case are so dependent on the ability to recognize the true nature of the problem, many methods designed to address this type of human error are based on methods derived from cognitive psychology.

One author (Hollnagel, 1993) has developed a scheme for the general classification of human reliability analysis methods, which is reproduced in Table 2-1. This table also places a limited number of human reliability analysis methods into those classification categories. Although some specialists in risk analysis and human reliability analysis may not entirely agree with the Hollnagel classification scheme, it is useful for this discussion because it shows the large number of specific methods available to perform human reliability analysis, and it helps to clarify the distinction among the various methods. The major classes in this system are Methods Based on Engineering Models and Methods Based on Cognitive Models; these different bases are likely to be more appropriate for the analysis of one or the other of the two types of human errors considered in human reliability analysis. The human reliability analysis methods based on engineering models are further subdivided into simulation models, expert judgment methods, and analytical methods. The human reliability analysis methods based on cognitive models are further subdivided into artificial intelligence models and psychological models. An important conclusion from this classification system is that there is a plethora of human reliability analysis methods available, that different attributes for these methods can be selected, and that there is no need to develop a new human reliability analysis methodology to analyze the repository preclosure risk. Selection of an appropriate methodology is necessary and sufficient.

Table 2-1. A General Classification of Human Reliability Analysis Methods*	
Methods Based on Engineering Models	
Simulation Models	Maintenance Personnel Performance Simulation Model (MAPPS) Systems Analysis of Integrated Networks of Tasks (SAINT) Dynamic Logical Analytical Methodology (DYLAM)
Expert Judgment Methods	Paired Comparison Absolute Probability Judgment Rating-Oriented Methods Success Likelihood Index Methodology (SLIM) Influence Diagram Approach Socio-Technical Approach to Assessing Human Reliability (STAHR)
Analytical Methods	Time-Dependent Activities: Accident Sequence Evaluation Program (ASEP) Technique for Human Error Rate Prediction (THERP) Systematic Human Action Reliability Procedure (SHARP) Human Cognitive Reliability (HCR) Operator Action Event Trees (OAET) Confusion Matrix (CM) Task Analysis-Linked Evaluation Technique (TALENT) Tree of Causes Variation Trees Time-Independent Activities: Confusion Matrix Component-specific errors Configuration errors
Methods Based on Cognitive Models	
Artificial Intelligence Models	Cognitive Environment Simulation (CES)
Psychological Models	System Response Analyzer/Generic Error Modelling System (SRA/GEMS) Systematic Human Error Reduction and Prediction Approach (SHERPA) Action Error Analysis Method (AEAM) Cognitive Simulations Model of Decision Making on Behavior in Complex Work (COSIMO) System Response Generator (SRG)
*Hollnagel, Erik. *Human Reliability Analysis—Context and Control.* San Diego, California: Academic Press. p. 137. 1993.	

With regard to the different level of maturity of the methods for analyzing the two types of human error, NUREG–1489 (NRC, 1994) contains two instructive comments:

(i) While the methods for the analysis of preaccident errors are fairly well established..., those for dynamic errors are still evolving.

(ii) There is much less agreement regarding the methods and results to be used for post-initiator human actions.

Even for the pre-accident error rates, this document cautions

> Even though the information contained in the handbook (Swain and Guttmann, 1983) is widely used, it should be borne in mind that the basis for these numbers is the professional judgment of the handbook's authors as shaped by analyses, field experience, and laboratory experience.

As in many other areas of probabilistic safety analysis, a practical, cautious, but utilitarian approach appears to be appropriate. The analysis will proceed using data and methods with known limitations, but the limitations need to be acknowledged.

2.2.1 Human Reliability Analysis Overall Approach

Human reliability analysis is usually conducted as part of an overall risk assessment or probabilistic safety analysis. The human reliability analysis draws upon the system description and system vulnerabilities encoded in a logic tree (fault tree, event tree, or some combination). The system failure modes are then expanded to encompass human error. The resulting system description then includes system failure resulting from equipment failures, external events, and events initiated by human error. In addition, the incorporation of human error considerations will modify the probabilities of system failure based on the possibility that human error will degrade the ability of the system to recover from adverse event initiation. As with most probabilistic safety analysis methods, an iteration of this process would be repeated as appropriate. An important variant of this general approach is to have an interdisciplinary team, including human factors engineers, hardware reliability engineers, and risk analysts, work as a team to develop the logic trees for a system, rather than having teams of different disciplines work sequentially (NRC, 2000b).

Figure 2-1, taken from the NRC Probabilistic Risk Assessment Procedures Guide (NRC, 1983), shows the various steps in an overview of a human reliability analysis for a nuclear powerplant. The same general approach would be applicable to any nuclear facility, including the preclosure operations of the repository. As a first step in human reliability analysis, errors are qualitatively identified; this in itself can be an important means of improving system performance. If the human reliability analysis is to support a probabilistic risk assessment or other probabilistic safety analysis, then, as indicated in this overall approach, a key aspect of a human reliability analysis method is the estimation of human error rates. Several methodologies (e.g., **T**echnique for **H**uman **E**rror **R**ate **P**rediction, human error assessment, and reduction technique) estimate these human error rates using a two-step process:

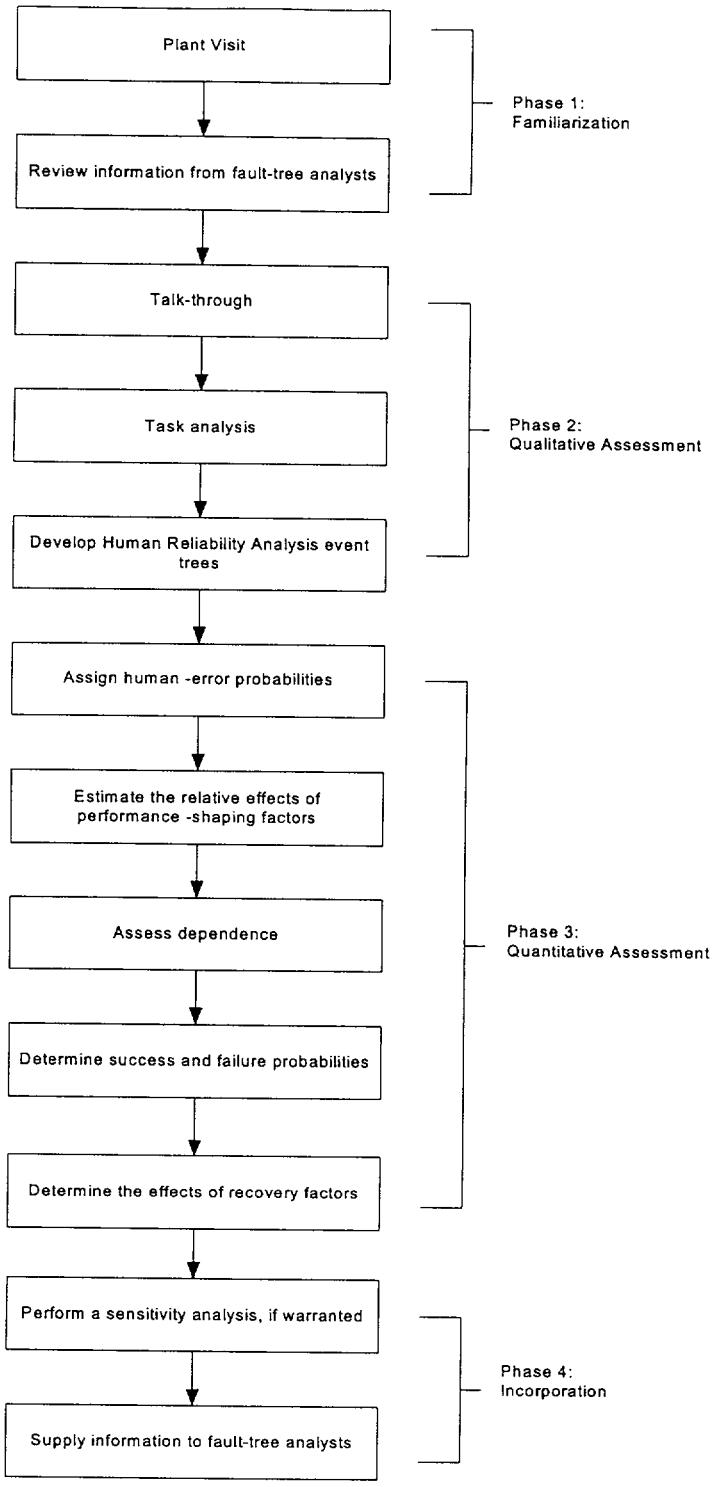

Figure 2-1. Overview of a Human-Reliability Analysis (NRC, 1983)

(i) Human error rates are chosen from a generic table of values that depend on the nature of the task

(ii) These generic human error rates are multiplied by performance-shaping factors that depend on conditions under which the task is performed

2.2.2 Description of Selected Human Reliability Analysis Methodologies

Several reviews have been performed on different human reliability analysis methodologies to evaluate them on the basis of various criteria. Some criteria that might be considered in comparing human reliability analysis methodologies (Smith, 1997) include (i) accuracy, (ii) consistency of results among different analysts employing the same methodology, (iii) ability to identify means to improve overall system performance, and (iv) level of resources needed to implement a particular methodology. One such study, the Human Reliability Assessor's Guide (Atomic Energy Authority, 1995), considered eight well-known human reliability analysis methodologies. Swain (1989) compared and evaluated 14 different human reliability analysis methods on the basis of three categories of criteria (i) usefulness, (ii) acceptability, and (iii) practicality. A few selected methodologies for human reliability analysis are summarized in the following sections.

2.2.2.1 Technique for Human Error Rate Prediction

Technique for **H**uman **E**rror **R**ate **P**rediction was developed by Swain and Guttmann (1983) for Sandia National Laboratories. This methodology has been broadly used for nuclear facilities. NRC has adopted the approach in several instances of formal guidance (e.g., NRC, 1996). The **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology can be considered to be comprised of five steps:

(i) Define system (or subsystem) failure

(ii) Identify and list human operations performed and the relationships of those operations to system tasks and functions

(iii) Predict error rates for each relevant human operation

(iv) Determine effect of human errors on the system failure rate

(v) Recommend changes to improve system reliability to an acceptable level

After the human activities have been delineated and related to system success or failure in Steps 1 and 2, the goal is to quantify the effect of human error on system performance in Steps 3 and 4. There are two basic situations: (i) a single task plays a role as either an initiating event or as a necessary function for successful system performance or (ii) a sequence of tasks plays such a role. For a single task, quantification of its probability of error is the only analysis needed. For a sequence of tasks, a more complex analysis is required.

The basic approach is to divide each task into a sequence of steps and then to identify the errors that can occur at each step. The sequence of steps is represented by a human reliability

analysis event tree; this is a qualitative step. The next step, the quantification of the human reliability analysis event tree, uses a two-stage process: (i) basic error rates are obtained from tabulated values for a variety of archetypical human activities and (ii) these basic error rates are modified by performance-shaping factors, which account for environmental factors (such as stress) or the nature of the human (such as training or fatigue level). The tree approach allows consideration of dependencies of later failure probabilities on previous failures. Figure 2-2 shows an archetypical human reliability analysis event tree diagram. This tree depicts three sequential human events: A, B, and C. An error is represented by an uppercase letter and success is represented by a lowercase letter. By convention, failure is the right branch and success is the left branch. The far left leg in Figure 2-2 represents total success; the far right leg represents failure in all sequential tasks. The **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology (Swain and Guttmann, 1983) suggests that for an initial analysis, only the fully successful leg needs to be quantified, since it can be used to obtain a pessimistic estimate of failure probability. That is, if the failure probability is derived by subtracting the fully successful probability (no failures in the entire sequence of tasks) from unity, it provides a pessimistic estimate of failure probability. This is a pessimistic estimate of failure probability because subsequent tasks may provide recovery, which will turn a failure situation into a success; during such conditions, assuming any failure will cause a system failure is a pessimistic approach. For human activities that provide redundancy, such as checking or inspection, such an assumption may be substantially pessimistic.

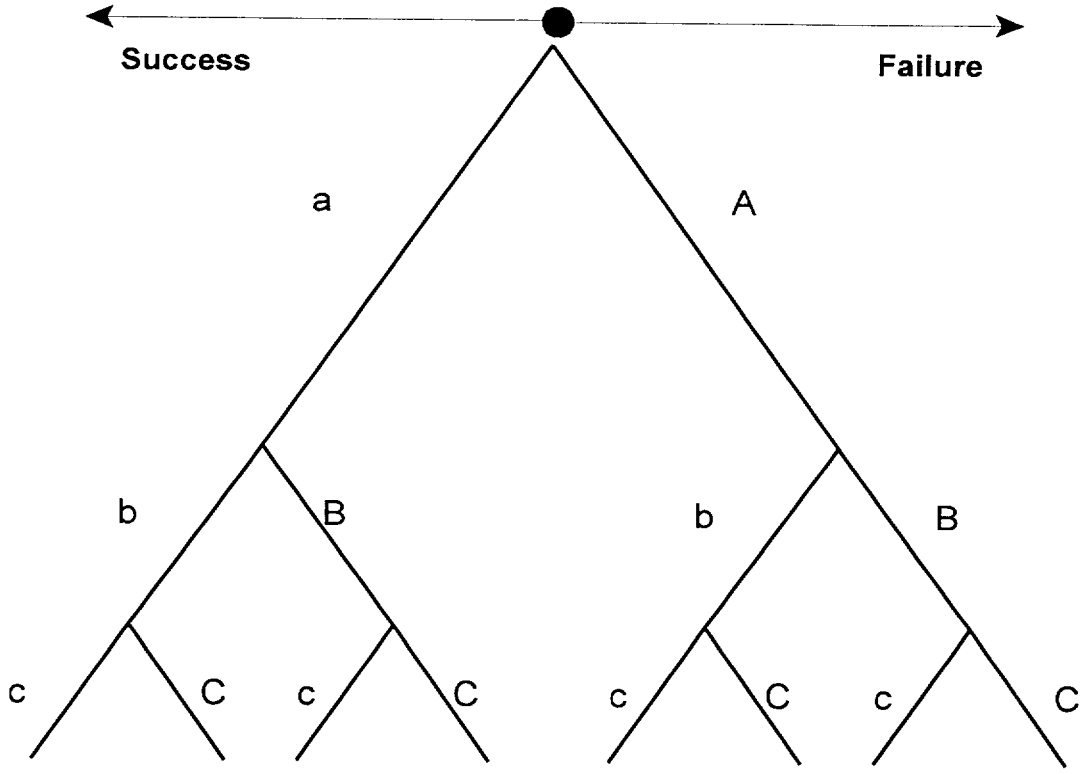

Figure 2-2. Archetypical Human Reliability Analysis Tree

Basic human error probabilities have been compiled as part of the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology; a sample is provided in Table 2-2. A general classification scheme for human errors used in the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology consists of the following

(i) Omits a step or an entire task
(ii) Selects a wrong command or control
(iii) Positions a control incorrectly
(iv) Executes wrong sequence of actions

(v) Implements incorrect timing (early or late)
(vi) Uses incorrect quantity

The basic human error probabilities listed in Table 2-2 include a representation of uncertainties inherent in those probabilities. The column labeled "Error Function" represents the error function defined by Swain and Guttmann (1983), which is the square root of the ratio of the

Table 2-2. A Sample of Technique for Human Error Rate Prediction Basic Human Error Probabilities*

Task Description	Human Error Probability	Technique for Human Error Rate Prediction Data Table	Error Function
Diagnosis of a single event given 30 minutes to respond	1.0×10^{-2}	Table 20-1	(5)
Writing an item incorrectly on a tag	3.0×10^{-3}	Table 20-5	(5)
Use a valve restoration list	1.0×10^{-2}	Table 20-6	(3)
Use a calibration checklist	5.0×10^{-2}	Table 20-6	(5)
Long list procedure with checkoff provision	1.0×10^{-2}	Table 20-7	(3)
Errors in reading and writing information from graphs	1.0×10^{-2}	Table 20-10	(3)
Errors in reading and writing information from analog displays	3.0×10^{-3}	Table 20-10	(3)
Selecting the wrong circuit breaker from a dense grouping	5.0×10^{-3}	Table 20-12	(3)
Checking routine tasks using written material	1.0×10^{-1}	Table 20-22	(5)

*Swain, A.D. and H.E. Guttmann. NUREG/CR–1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." SAND 80-0200. Washington, DC: NRC. 1983.

upper bound of the probability to the lower bound of the probability. A more precise mathematical definition is that the basic human error probabilities are assumed to be the geometric mean of the upper and lower bounds; this definition is consistent with assuming that the upper and lower bounds are symmetrically distributed about the basic human error probabilities value on a logarithmic scale. If the human error probabilities are assumed to be lognormally distributed, then the basic human error probabilities value is the median of the distribution. As an example, consider the third entry in Table 2-2, the basic human error probability (errors per attempt—a dimensionless quantity) is 1.0×10^{-2}. The upper bound would be 3.0×10^{-2}, and the lower bound would be $1.0 \times 10^{-2} \div 3 \approx 3 \times 10^{-3}$.

Before applying these basic human error probabilities, they should be modified by performance-shaping factors appropriate to the task, the human performers, and the environment. A relatively comprehensive list of performance-shaping factors and their definitions is provided in Table 2-3. Based on the presence of one or more performance-shaping factors, the basic human error probabilities are multiplied by factors that increase the basic error probability (e.g., stress, fatigue) or decrease the basic error probability (e.g., training, experience). In the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology, these adjustments are accomplished in two ways: (i) the upper or lower bounds of the human error probability, as determined by the error function, are used to replace the basic human error probabilities or (ii) a separate scaling factor is applied. As an example of the first approach, **T**echnique for **H**uman **E**rror **R**ate **P**rediction defines four levels of tagging or locking systems (Swain and Guttmann, 1983). Three of these levels involve increasing levels of control intended to assure accurate completion of the tasks. For the level in which a specific number of tags is issued for a job, tagging is the primary assignment for the worker, a record is kept of tag disposition, the lower uncertainty bound of the human error probability is used. For the level in which tags are not accounted for individually, tagging is a collateral duty, and record-keeping is not controlled, then the nominal human error probability is used. For the level in which record keeping is inadequate to determine whether all appropriate equipment has been tagged, then the upper uncertainty bound of the human error probability is used. As an example of the second approach, **T**echnique for **H**uman **E**rror **R**ate **P**rediction provides modifying factors based on different stress and experience levels (Swain and Guttmann, 1983, Table 20-16). For example, for an optimum stress level, the basic human error probability would be multiplied by a factor of 1 for an experienced worker, but by a factor of 2 for a novice (less than 6 months experience with the tasks). For extremely high stress, the basic human error probability would be multiplied by a factor of five for an experienced worker, but by a factor of ten for a novice.

One additional feature of the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology that may be important in some situations is that it can treat dependencies. The basic human error probabilities, examples of which are given in Table 2-2, do not consider the specific characteristics of the environment, process, or humans for a particular situation. These basic human error probabilities are converted to human error probabilities by considering the performance-shaping factors appropriate for the situation, but without considering the influences of other tasks. Conditional human error probabilities are modifications of the basic human error probabilities to account for the influences of other tasks or events. In Figure 2-2, suppose the three human activities (a,b,c) act in a redundant fashion; suppose these activities are as follows:

Table 2-3. Definitions of Performance-Shaping Factors (from Bickel, et al., 1976)	
Performance-Shaping Factor	**Definition**
Crew experience	Characterizes the experience of the crew
Time to perform	Defines how much time is required to perform the task
Time available	Defines how much system time is available to perform the task before it no longer matters whether the task is performed or not
Stress	Characterizes the amount of stress the task performer is under
Quality of plant interface	Characterizes the quality of the controls and instrumentation. Do they meet basic ergonomic standards and provide the necessary information?
Type of instrument/control	Describes the type of instrument or control. Is it a video display screen, a rotary control, a meter.
Feedback to operator action	What type of feedback does the operator receive after a control action? For example, does the operator know that a valve is closed?
Procedure required	Is a procedure required for use by the operator?
Action covered by procedure	Does the content of the procedure address the actions required to perform the task(s)?
Procedure well written	Does the procedure conform to acceptable procedure-writing standards?
Procedure understood	Is the procedure understood by the operator?
Procedure practiced	Is the procedure practiced by the staff?
Cognitive level of behavior	Is the behavior or action taken by the operator skill-based, rule-based, or knowledge-based?
Recovery actions	Are any actions possible that would aid the operator recovering from an error?
Tasks dynamic or step-by-step	Is the task performed concurrently with other tasks or is it performed step-by-step?
Task dependency	Is the correct performance of this task dependent on the performance of another task?
Tagging	Is tagging (i.e., the degree to which it is easy to identify whether equipment is in or out of service) involved in performance of the tasks?
Local versus remote control	Is the task performed in the control room or locally at a valve, switchgear room, or fuel farm?

Table 2-3. Definitions of Performance-Shaping Factors* (continued)	
Performance-Shaping Factor	**Definition**
Clothing and tools required	What special tools or equipment such as anticontamination clothing are required to complete the task, and are they available?
Environment	What is the temperature, radiation level, or noise level during task performance under conditions specified by the event sequence? The environment needs to be specified in detail.

*Bickel, J.H., D.L. Kelly, and T.J. Leahy. "Fundamentals of Probabilistic Risk Assessment (PRA)." DOE Contract No. DE–AC07–76ID01570. Idaho Falls, Idaho: EG&G Idaho, Inc. 1976.

(i) Monitor the external contamination on the cask upon receipt
(ii) Decontaminate the cask, if needed
(iii) Check the external contamination, before transfer of the cask to the waste handling building

Further suppose that all three activities must be performed in error for the contaminated cask to be transferred to the waste handling building. If the three activities are completely independent, then the probability of failure is P(A)·P(B)·P(C), where P(X) is the probability that the activity is performed in error. If $P(X) = 10^{-3}$ for each activity, then the probability of failure is small, 10^{-9}. If, as is more likely, the tasks are dependent, the probability of failure will be higher. For example, the probability of decontamination (Activity B) may be 0 if the contamination is not detected in Activity A. If the same staffer misreads the radiation meter in Activity A, the probability is near one that the meter will be misread in Activity C. Under these dependent circumstances, the probability of failure is 10^{-3}, much larger. Treatment of more complex dependencies is possible under the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology.

2.2.2.2 Human Error Assessment and Reduction Technique

Human error assessment and reduction technique is similar in approach to the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology and has been widely used in a variety of contexts. As with **T**echnique for **H**uman **E**rror **R**ate **P**rediction, the methodology proceeds with some basic human error probabilities for a few (9) fundamental types of human tasks and then modifies these probabilities by using varying levels of error-producing conditions (38 in number), which play a role similar to the performance-shaping factors in **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology. In addition, a subjective weight is applied to the error-producing condition, to determine to what degree it may have an effect in a particular application.

Table 2-4 is a list of the nine fundamental types of human error used in the **H**uman **E**rror **A**ssessment and **R**eduction **T**echnique methodology. As shown, error probabilities range from more than 0.55 for totally unfamiliar tasks performed at normal speed to 2×10^{-5} for responding when there is an augmented supervisory system providing help. Examples of the 38 error-producing conditions are given in Table 2-5. The factors for these examples range from 17 to 1.1. Subjective weights, *w*, may range from 0 to 1. To calculate an error probability

Table 2-4. Basic Human Error Probabilities for the Human Error Assessment Reduction Technique Methodology*	
Task	**Probability of Error**
Totally unfamiliar, perform at speed, no idea of outcome	0.55
Restore system to new or original state on a single attempt without supervision or procedures checks	0.26
Complex task requiring high level of comprehension and skill	0.16
Fairly simple task performed rapidly or given scant attention	0.09
Routine highly practiced, rapid task involving relatively low level of skill	0.02
Restore system to new state following procedure checks	0.003
Totally familiar task, performed several times per hour, well motivated, highly trained staff, time to correct errors	0.0004
Respond correctly when there is augmented supervisory system providing interpretation	0.00002
Miscellaneous task—no description available	0.03
*Smith, D.J. *Reliability, Maintainability and Risk*. 5th Edition. Oxford: Butterworth-Heinemann. 1997.	

for a given circumstance, the basic error probabilities are modified by a factor that depends on the error-producing condition(s) and the subjective weights, as follows:

$$f_i = \left[(EPC_i - 1) \bullet w_i \right] + 1 \qquad (2\text{-}1)$$

where

f_i — factor for error-producing condition i
EPC_i — multiplier for error-producing condition i
w_i — subjective weight for error-producing condition i and the particular case

The error probability is given by:

$$P_m = P_b \bullet F \qquad (2\text{-}2)$$

where

P_m — modified error probability
P_b — basic error probability

and F is a multiplicative factor given by:

Table 2-5. Error-Producing Conditions and Human Error Rate Multipliers Used in the Human Error Assessment Reduction Technique Methodology*	
Error-Producing Condition	**Maximum Multiplier**
Unfamiliar with infrequent and important situation	17.0
Shortage of time for error detection	11.0
No obvious means of reversing an unintended action	8.0
Need to learn an opposing philosophy	6.0
Mismatch between real and perceived task	4.0
Newly qualified operator	3.0
Little or no independent checks	3.0
Incentive to use more dangerous procedures	2.0
Unreliable instrumentation	1.6
Emotional stress	1.3
Low morale	1.2
Inconsistent displays and procedures	1.2
Disruption of sleep cycles	1.1
*Smith, D.J. *Reliability, Maintainability and Risk*. 5th Edition. Oxford: Butterworth-Heinemann. 1997.	

$$F = \begin{cases} \prod f_i \text{ when } F \bullet P_b \text{ is less than 1} \\ 1/P_b \text{ when } F \bullet P_b \text{ is greater than or equal to 1} \end{cases} \quad (2\text{-}3)$$

The **H**uman **E**rror **A**ssessment and **R**eduction **T**echnique methodology has an advantage over the **T**echnique for **H**uman **E**rror **R**ate **P**rediction in that it is less cumbersome to apply; the disadvantage is that the weighting factors are subjective and require expertise to apply properly.

2.2.2.3 Empirical Technique to Estimate Operator Errors

Empirical **T**echnique to **ESt**imat**E** **O**perator Errors is similar in approach to the **T**echnique for **H**uman **E**rror **R**ate **P**rediction and human error assessment and reduction technique methodologies in that basic human error probabilities are selected and then modified by various

factors to obtain the human error probability applicable to a particular case. The empirical technique to estimate operator errors methodology is even simpler than the **H**uman **E**rror **A**ssessment and **R**eduction **T**echnique methodology. A value from each of five classes of

factors is multiplied together to determine the case-specific human error probability. These factors are listed in Table 2-6.

2.2.2.4 A Technique for Human Event Analysis

A Technique for **H**uman **E**vent **ANA**lysis is a major effort to develop a model for human performance based on a cognitive-model paradigm that focuses on the context within which the operators must act as well as on the error mechanisms of the operators (NRC, 1998a; 2000b). **A** Technique for **H**uman **E**vent **ANA**lysis deals with operator actions that take place after an abnormal event occurs (e.g., a fire or earthquake) that have been previously defined in probabilistic risk assessment for the facility. Like many human reliability analysis methods, **A** Technique for **H**uman **E**vent **ANA**lysis has both qualitative and quantitative aspects. The

Table 2-6. Factor Categories, Attributes, and Factor Values Used in the Methodology*

Factor Category	Attribute	Factor Value
1. Activity	simple	0.001
	requires attention	0.01
	nonroutine	0.1
2. Time Stress (seconds available)	2, routine; 3, nonroutine	10.0
	10, routine; 30, nonroutine	1.0
	20, routine	0.5
	45, nonroutine	0.3
	60, nonroutine	0.1
3. Operator	expert	0.5
	average	1.0
	poorly trained	3.0
4. Anxiety	emergency	3.0
	potential emergency	2.0
	normal	1.0
5. Ergonomic	excellent	0.7
	good	1.0
	average	3-7
	very poor	10.0

*Smith, D.J. *Reliability, Maintainability and Risk*. 5th Edition. Oxford: Butterworth-Heinemann. 1997.

qualitative aspect seeks to provide an analytical methodology that will realistically and consistently evaluate previous incidents involving human responses and then develop potential accident sequences, based on these evaluations of prior incidents. The quantitative aspect seeks to provide realistic estimates of the probabilities of unsafe human actions for inclusion in probabilistic risk assessments. **A** Technique for **H**uman **E**vent A**NA**lysis does not consider human errors made under normal operating conditions, such as those errors treated effectively by the Technique for **H**uman **E**rror **R**ate **P**rediction methodology (Swain and Guttmann, 1983). A principal assumption of the **A** Technique for **H**uman **E**vent A**NA**lysis approach is that (i) the conditions in the plant (e.g., the nature of the upset event, the degree of stress-producing environmental factors, such as sirens or alarms, whether immediate physical danger is threatened) and (ii) the previous conditioning of the humans (i.e., the usual performance-shaping factors), together may produce an error-forcing context that could produce an erroneous human response to an upset condition. Such an erroneous response was illustrated at Three Mile Island when a misdiagnosis of an abnormal condition was not changed, even though evidence continued to indicate otherwise. Error-forcing contexts are determined by structured search schemes using the efforts (considered to be large and costly by some)[1] of a multidisciplinary team consisting of human-reliability experts, plant operators, probabilistic risk assessment specialists, and possibly others. This team integrates knowledge and experience in engineering, probabilistic risk assessment, human factors, and psychology with plant-specific information and knowledge gained from the analysis of past accidents.

A Technique for **H**uman **E**vent A**NA**lysis methodology differentiates between the underlying mechanisms for human error and the manifestation of the human error, an unsafe action. The methodology avoids using the term human error, because it imprecisely distinguishes between the underlying conditions and the resulting actions and because error has an inappropriate connotation of blame. Human failure events are used in the context of a probabilistic risk assessment, of which the human reliability analysis is a part. Unsafe actions may have a direct correspondence to human failure events or may provide a finer level of analysis. **A** Technique for **H**uman **E**vent A**NA**lysis methodology can be considered to have the following components:

- Incorporation of the defined issues into **A** Technique for **H**uman **E**vent A**NA**lysis human reliability analysis perspective
- Identification of human failure events and unsafe actions relevant to these issues of concern
- Identification of the causative factors (error-forcing contexts, performance-shaping factors) for the human failure events or unsafe actions
- Quantification of the error-forcing contexts and the probability of each unsafe action, given the context
- Evaluation of the analytical results versus the issues of concern

---

[1]Powers, D.A. "Technical Basis and Implementation Guidelines For a Technique For Human Event Analysis (ATHEANA)." Letter to William D. Travers, Executive Director for Operations, NRC. Washington, DC: Advisory Committee on Reactor Safeguards, NRC. 1999.

A more implementation-oriented breakdown of **A** Technique for **H**uman **E**vent A**NA**lysis process, as a type of human reliability analysis, includes the following (NRC, 2000b):

- Define and interpret the issue being analyzed
- Define the resulting scope of the analysis
- Describe basecase scenarios
- Define the human failure events and unsafe actions of concern
- Identify potential vulnerabilities
- Search for deviations from basecase scenarios
- Identify and evaluate complicating factors
- Evaluate the potential for recovery
- Interpret the results (including quantification, if necessary)
- Incorporate into the probabilistic risk assessment (if necessary)

3 SUMMARY OF NRC GUIDANCE AND RESEARCH ON HUMAN RELIABILITY ANALYSIS

For many years, NRC has had a significant interest and activity in human reliability analysis and human factors. Although much of the guidance issued by the NRC is more properly characterized as related to human factors rather than human reliability, it is included in this report for two reasons:

- The NRC staff may wish to develop or adopt guidance related to human performance for the preclosure repository operations.
- Implementation of existing NRC guidance may significantly affect conditions at the facility and the characteristics of the workers. Implementation of NRC guidance could have a major influence on the qualitative and quantitative nature of human reliability involved with these operations.

3.1 Existing NRC Guidance on Human Reliability Analysis

Existing NRC guidance on human reliability analysis and human factors is largely contained in the NRC regulatory guide series. Additional guidance may also be found in other forms, such as Standard Review Plans, Branch Technical Positions, and other documents. The NRC regulatory guides are organized in ten divisions; those divisions with the most relevance for human performance in preclosure repository safety are Division 1—Power Reactors and Division 3—Fuels and Materials Facilities.

Table 3-1 lists those guides with at least some relevance to human performance in preclosure repository safety and characterizes the degree of relevance. Subsequent sections provide a brief description of those regulatory guides that are most relevant.

Although the existing guidance on human reliability analysis and human factors contained in NRC regulatory guides is substantial, little (except for Draft Guide–3003) can be identified as applying specifically to repository operations. This characteristic of NRC regulatory guide raises the question of whether the NRC staff should develop specific guidance for repository operations or whether existing guidance can be used.

3.1.1 Materials Guidance

The following are the regulatory guidance documents on Fuels and Materials Facilities that may have some relevance to human reliability or human factors or both.

Regulatory Guide 3.42 is concerned with emergency planning for fuel cycle facilities and specifies planning for training certain categories of workers in Section 8.1, Organizational Preparedness.

Table 3-1. List of NRC Regulatory Guides with Some Relevance to Human Performance Related to the Repository Preclosure Operations. Relevance Key: H–high; M–moderate; S–slight; P–potential				
Guide Number	**Title**	**Last Revision**	**Publish Date**	**Relevance**
1.8	Qualification and Training of Personnel for Nuclear Power Plants	3	05/00	H/P
1.71	Welder Qualification for Areas of Limited Accessibility		12/73	P
1.114	Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit	2	05/89	P
1.134	Medical Evaluation of Licensed Personnel for Nuclear Power Plants	3	03/98	P
DG–1052	Time Response Design Criteria for Safety-Related Operator Actions		09/96	H/P
3.42	Emergency Planning for Fuel Cycle Facilities and Plants Licensed Under 10 CFR Parts 50 and 70	1	09/79	S
3.44	Standard Format and Content for the Safety Analysis Report for an Independent Spent Fuel Storage Installation	2	01/89	S
3.48	Standard Format and Content for the Safety Analysis Report for an Independent Spent Fuel Storage Installation or Monitored Retrievable Storage Installation	1	08/89	S
3.50	Standard Format and Content for a License Application to Store Spent Fuel and High-Level Radioactive Waste	1	09/89	S
3.61	Standard Format and Content for a Topical Safety Analysis Report for a Spent Fuel Dry Storage Cask		02/89	S
3.62	Standard Format and Content for the Safety Analysis Report for Onsite Storage of Spent Fuel Storage Casks		02/89	M
3.67	Standard Format and Content for Emergency Plans for Fuel Cycle and Materials Facilities		01/92	M
DG–3003	Format and Content for the License Application for the High-Level Waste Repository		11/90	H

Table 3-1. List of NRC Regulatory Guides with Some Relevance to Human Performance Related to the Repository Preclosure Operations. Relevance Key: H–high; M–moderate; S–slight; P–potential (continued)				
Guide Number	**Title**	**Last Revision**	**Publish Date**	**Relevance**
HF608–4	Training and Certification of Independent Spent Fuel Storage Installation Operators		03/82	M/P
5.20	Training, Equipping, and Qualifying of Guards and Watchmen		01/74	P
5.43	Plant Security Force Duties		01/75	P

Regulatory Guide 3.44 is concerned with the format and content for the safety analysis report for a water-basin-type, independent, spent nuclear fuel storage installation. This guide includes general requirements for organization and training of the facility staff.

Regulatory Guide 3.48 is concerned with the format and content for the safety analysis report for a dry-storage-type, independent, spent nuclear fuel storage installation or monitored retrievable storage. This guide includes general requirements for control room design.

Regulatory Guide 3.50 is concerned with the format and content for a license application to store spent nuclear fuel and high-level waste and includes general requirements for training of staff and facility security.

Regulatory Guide 3.61 is concerned with the format and content for a topical safety analysis report for a spent nuclear fuel dry storage cask; it includes a requirement to delineate operational procedures in the facility, but does not specify those procedures.

Regulatory Guide 3.62 is concerned with the format and content for the safety analysis report for onsite storage of spent nuclear fuel storage casks. This guide requires delineation of control room features (5.2), conduct of operations (9), including organizational structure (9.1), training (9.3), emergency planning (9.5), and operating controls and limits (10). [Note: number in parenthesis indicate section in the Regulatory Guide.]

Regulatory Guide 3.67 is the format and content guide for emergency plans for fuel cycle and materials facilities; it delineates emergency response actions and responsibilities to a limited extent.

Draft Guide–3003 is the format and content guide for the license application for the proposed high-level waste repository. Although this draft guide is heavily keyed to 10 CFR Part 60, it does contain requirements to describe 7.3, Organizational Structure, Management, and Administrative Controls; 7.4, Procedure Development; and 7.6, Training Programs. (The NRC staff is currently developing a Yucca Mountain Review Plan which will be keyed to 10 CFR Part 63 when it is finalized.) HF608–4 is a draft regulatory guide for the training and certification of independent, spent nuclear fuel storage installation operators; it specifies topical areas of training and a certification procedure, including testing.

3.1.2 Reactor Guidance

The following are the regulatory guidance documents on power reactors that may have some relevance to human reliability or human factors or both:

Regulatory Guide 1.8 endorses ANSI/ANS–3.1–1993 (American National Standards Institute, 1993) with certain clarifications, additions, and exceptions. The requirements specified in the guidance may have a significant effect on certain performance-shaping factors. However, this regulatory guide is intended only for nuclear powerplants, not other nuclear facilities.

Regulatory Guide 1.71 specifies procedures to assure the quality of reactor vessel welds, by simulating the conditions of a weld when access to the welding area is limited. Because welding is an important part of the proposed repository operational activities, this procedure or a similar procedure might be useful if access to the welding areas of the disposal containers are actually performed by human welders rather than machines, and if access to the welding area is restricted or limited.

Regulatory Guide 1.114 specifies requirements for an operator at the controls of a nuclear power reactor and requirements for a senior operator to be present in the control room. Requirements for operators at the control include (1.1) an unobstructed view of and access to the operational control panels, (1.2) a need for the operator to remain in the control room, (1.3) the definition of a surveillance area within the control room, and (1.4) an operator entering a new shift must be briefed on the status of the power unit. The senior operator has similar requirements, but more flexibility. If central control and the equivalent of a reactor operator are not part of the operational plan of the repository, then this guidance would not apply.

Regulatory Guide 1.134 endorses the requirements of ANSI N546–1976, which delineates an acceptable method for determining the medical qualifications of applicants for initial or renewal operator or senior operator licenses for nuclear powerplants. If central control and the equivalent of a reactor operator are not part of the operational plan of the repository, then this guidance would not apply.

Draft Guide–1052 specifies credit that can be taken for operator actions in responding to emergency situations in a nuclear powerplant. This guidance provides criteria to differentiate those conditions when operator actions may be relied upon and those conditions that must be responded to without human intervention. Although this guidance is intended for the control personnel at a nuclear powerplant, some of the guidance or its bases may be useful in the repository context.

3.1.3 Other Guidance

The following are regulatory guidance document in other divisions that may have some relevance to human reliability or human factors or both.

Regulatory Guide 5.20 specifies requirements for the qualification (C.1), training (C.2), testing (C.3), and equipping (C.4) of guards and watchmen at nuclear facilities. These requirements may be adopted at the repository and would then have an influence on the human performance of such staff during repository operations.

Regulatory Guide 5.43 specifies the organization (C.1) and duties (C.2), including duties during security events (C.2.e and f), of the security force at nuclear material facilities requiring physical protection under the requirements of 10 CFR Part 73. If the repository requires such physical protection, the requirements would have an influence on the human performance of the security force.

3.2 NRC Research on Human Reliability Analysis

3.2.1 Summary of Past Research

Recent Commission papers describe the NRC program in human reliability and human factors (NRC, 1998b, 2000a). NRC began an intense consideration of the implications of human reliability for nuclear facility safety, subsequent to the accident at Three Mile Island-Unit 2 in 1979. This intense consideration was motivated, in part, by the recommendations of several blue-ribbon panels (e.g., Rogovin and Frampton, 1980; Kemeny, 1979) that identified human factors as a significant contributor to this momentous event. As a consequence, the NRC changed its organization to reflect this additional emphasis on human factors and human reliability by establishing a Human Factors Branch in the Office of Nuclear Regulatory Research and a Division of Human Factors Safety in the Office of Nuclear Reactor Regulation.

During the 1980s, these organizations at the NRC developed several guidance documents about human reliability aspects of nuclear facility safety. These guidance documents include (as referenced in Section 7):

- NUREG–0700: Guidelines for Control Room Design Reviews (NRC, 1981b)
- NUREG–0801: Evaluation Criteria for Detailed Control Room Design Review (NRC, 1981d)
- NUREG–0799: Draft Criteria for Preparation of Emergency Operating Procedures (NRC, 1981a)
- NUREG–0899: Guidelines for the Preparation of Emergency Operating Procedures (NRC, 1982)
- NUREG–0835: Human Factors Acceptance Criteria for the Safety Parameter Display System (NRC, 1981c)
- NUREG–0731: Guidelines for Utility Management Structure and Technical Resources (NRC, 1980b)
- NUREG–1280: Power Plant Staffing (NRC, 1980a)

The NRC staff also engaged in rulemaking regarding human reliability, which included

- 10 CFR 50.54: Requirements for minimum licensed operator staffing
- 10 CFR 50.120: Requirements for training programs at nuclear power plants

- 10 CFR Part 26: Requirements for a fitness-for-duty program
- 10 CFR 52.47: Requirements for applications for standard design certification
- 10 CFR Part 55: Requirements for operator licensing and simulators

During this time, in addition to these substantial activities by the NRC staff, the two **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology reports were issued (Swain and Guttmann, 1983; Swain, 1987), as discussed in Section 2. In addition, some work was sponsored on a cognitive approach to modeling human performance in emergencies at nuclear powerplants (Woods, et al., 1987). The Cognitive Environment Simulation employed techniques developed for artificial intelligence to simulate the cognitive processes that produce situation assessment and intention formation.

SECY–98–244 (NRC, 1998b) also notes that several industrial groups (the Nuclear Energy Institute, the Institute for Nuclear Power Operations, and the Electric Power Research Institute) are engaged in developing research and guidance for human factors and human reliability, including control room design, procedure development, protective clothing for extreme environments, proficiency training and testing, and corrective action tools and aides. The NRC staff remains cognizant of these activities and will endorse suitable guidance when it is developed.

3.2.2 Current Research

Current activities at NRC in human performance are fully integrated into the larger regulatory framework for nuclear power reactors and the research activities supporting reactor regulation. This framework consists of four key program areas directed toward nuclear power plant safety:

- Reactor Oversight Process
- Plant Licensing and Monitoring
- Risk-Informed Regulation Implementation Plan
- Emerging Technology/Issues

The focus of these activities is nuclear reactor regulation, with some interest in Office of Nuclear Material Safety and Safeguards applications. Some activities in this program include

- Revise Regulatory Guide 1.8, Qualification and Training of Personnel for Nuclear Power Plants to endorse ANSI/ANS–3.1–1993 (American National Standards Institute, 1993) with exceptions

- Develop a human performance evaluation protocol

- Characterize the effects of human performance in reactor oversight process

- Control station review guidance, including
  - Hybrid control stations
  - Alarm systems
  - Interface management I
  - Halden experiments
  - Integration with digital instrumentation and control program

Also included in the program is interaction with international entities involved in human reliability analysis applied to nuclear safety (e.g., the International Atomic Energy Agency, the Halden Reactor Project, Swedish Nuclear Power Inspectorate) and other federal agencies similarly involved (e.g., Department of Transportation, Department of Defense, National Aeronautical Space Agency, Occupational Safety and Health Agency, National Institute of Occupational Safety and Health Administration).

Also of note is the fact that NRC developed and maintained a Human Factors Information System; this database includes data collected from Licensee Event Reports from January 1992 through April 1998; the program is now continuing. At least one Human Performance Item has been identified for each reported licensee event included in this database.

3.3 Current Issues in Human Reliability Analysis at the NRC

Some current issues in human reliability analysis at the NRC include those discussed in the Human Factors Program Plan [described in Section 4 of the document, A Prioritization of Generic Safety Issues, (Emrit, et al., 2000)]. This program plan identifies seven program elements: (i) staffing and qualification, (ii) training, (iii) licensing examinations, (iv) procedures, (v) management and organization, (vi) human-machine interface, and (vii) human reliability. A long-standing issue that has not yielded in any significant fashion to research is how to characterize and factor into a risk analysis the effects of organization, management, and culture of the entities operating nuclear facilities.

3.3.1 Spent Nuclear Fuel Risk Studies

3.3.1.1 Technical Study of Spent Nuclear Fuel Pool Accidents at Decommissioning Plants

This recent staff analysis considered the risks from spent nuclear fuel pool accidents at nuclear powerplants undergoing decommissioning (NRC, 2000c). Nine initiating event categories were investigated as part of the quantitative assessment on spent nuclear fuel pool risk:

(i) Loss of offsite power from plant-centered and grid-related events
(ii) Loss of offsite power from events initiated by severe weather
(iii) Internal fire
(iv) Loss of pool cooling
(v) Loss of coolant inventory
(vi) Seismic event
(vii) Cask drop
(viii) Aircraft impact
(ix) Tornado missile

An important failure scenario is (i) loss of some or all of the water coolant in the spent nuclear fuel pool, (ii) the resulting uncovering of the spent nuclear fuel, (iii) the subsequent overheating of the stored spent nuclear fuel, (iv) the potential severe consequence of a zirconium fire, and (v) release of ruthenium and fuel fines. Human intervention is considered to be a key factor in recovery from a loss of coolant event providing for resubmersion of the spent nuclear fuel in water. Because of the thermal dynamics of the spent nuclear fuel pool, there is a long time

(hundreds of hours, depending on the time since the fuel was removed from the reactor) during which recovery from a loss of coolant situation is possible. Significant initiating events for loss of water coolant in the spent nuclear fuel pool are seismic events and very large load drops (spent nuclear fuel casks) onto the floor of the pool.

3.3.1.2 Fuel Cycle Risk Assessment

In the early 1980s, the NRC staff commissioned a comprehensive risk assessment of nuclear fuel cycle, nonreactor facilities (Schneider, 1982). Section 16 of this assessment evaluates the risk from Spent Fuel and High-Level and Transuranic Waste Storage, which may have some relevance for the preclosure repository operations. Although operations at spent nuclear fuel storage facilities are given, the details represent equipment (e.g., shipping and storage casks) and procedures that are either hypothetical or dated. Furthermore, there is no special emphasis on human reliability.

4 OVERVIEW OF ANALYSIS CONSTRAINTS AND SOLUTIONS

Human reliability analysis methods were developed and are usually applied to existing facilities with ongoing operations. A significant issue in attempting to apply human reliability analysis methods to evaluate preclosure repository safety is that the design and, more importantly, operational details needed to apply human reliability analysis methods are lacking. Although the broad outline of the designs for operational facilities is available, the details of operational procedures are almost completely lacking. This lack of detail raises many questions regarding repository operations. Two very broad, but fundamental, questions arise regarding (i) operational control (centralized or distributed) and (ii) training, supervision, and control of various classes of workers.

A fundamental question that does not appear to be answered yet is whether control functions during the preclosure phase will be centralized or distributed. Most operational functions at a facility like a nuclear powerplant are centralized and controlled from the control room. Although some activities, such as spent nuclear fuel handling and security, are not directly controlled by the control room operators, they maintain some visibility of such operations and would be aware of any off-normal event. It is not clear whether the repository will have a centralized control room, monitoring and controlling operations throughout the facility, or whether operations in each functional area (receiving and shipping, handling, emplacement) will be monitored and controlled locally, or perhaps monitored and controlled at an even lower level of aggregation. Depending on which approach is chosen, the focus for human reliability considerations will change. With a central control strategy, significant thought will have to be given to the interfaces between functional areas and assuring that problems that develop in one functional area do not adversely impact activities in another. With a distributed control strategy, considerations will be focused on assuring error-free operations within the functional area. A strength of the centralized strategy is that the safety of the overall facility is utmost, so suboptimal decisions that are possible with a distributed strategy would be avoided. One weakness of the centralized strategy is that a control room staff may have too much to observe and control; furthermore, a centralized strategy is vulnerable to cognitive errors on the part of the control room staff. The strength of the distributed strategy is that the monitoring and control are more limited and simpler; a weakness is that actions in one operational area may inadvertently have an adverse effect on operations in another area. The treatment of human reliability for repository operations depends on the degree to which monitoring and control are centralized or distributed, so this fundamental question needs to be resolved to develop an appropriate treatment and to develop appropriate regulatory guidance.

Another broad question regarding repository operations is how various kinds of persons at the repository will be trained, supervised, and controlled. Radiation workers directly involved in handling radioactive material, will have stringent requirements for training, supervision, and control. Workers engaged in servicing and maintaining safety-related equipment will also have significant requirements of this type. However, other persons present on the site (see Table 4-1), such as construction workers (miners), security personnel, managers, visitors, and general facility workers, may perform acts that adversely affect the safety of the facility. For example, cleaning staff may misapply corrosive cleaning materials and damage the functionality of a safety-related piece of equipment. In general, human errors by staff not directly involved in handling radioactive material or maintaining equipment for handling radioactive material will be

Table 4-1. Categories of Workers in the Repository	
1. Radiation workers	Handle spent nuclear fuel and other radioactive material
2. Maintenance workers	Maintain equipment involved in safety-related tasks, such as hoists, transporters, cranes, and hot-cells
3. Nonradiation workers	Handle excavation, mechanical, and other tasks, but do not handle radioactive material or equipment for handling radioactive material
4. Managers	Do not perform operational tasks, but supervise others in those tasks
5. Security	Provide for physical security for the site
6. Nonsafety facility workers	Ordinary maintenance workers perform common janitorial and other routine tasks
7. Visitors	As with the current facility, visitors are expected on a frequent basis

unintentional errors of commission. An overall approach to training, supervising, and controlling these various categories of persons needs to be articulated.

4.1 Definition of the Problem

4.1.1 Contexts for Human Reliability Analysis Applied to Repository Preclosure Safety

To recommend an approach to human reliability analysis for repository preclosure safety, the various contexts in which the human reliability analysis will be conducted should be considered. These contexts are briefly described.

4.1.1.1 Regulatory Context

NRC regulation 10 CFR 63.111 specifies performance objectives for the geologic repository operations area for the preclosure operational period, until permanent closure. This regulation is currently undergoing revision to conform to the finalized U.S. Environmental Protection Agency standard for Yucca Mountain (40 CFR 197); thus the following limits may be revised in that process. Currently 10 CFR Part 63 limits are placed on dose to workers and dose to members of the public. Consideration is given to design basis events (a combination of postulated challenges and failure events against which the operational facility is designed) in two categories: (i) Category 1 events expected to occur one or more times during the operational phase (about 100 years), including "anticipated operational occurrences" and (ii) Category 2 events expected to occur with at least one chance in 10,000 during the operational phase.

Events with a probability of occurrence of less than 1 in 10,000 during the operational phase are not considered credible. In the proposed rule, dose limits are:

(1) For workers, doses are limited, during routine operations and for Category 1 events, to 5 rem [0.05 Sv] total effective dose equivalent plus additional limits for individual organs or tissues, the lens of the eye, and the skin or any extremity.

(2) For the public, doses are limited:

(a) To any real member of the public, located beyond the boundary of the site, during routine operations and for Category 1 events, to 25 mrem [0.25 mSv] total effective dose equivalent

(b) For any individual located on, or beyond, any point of the boundary of the site, for Category 2 events, to 5 rem [0.05 Sv] total effective dose equivalent, plus additional limits for individual organs or tissues, the lens of the eye, and the skin or any extremity.

Given these different end points (dose to the workers or to the public), the different limiting doses, and the two categories of events, the goal of the probabilistic safety assessment is not singular, so the preclosure safety analysis, including any imbedded human reliability analysis, must be expanded to consider all these factors. One can easily envision the calculation of both onsite and offsite consequences for each event progression end state. Comparing the end-state doses to their probability will indicate whether the facility complies with the performance objectives of the preclosure safety regulation.

4.1.1.2 Operational Context—The PCSA Tool

Human reliability analysis is expected to be employed by the U.S. Department of Energy (DOE) in formulating an Integrated Safety Analysis to demonstrate compliance with the applicable NRC regulations for the repository. The NRC and its contractor, the CNWRA, have developed a tool and review methodology for assessment of preclosure safety analysis (Dasgupta, et al., 2000). The PCSA Tool is intended for use by the NRC to assess, through independent analysis of critical aspects of the DOE Integrated Safety Analysis, whether DOE has adequately (i) calculated potential doses to workers and the public, and (ii) identified structures, systems, and components important to safety. Because DOE is expected to treat human reliability analysis in its Integrated Safety Analysis, the NRC auditing analysis tool should have this component also.

Dasgupta, et al. have described a methodology for preclosure safety assessment (Dasgupta, et al., 2001). The PCSA Tool structure, described by Dasgupta, et al., is reproduced as Figure 4-1. The PCSA Tool follows the approach common to many probabilistic safety assessment with steps that include facility familiarization, system description, determination of internal and external initiating events, development of accident sequences, and determinations of consequences. Because the PCSA Tool traverses the entire analytical structure, including calculation of dose to the public and workers, it has parallels with a Level 3 probabilistic risk assessment. In Section 5, of this report, some suggestions are made to clarify

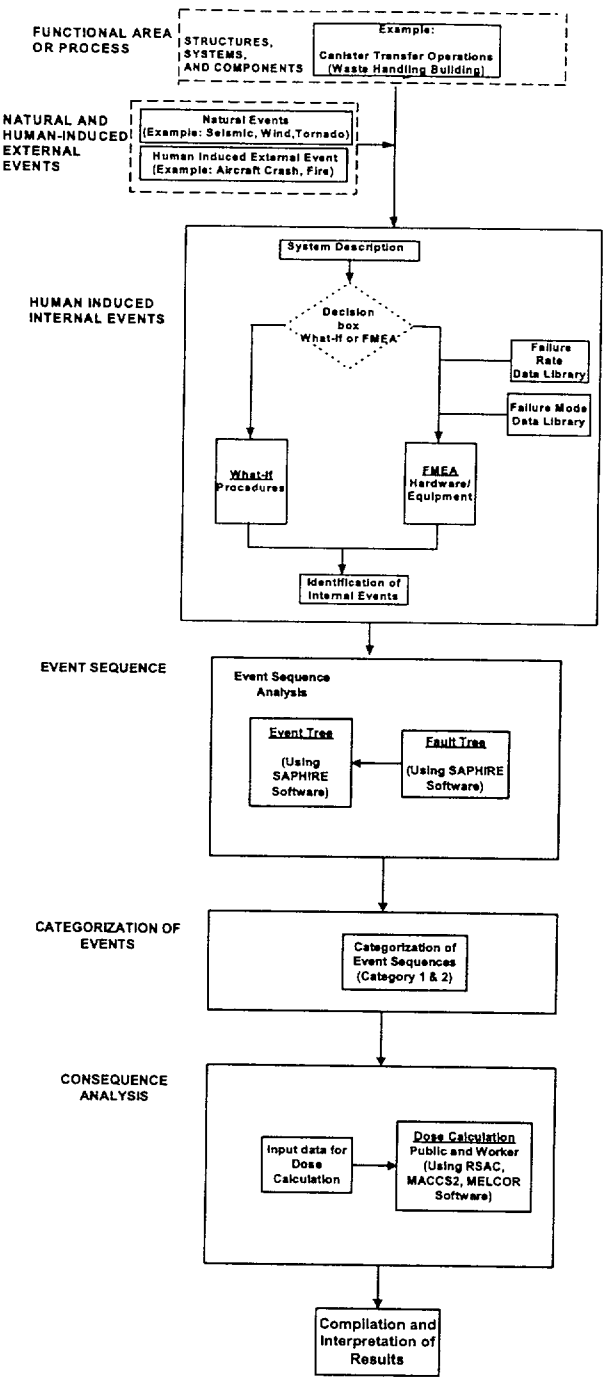

Figure 4-1. PSCA Tool Structure and Modules (Dasgupta, et al., 2001)

the role of human reliability analysis and to ensure inclusion of all aspects needed for the defined task.

4.1.1.3 Organizational Context—NRC Research, Guidance, and Applications

As the discussion in Section 3 indicates, an extensive body of technical and regulatory work has been done in considering human reliability analysis and human factors engineering in nuclear facilities. NRC has been a leader in developing and applying human reliability analysis methods to nuclear safety issues. NRC has developed specific guidance for human reliability analysis applied to spent nuclear fuel handling facilities and conducted independent studies quantifying risks in such facilities. For these compelling reasons, any approach incorporating human reliability analysis into the PCSA Tool should recognize guidance and previous approaches; to the extent possible, the use of human reliability analysis should be consistent with these approaches.

4.1.1.4 Informational Context

Analysis of human performance in repository preclosure safety and risk is limited by two key elements:

(i) Lack of detailed information
  (a) Design detail is incomplete in some areas
  (b) Operational plans are largely unavailable

(ii) The repository is not an operating facility
  (a) Observation of actual operational practices is precluded
  (b) Determination of human error rates from actual operational data is precluded

Until more information becomes available on the plans for operations, a human reliability analysis of those operations is largely hypothetical, if not speculative.

The lack of useable information about repository operations can be illustrated by an example. Consider the table of contents for the Waste Handling Building System Description Document (CRWMS M&O, 2000b):

Summary

Quality Assurance

1. System Functions and Design Criteria
2. Design Description
3. System Operations
4. System Maintenance

Appendix A Criterion Basis Statements
Appendix B Architecture and Classification
Appendix C Acronyms, Symbols, and Units
Appendix D Future Revision Recommendations and Issues

Appendix E References

It appears from this list that there will be a description of System Operations is in Section 3; however, when that part of the report, and others, are examined, the following are observed:

> Criteria Compliance
>
> The surface facility is developed conceptually at this time without criteria compliance analyses. The criteria compliance for this system will be addressed in future issues of this SDD [system description document] as the design and analysis for the system matures.
>
> System Operations
>
> This section will be completed in a later revision (emphasis added)
>
> System Maintenance
>
> This section will be completed in a later revision.
>
> Appendix A Criterion Basis Statements
>
> This section presents the criterion basis statements for criteria in Section 1.2. Descriptions...

The implication is clear. Although several reports outline the design of the preclosure facilities, scant detail, useful to human reliability analysis, is available on the actual operations planned.

4.1.2 Implication of Constraints and Broad Outline of an Approach to Human Reliability Analysis

As described previously, the constraints on the incorporation of human reliability analysis into the PCSA Tool fall into four main categories.

(i) Regulatory: The application of human reliability analysis needs to focus on compliance with the preclosure regulations (proposed 10 CFR 63.111)

(ii) Operational: The human reliability analysis must be compatible with the PCSA Tools that are to be used to evaluate and probe analyses performed by the DOE.

(iii) Organizational: The human reliability analysis should use NRC-developed methods, models, and data, unless for some unforeseen reason, other techniques offer a unique capability that is required.

(iv) Informational: Because the information to support the human reliability analysis is sparse, initial attempts to incorporate human reliability analysis into the PCSA Tool should be qualitative; as more information becomes available from DOE, the human reliability analysis can become more quantitative.

Broadly speaking, the human reliability analysis should be incorporated into the PCSA Tool in two major elements: (i) the preliminary analysis identifying event sequences and (ii) the detailed analysis of event sequences. In addition, consideration of operator actions relative to an initiated event sequence may qualitatively change the consequences of the event and may change the likelihood of a particular outcome. The application of human reliability analysis should be consistent with the scope and detail of the overall analytical element that it supports. Furthermore, the scope and detail of the human reliability analysis must reflect the level of information available from DOE on operational activities.

5 DESCRIPTION OF AN APPROACH TO HUMAN RELIABILITY ANALYSIS FOR REPOSITORY PRECLOSURE SAFETY

Because the DOE plans have not reached a stage of maturity that speaks to human reliability analysis issues, except in the broadest context, the ability to perform a meaningful human reliability analysis at this time is limited. The goals of this section are (i) to show how human reliability analysis principles and methods can be applied to the preclosure repository safety, and (ii) to obtain estimates, by a few examples, of the impact that human reliability analysis considerations might have on overall risk estimates.

5.1 Summary of Approach

5.1.1 Overview

As described in Section 2, human reliability analysis is generally applied to two situations:

(i) Human errors that occur prior to an accident initiator
(ii) Human errors that occur during an accident sequence

Treatment of human errors of these different types requires different approaches and databases. However, both types of human errors need to be integrated into the overall approach and tool for preclosure safety analysis. Existing methods, developed or endorsed by the NRC, are available to treat both types of human errors. The **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology addresses Type 1 human error while the **A T**echnique for **H**uman **E**vent **ANA**lysis methodology addresses Type 2 human error.

To be compatible with the PCSA Tool, these methodologies must be applied at two levels: (i) at a qualitative, preliminary level for the identification of internal events, and (ii) at a quantitative, detailed level for the development of fault and event trees. However, because these analyses are not currently well developed and the descriptions of operations by DOE are extremely limited in operational detail, it is not meaningful at this time to attempt modification of event trees using cognitive methods to represent how dynamic human errors may affect system response; however, general qualitative analyses may have some limited utility.

5.1.2 Detailed Recommendations

Dasgupta, et al. (2001) have described a methodology for preclosure safety assessment. The preclosure safety analysis tool structure, described by Dasgupta, et al., is reproduced as Figure 4-1. Based on the discussions in Section 2, the following changes to this tool are recommended.

(i) The Human Induced Internal Events part of the analysis needs to be expanded to account for human errors that (1) may initiate event sequences or (2) may be committed during the evolution of accident sequences. The level of detail of the human reliability analysis in this part of the analysis should be on a general, preliminary level to correspond to the qualitative, Preliminary Hazard Analysis nature of this part of the analysis. One approach would be to consider a parallel, but interactive path for the analysis; one path would focus on mechanical reliability, while the other would focus on

human reliability. These results would be combined, with some consideration given to interactions between the human and mechanical parts of the system, and iterated as needed. In addition, some qualitative consideration should be given to the effect of human performance on the development of the event sequences, to evaluate (on a preliminary basis) whether human performance could substantially increase or decrease the consequences resulting from the development of an event sequence. Alternatively, the mechanical and human aspects of the system could be analyzed by a team, as suggested in the A Technique for Human Event Analysis methodology (NRC, 2000b). One approach to incorporating human reliability is shown in Figure 5-1, where a human reliability analysis path parallel to the Failure Modes and Effects Analysis is introduced. Parallel to the failure rate and failure mode data libraries that are inputs to the Failure Modes and Effects Analysis box, two data inputs provide input to the Human Reliability Analysis box: (1) basic human error probabilities and (2) performance shaping factors. Determination of the performance shaping factors will require information about the facility, the staff, and procedures that can influence human performance.

(ii) The "Event Sequence" part of the analysis needs to be expanded to account for human errors that (1) may initiate event sequences or (2) may be committed during the evolution of accident sequences. The level of detail of the human reliability analysis in this part of the analysis should be on a detailed, advanced level to correspond to the quantitative fault tree/event tree nature of this part of the analysis. The human reliability analysis should be quantified to the extent possible. While the initiating events caused by human error under routine conditions may be quantified (e.g., by the technique for human error rate prediction methodology), the evolution of event sequences substantially influenced by human error, may be much more difficult to quantify. Cognitive modeling considerations may be quite significant in classifying event sequences for demonstrating compliance because (1) the qualitative nature of the events could change; new types of events with qualitatively different outcomes, especially higher consequences, could be identified; (2) the probability of occurrence of identified events could change, thereby moving event sequences between the two categories with the corresponding effects on classification of systems, structures, and components. As with the preliminary analysis, iteration between the mechanical and human reliability analyses should be performed, as needed. Alternatively, a combined analysis by a team of experts could be used.

(iii) Introduction of human reliability analysis into the preclosure safety analysis tool may engender some confusion, based on the terminology currently in use. To lessen potential confusion with human error, human reliability, and human-caused safety issues, it may be useful to change the term human induced to anthropogenic. Human induced is currently used in conjunction with external events and internal events. In those contexts it is used to characterize events which are related to man's activities, such as airplane crashes or equipment failure. The entire set of internal events is characterized as human induced because the facility is man-made; however, human induced may have too much of a connotation of resulting from human error, which is not the intended meaning. Internal events, used without any qualification, may help to lessen confusion, if a human reliability analysis is added.

One approach to influence these suggestions is indicated in Figure 5-1.

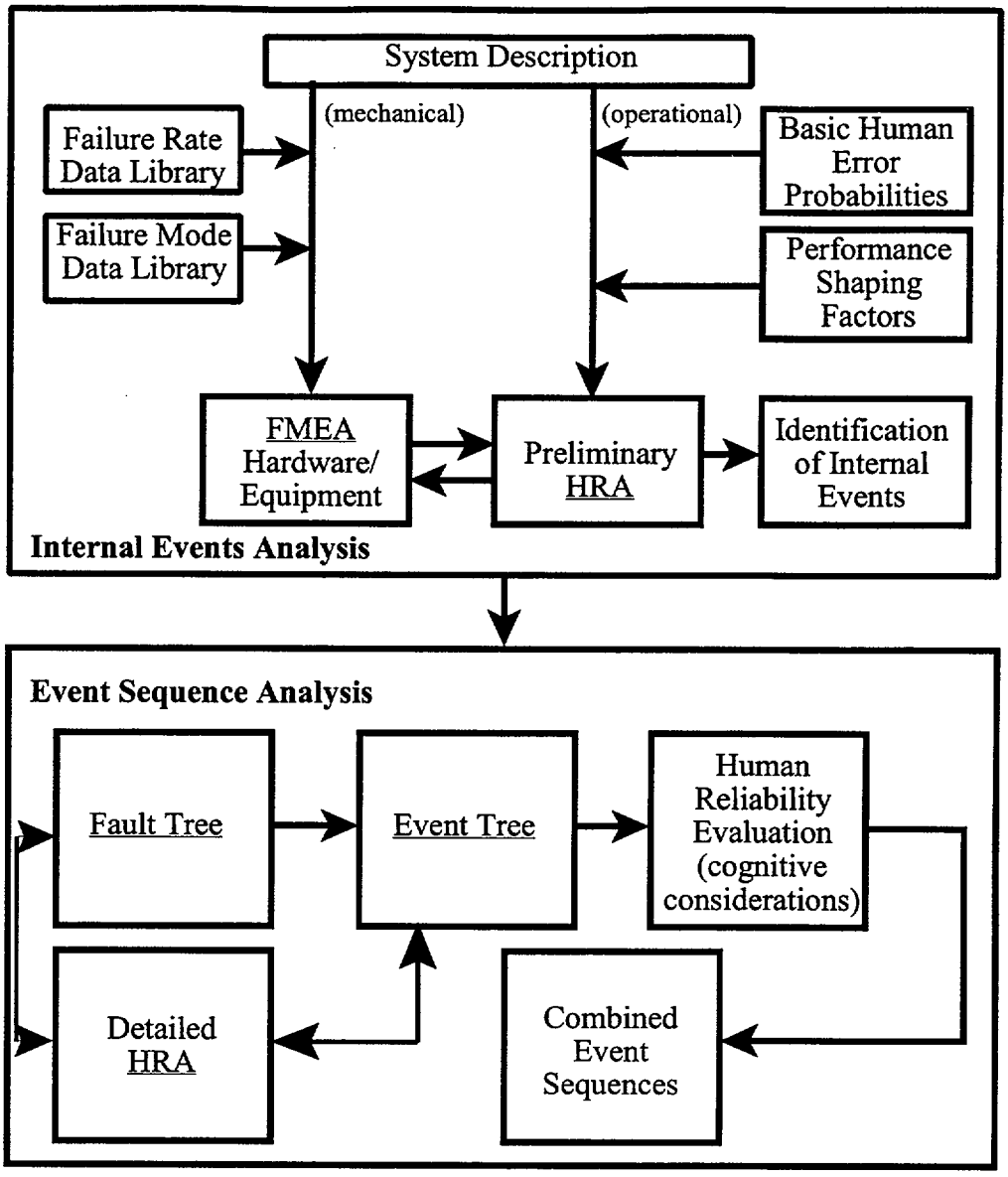

Figure 5-1. Suggested Modifications to the Structure of the PCSA Tool, Incorporating Considerations of Human Reliability

5.2 Discussion of Relation of Approach to NRC Guidance and Research

Guiding principles in developing an approach to apply human reliability analysis to repository preclosure safety include

(i) Develop no new methods, data, or approaches, if existing methods are sufficient; this use of existing methods will conserve resources

(ii) Use, to the extent practicable, methods developed, in use, or endorsed by the NRC staff, so the staff will be familiar with the approaches and require minimal additional training.

5.2.1 Applicability of Databases

Databases for use in human reliability analysis have been compiled by several authors, as indicated in Section 2, especially Section 2.2. Databases for human error probabilities in a routine or preinitiator context are well established. It may be possible to refine the estimates for human error probabilities in the subsurface environment by examining databases or studies performed in relation to mining activities or mine safety; such a refinement is beyond the scope of this effort. Data to support both the qualitative examination of error type and the quantification of error probabilities for a post-initiator or dynamic context are less well developed. Although some generic data and some specific data for nuclear facilities are available, it may be worthwhile to investigate whether data are available to characterize the special environments and the cognitive errors potentially generated by such environments in mines and other underground works.

5.2.2 Applicability of Methods

The generic methods of human reliability analysis appear to be adequate for application to the repository preclosure safety problem. Improvements of the databases to characterize underground environments and human errors better, as indicated in Section 5.2.1, may be useful.

5.3 Examples of Application of Approach

The approach outlined will be demonstrated on some hypothetical examples. These examples are hypothetical because the information available on repository operational activities is extremely limited. For example, some key information that is not clear based on current documentation includes:

- Whether there will be a facility-wide control room observing and managing all aspects of the operation; alternatively, whether operations in different functional areas will be monitored and controlled separately.

- To what degree operations will be performed remotely and which operations will be performed that way.

- Conditions that determine the performance-shaping factors, which are required to produce meaningful quantitative estimates of human error probabilities, are largely unspecified;

  — The degree of training and experience of the staff
  — The length of shifts
  — The degree to which electronic controllers are used and the manner by which humans interface with them
  — Whether written instructions and checklists will be mandated
  — The degree of checking and supervision

These examples are not presented in the same order as the sequence of operations in the proposed repository (Receiving and Shipping, Handling, Emplacement); instead the examples are presented in the order of decreasing ability to quantify. The inability to quantify result arises primarily from the lack of detail available for design and operations, as described in the preceding paragraph. The order of presentation gives the fullest example of incorporating human reliability analysis methods first; subsequent examples show, successively, the limiting effects of lack of detail.

5.3.1 Example for Handling

As an example of applying a human reliability analysis methodology for the handling operations area, consider the following description of preclosure repository operations for Waste Handling–Assembly Transfer (CRWMS M&O, 2000a):

> Remote or manual cask preparation operations consist of gas sampling, venting, lid unbolting and removal, gas and water cool-down, shield plug unbolting, and attachment of the shield-plug lifting fixture. If the cask contains individual spent nuclear fuel assemblies with no dual-purpose canister, it will be filled with water in the preparation pit and then transferred to the cask unloading pool.

These operations are prior to removal of the spent nuclear fuel assemblies from the transport cask for processing in the waste handling building. If the cask gases are determined to be contaminated during the sampling process, then the cask is supposed to be transferred to a special remediation hot cell for special handling and decontamination. If the cask gases are not determined to be contaminated, then the cask will remain in the routine processing area, where the spent nuclear fuel assemblies will be removed from the transportation cask and ultimately packaged in a disposal container.

5.3.1.1 Qualitative Analysis

The qualitative analysis of potential human error would support the Internal Events Analysis segment of the overall PCSA Tool. Consider the potential for a worker to experience an abnormal dose from release of cask gases into the assembly transfer area. Because this abnormal dose can only happen if the cask gases are contaminated, the human reliability analysis is conditional on the cask being contaminated. The probability that the cask gases are, in fact, contaminated will need to be determined from operational experience or estimated from other spent nuclear fuel handling facilities. A qualitative analysis might identify the following potential human errors, which could lead to exposure of workers to contaminated cask gases:

- The cask vent port is not properly connected to the radiation detector
- The radiation detector is not read correctly to identify contamination, when present
- The cask is not transferred to the remediation hot cell, even though contamination is detected
- A contaminated cask is not properly connected to the exhaust system
- A contaminated cask is not properly purged of contaminated cask gases

A separate qualitative evaluation would need to assess the potential for excessive dose to workers from their unintended exposure to contaminated cask gases. One analysis for release of cask gases from relatively fresh fuel gave a postulated dose to a control room occupant of 3.5×10^{-3} rem [3.5×10^{-5} Sv] (whole body) and 7.8×10^{-4} rem [7.8×10^{-6} Sv] (thyroid) (NRC, 1999).

5.3.1.2 Quantitative Analysis

The quantitative analysis of potential human error would support the Event Sequence Analysis segment of the overall PCSA Tool. Figure 5-2 shows a hypothetical human reliability analysis tree for such an event. This human reliability analysis tree is hypothetical, because there is very little detail in the DOE documentation upon which to base a more realistic analysis. The human reliability analysis is divided into two parts:

> Part A considers the probability that the contaminated cask is not transferred, as it should be, to a special hot cell for handling contaminated casks
>
> Part B considers that the contaminated cask is mishandled, so that contaminated cask gases are released to the room

The Part A analysis consists of three dependent sequential actions by workers (see Figure 5-3):

(1) Sampling the cask port for contaminated cask gases
(2) Correctly noting the contamination, if present
(3) Transferring the cask to the waste package remediation system, if contaminated

The probability of incorrectly performing these tasks is denoted by a, b, and c, respectively, for Tasks 1, 2, and 3. In Swain and Guttmann (1983,Table 20-5), the human error probability for action 1 is estimated to be a = 0.003, omitting a step or important instruction from a formal or ad hoc procedure. The human error probability for action 2 is estimated to be a = 0.001, check-reading error in reading an analog meter with easily seen limit marks [Swain and Guttmann (1983, Table 20-11)]. The human error probability for action 3 is, like action 1, estimated to be c = 0.003, omitting a step or important instruction from a formal or ad hoc procedure. Note that to obtain these numbers, it has been assumed (i) there are no written procedures; (ii) a checklist is not being used; and (iii) the contamination level is monitored by an analog gauge, without annunciation, but with limit marks. Also, no performance-shaping factors have been used (e.g., factors related to the level of stress, the number of tasks assigned, training, experience), because the information available is insufficient to determine these factors. As indicated in Figure 5-2, the conditional probability of a contaminated cask being transferred,

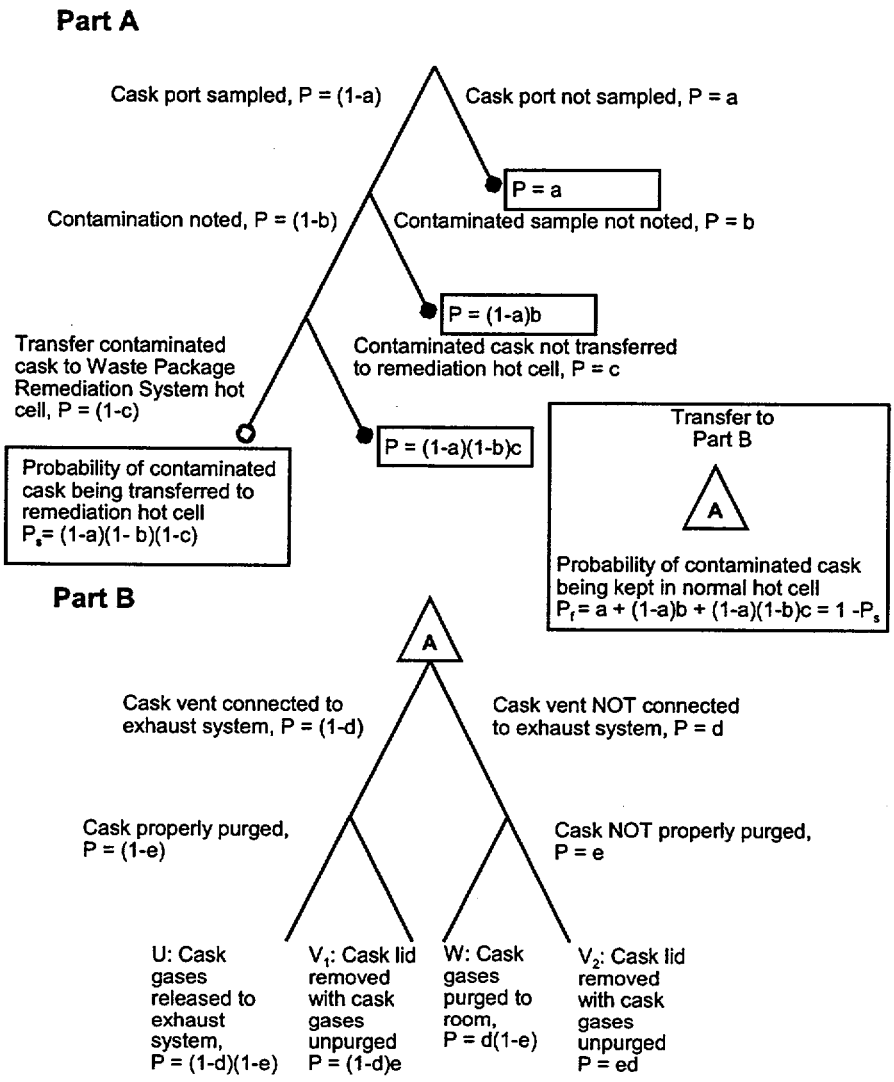

Figure 5-2. Human Reliability Analysis Trees for Handling Incident Branch Definitions and Their Conditional Probabilities Are Shown on Either Side of the Branch Points. In Part A, Branches Terminating in Failure Are Indicated with Filled-in Circles with the Probabilities Enclosed in a Rectangle. The Success Path in Part a Is Terminated by an Open Circle. The Terminal Probabilities Shown in Part B (For Outcomes U, V, and W) Are Conditional Probabilities.

as required, to the remediation hot cell is given by the quantity: $P_s = (1-a)(1-b)(1-c) = 0.997 \times 0.999 \times 0.997 \approx 0.993$ [$= 1-P_f = 1-0.006985$] ; the conditional probability that a contaminated cask is left in the general cask preparation and decontamination area, contrary to requirements, is given by (Condition A): $P_f = a + (1-a)b + (1-a)(1-b)c = 0.003 + 0.997 \times 0.001 + 0.997 \times 0.999 \times 0.003 = 0.003 + 0.000997 + 0.002988 = 0.006985$; these probabilities are conditional on the cask being contaminated, which does not appear to be known at this time.

The Part B analysis consists of two sequential actions by workers assumed to be independent (see Figure 5-2):

(i) Connecting the cask vent port to the exhaust system
(ii) Purging the contaminated cask gases, before removing the cask lid

The probability of incorrectly performing these tasks is denoted by d and e, respectively, for tasks 1 and 2. Both tasks are like Tasks 1 and 3 in Part A; so, as before, a probability of error of 0.003 is used. There are three possible outcomes, U, V, and W (see Figure 5-2):

U: Cask gases are released to the exhaust system; no undue exposure of workers.
V: Cask lid is removed with cask gases not purged; possible excessive exposure of workers.
W: Cask gases are purged into the waste handling building; possible excessive exposure of workers.

The conditional probabilities of these outcomes (conditional on Condition A, calculated in Part A) can be calculated from the human reliability analysis tree as follows:

$P(U) = (1-d)(1-e) = 0.997 \times 0.997 \approx 0.994$;
$P(V) = P(V_1) + P(V_2) = (1-d)e + de = e = 0.003$;
$P(W) = d(1-e) = 0.003 \times 0.997 = 0.00299 \approx 0.003$.

Because both Outcomes V and W have the potential for excessive exposure of radiation workers, the conditional probability of excessive exposure is 0.006. Then the overall probability, combining the results of Part A and Part B, with the overall probability of a contaminated cask, gives:

probability of excessive contamination $= P(\text{contaminated cask}) \times 0.007 \times 0.006$
$= 4 \times 10^{-5} \times P(\text{contaminated cask})$

where this probability is on a per-cask basis. Instead of using the human reliability analysis trees as shown in Figure 5-2, this analysis could have been done using a standard fault-tree approach and symbols. The use of either approach could be left as a choice to the analyst. However, the human reliability analysis trees might more easily accommodate dependencies among different activities, which may be more difficult to represent in a standard fault-tree approach.

Regardless of the exact nature of the human reliability analysis, it can be incorporated into the larger fault tree, event tree analysis, which considers mechanical failures and external events. Figure 5-3 shows a hypothetical example of how the results of a human reliability analysis may

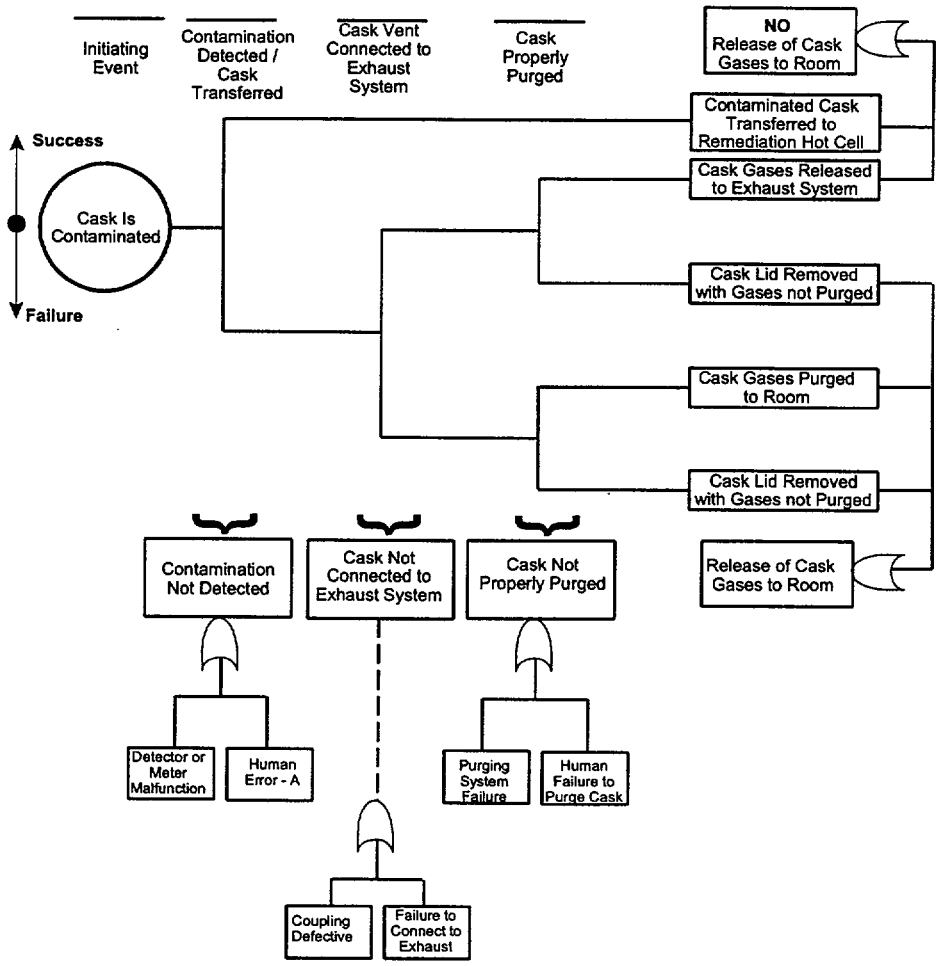

Figure 5-3. In Each Branch of the Event Tree Expanded as a Fault Tree, the Input to the OR Gate on the Left Side Represents a Mechanical Failure, While the Right Side Represents a Human Error

be incorporated into a larger analytical framework. An event tree approach is supported by fault trees for each branch in the event tree. Four possible outcomes, in two classes, are listed:

(i) The contaminated cask is transferred to the remediation hot cell [No Release]

(ii) The contaminated cask gases are released to the exhaust system [No Release]

(iii) The contaminated cask gases are purged into the room [Release]

(iv) The cask lid is removed without purging the contaminated cask gases, thereby allowing these gases to enter the room [Release]

For each branch of the event tree

(i) Contamination is detected, and the contaminated cask is transferred to the remediation hot cell

(ii) The cask vent port is properly connected to the exhaust system

(iii) The contaminated cask gases are properly purged, before the cask lid is removed

A fault can occur through a mechanical failure or through a human error. As shown in the event-tree and fault tree development, the original human reliability analysis tree must be subdivided and integrated with the possibilities for mechanical failure. This need for subdivision and integration would indicate that quantification of the human reliability analysis trees and their detailed development should be preceded by the incorporation of human error events into the general fault trees and event trees for the system under study. Changing the order of analysis in this way has two analytical benefits. First, definition of the human reliability analysis trees comes naturally from the development of the general analysis, thereby avoiding development of detailed human reliability analysis trees, that may later need to be modified to fit into the general framework. Second, the development of the human reliability analysis trees can proceed, at that point, as a separate activity and on an independent schedule (which may be advisable, if the information from DOE on design and operation is not produced at the same time). This hypothetical fault tree is not quantified because the details of the design are not available; however, the human error rates appear to be much higher ($\sim 10^{-3}$) than the rates anticipated for equipment failure. Since these events are combined with OR logic, the human errors are expected to have a significant impact, unless they are reduced by adding procedural or hardware redundancies to the system.

5.3.2 Example for Emplacement

As an example of applying a human reliability analysis methodology for the emplacement operations area, consider the following description of operations used to move a loaded disposal container into the emplacement drift (CRWMS M&O, 2000a):

> The locomotives will move the loaded transporter from the waste handling building to the North Portal, down the North Ramp to the North Ramp Extension, and from there to the preselected emplacement drift turnout. The train will generally follow the shortest route to the emplacement drift; however, orientation of the transporter is important depending on whether the emplacement drift is

going to be reached from the east or west mains. The reason is that the open deck of the transporter has to face the drift docking area for transfer of the waste package. The transporter and locomotives, once they enter the subsurface area in the early emplacement years, cannot rotate or change the orientation of the transporter. Therefore, the transporter must be oriented in the proper direction at the surface facilities using railroad turnouts.

Although the orientation of the transporter may be a minor element of the repository emplacement operations, it is instructive to consider it.

5.3.2.1 Qualitative Analysis

The qualitative analysis of potential human error would support the internal events analysis segment of the overall PCSA Tool. Consider the following types of hypothetical human errors related to this operation:

(i) The emplacement transporter is not oriented properly in the railroad turnout on the surface, but proceeds into the subsurface with an improper orientation

(ii) An improperly oriented transporter is returned from the emplacement drift without an attempt at emplacing the disposal container; alternatively, emplacement is attempted even though the transporter is oriented improperly

(iii) In negotiating the surface railroad turnout, the emplacement transporter derails, runs off the end of the turnout, or collides with the stop at the end of the turnout

(Iv) Exiting the surface railroad turnout, the emplacement transporter collides with another transporter that is traveling either toward (loaded) or away from (empty) the subsurface.

The consequences of these human errors would need to be determined by a separate analysis. For some of these events, it would be expected that various mitigating measures (both hardware and procedures) would prevent a release. In this regard, it is instructive to examine Table 5-1 which is an excerpt from Table 5-7 of the DOE Preliminary Preclosure Safety Assessment (CRWMS M&O, 2000a). Note that if hypothetical human error 1 (misoriented transporter) is followed by an attempt to emplace the disposal container in the subsurface anyway (hypothetical human error 2), then the frequency of waste package drops in the subsurface may increase. Furthermore, a qualitative change is that the disposal container may collide with the drift wall or other equipment, during an attempt to emplace the disposal container with the transporter in the wrong orientation. This design basis event is not currently listed. Similarly a transporter derailment or collision on the surface, as would be the case with hypothetical human errors 3 and 4, is not listed as a design basis event. This result illustrates how incorporation of human reliability considerations into a safety analysis may qualitatively change the scope of considerations; in this case, potential additional design basis events.

5.3.2.2 Quantitative Analysis

The quantitative analysis of potential human error would support the event sequence analysis segment of the overall PCSA Tool. Figure 5-4 shows a hypothetical event tree for the set of

Table 5-1. Excerpt from Table 5-7. Internal Event Sequences with No Release (CRWMS M&O, 2000a, pp. 5-25, 5-26)			
Event Group	**Design Basis Event**	**Event Location**	**Structures, Systems and Components Credited to Prevent a Release**
Waste Package Drops	Aboveground lifting system drops vertically oriented waste package	Disposal Container Handling System Cell	Disposal Containers
	Above ground lifting system drops horizontally oriented waste package	Disposal Container Handling System Cell	Disposal Containers
	Bed plate rolls out of waste package transporter	Subsurface	Disposal Containers
	Emplacement gantry drops horizontally oriented waste package	Subsurface	Disposal Containers
	Waste package falls onto a sharp object	Disposal Container Handling System Cell or Subsurface	Disposal Containers
Waste Package Collisions	Waste package collides in lag storage area	Disposal Container Handling System Cell	Disposal Containers
	Transporter collisions at normal operating speeds	Subsurface	Disposal Containers
	Transporter derails without tipover, but with waste package restraint failure	Subsurface	Disposal Containers
	Transporter derails with tipover	Subsurface	Disposal Containers
	Transporter door closes on waste package	Subsurface	Disposal Containers
	Operation of emplacement gantry causes waste package collision	Subsurface	Disposal Containers

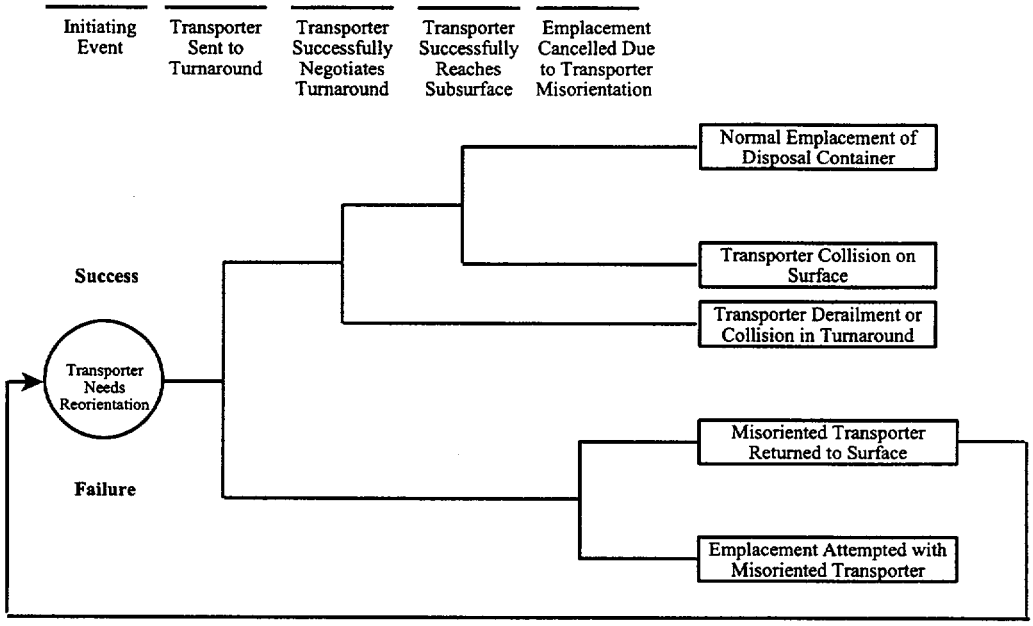

Figure 5-4. Event Tree Showing Hypothetical Human Error in Site Transportation

human errors postulated. Note that the event trees are not expanded by fault trees. In the case of transportation accidents, which comprise most of the human error events in this event tree, the use of actuarial data on railroad operations may be more appropriate than expanding each accident into a sequence of potential human errors.

5.3.3 Example for Receiving and Shipping

Like the other preclosure operations, there is little detail on the shipping and receiving operational area for the repository. A brief description follows (CRWMS M&O, 2000a):

> Transportation casks containing spent nuclear fuel and vitrified high-level waste and associated carriers are received at the repository waste entry point or security gate. The spent nuclear fuel and high-level waste are contained in casks equipped with impact limiters and personnel barriers. At the security gate, the cask carrier and offsite prime mover are inspected for contraband, sabotage, and radioactive contamination. Following inspection, the offsite prime mover is decoupled, and an onsite diesel-driven prime mover is used to transport the carrier and cask to the carrier preparation building. The carrier and cask transport system also transports empty transportation casks and associated carriers from the waste handling building to the carrier preparation building for preparation and, then to the repository security gate for dispatch from the site.

Although these operations are somewhat prosaic, there is the possibility for human error. A limited qualitative analysis of these operations might identify the following potential human errors:

(i) One onsite prime mover, with a transportation cask in tow, could collide with another prime mover

(ii) An onsite prime mover could collide with part of the Cask Preparation Building

(iii) A loaded onsite prime mover could overturn due to operator error

(iv) The entry and exit from the Cask Preparation Building, intended to be one way, could be violated by a prime mover in forward or reverse motion, resulting in a collision

(v) Offsite carriers might cause a fire or explosion onsite due to operator error

Although a human reliability analysis could be generated for each of these conditions, a more efficient and straightforward approach would be to use actuarial data to estimate the probabilities of postulated human error events of this type. Furthermore, existing regulatory and industrial guidance, if utilized, would help to reduce the probability of occurrence of events such as these or would mitigate the adverse effects, if they occurred. Excessive analysis and unnecessary detail should be avoided for more routine aspects of preclosure operations.

5.4 Importance of Human Reliability in Preclosure Safety Analysis

Because neither the broad outlines of the preclosure operations nor the details of human involvement in specific tasks are available at this time, the importance of human reliability to the overall risk of the facility cannot be estimated. However, as the broad outlines and details of operational procedures become available, quantitative estimates of the impact of human error should be able to be made. It is recommended that standard importance measures (Cheok, 1998), such as the risk achievement worth, and risk reduction worth be used to evaluate the importance of human reliability. The risk achievement worth can help to evaluate how important human reliability is to achieving the current risk level in the preclosure operations. The risk reduction worth can help to evaluate how improvements in human reliability may impact the preclosure risk level.

6 CONCLUSIONS, RECOMMENDATIONS, AND ISSUES

6.1 Conclusions

Arriving at specific, definitive conclusions about human reliability and (i) its role in preclosure repository safety and (ii) how it should be incorporated into the analysis of preclosure safety requires additional investigation, further development of the PCSA Tool, and, most importantly, further details about repository operations from DOE. A few general conclusions can be made.

- Human reliability could be a significant aspect of preclosure repository safety; a human reliability capability should be incorporated into the PCSA Tool.

- Many human reliability analysis methodologies are available, that can be adapted to evaluate repository safety; there is no need to develop methods especially for the repository analysis.

- With the possible exception of the underground facility (with the unique aspect of highly radioactive material in an underground environment), sufficient fundamental data exist to describe human reliability (basic human error probabilities and performance-shaping factor) for repository preclosure operations.

- The effort and detail of the human reliability analysis used as part of the PCSA Tool should be consistent with the level of detail in the remaining aspects of the analysis and with the availability of information about the repository design and operational characteristics.

- The NRC has been a leader in developing and applying human reliability analysis methods to problems of nuclear safety; adoption of methodologies developed or used by the NRC is advocated. Benefits of doing so include ready acceptance by the regulatory staff, NRC staff familiarity and experience in use of these methods, and familiarity and acceptance by the broader nuclear safety community. In particular, the **T**echnique for **H**uman **E**rror **R**ate **P**rediction and **A T**echnique for **H**uman **E**vent a**NA**lysis methodologies should be used, as applicable. The potentially significant large deployment cost for the **A T**echnique for **H**uman **E**vent A**NA**lysis methodology should, however, be recognized.

- A large body of guidance is issued by NRC related to human reliability analysis and human factors. The NRC staff should determine what part of this guidance, if any, may be applicable to preclosure safety. Specifying which guidance is applicable will help to constrain the issues that need to be addressed by human reliability analysis incorporated into the PCSA Tool.

- In order to perform meaningful evaluation of the influence of human reliability on repository preclosure safety, DOE needs to provide more details of design and operational plans.

6.2 Recommendations for Further Study

The following are recommendations for further study.

- Determine if mine safety records can provide insights into the types of human error induced by mining emergencies; a special focus would be how mine accidents could influence the effectiveness of repository staff in maintaining radiological safety while responding to a mine accident.

- To a limited extent, implement human reliability analysis (using the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology) into the PCSA Tool to test the ability to integrate these considerations into the computer tool. Hypothetical procedures and operations may need to be used in the absence of more detailed information from DOE. Partial implementation would also explore the applicability of the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology and databases. Such an implementation would investigate human-error- caused initiating events and modifications to the probability of success for mitigating systems. It would not explore the qualitative or quantitative impact of human error involved in response to an accident or other event.

- Further explore the qualitative or quantitative effects of human error involved in response to an accident or other event. An initial effort of this type would not necessarily attempt to quantify the probability of a particular outcome because the supporting data for such analyses are not available at this time.

- Consider an analysis of the information contained in the NRC Human Factors Information System (Section 3.2.2) to obtain a better qualitative description of human errors involved in spent nuclear fuel handling and to obtain a better quantification of the frequencies of such human errors.

- Seek a complete explanation from DOE of the probabilities used in the development of fault trees involving human reliability. When this information becomes available, check the analysis to determine if appropriate models have been used for human reliability and if they have been correctly applied.

- When sufficient information becomes available to support quantitative analyses, use standard importance measures to determine the relative importance of mechanical reliability and human reliability to the risk of preclosure repository operations. Consider integrating the capability to compute a variety of importance measures into the PCSA Tool.

6.3 Concerns Arising From This Study

6.3.1 Technical and Policy Issues for Consideration by NRC Staff

Concerns about NRC technical guidance include the following:

- The regulation and development of the repository may be enhanced by providing additions to existing guidance. In particular, the existing guidance on human factors

may not be sufficient for repository regulation, especially operations in the underground facility.

- Existing guidance developed for the control rooms and operating personnel of nuclear power plants may be applicable to repository preclosure operations; however, the degree to which that guidance, developed for substantially different facilities, may need to be determined.

6.3.2 Information Needs Related to DOE Operational Plans

Information needs related to DOE operational plans for the repository include the following.

- A key element in human reliability analysis is determination of performance shaping factors, so that basic human error probabilities may be appropriately modified; it may be important for DOE to identify how these factors will be determined and documented. In particular, in order to evaluate the adequacy of the DOE analysis, it will be important to know in what document or set of documents DOE will specify those items listed in Table 2-3 for each category of repository workers.

- DOE should indicated whether monitoring and control functions during the preclosure phase of repository development will be centralized or distributed.

- DOE should indicate its plans for how various kinds of persons at the repository will be trained, supervised, and controlled; in particular, DOE should indicated how persons that may be at the repository, but who are not radiation workers (see Table 3-1) will be trained, supervised, and controlled.

6.3.3 Information Needs Related to DOE Designs

Information needs related to DOE designs for the repository include the following.

- DOE should indicate what measures it plans to employ to assure that human factors considerations are being incorporated into the design of preclosure repository facilities.

- DOE should indicate the measures it is using to assure that designs reflect good practices regarding (i) ergonomics, (ii) instrumentation readability, (iii) control panel layout, (iv) wearable equipment and protective clothing (especially in the underground facility).

6.3.4 Information Needs Related to DOE Incorporation of Human Reliability Analysis Considerations into Operational Planning and Facility Design

Information needs related to DOE incorporation of human reliability analysis considerations into both operational planning and facility design include the following:

- DOE should articulate the strategy it plan to employ to develop preclosure designs and operational plans in a consistent, unified fashion, including the programmatic controls and management methods.

- If operational planning continues to lag behind facility design, DOE should address how it plans to: (i) demonstrate that designs meet the applicable regulatory requirements and (ii) assure that facility designs adequately compensate for potential human error.

7 REFERENCES

American National Standards Institute. "Selection, Qualification, and Training of Personnel for Nuclear Power Plants." ANSI/ANS–3.1–1993. Washington, DC: American National Standards Institute. 1993.

Atomic Energy Authority. *Human Reliability Assessor's Guide.* SRDA R11. Risley, Chesire, United Kingdom: Thomson House. 1995.

Bickel, J.H., D.L. Kelly, and T.J. Leahy. "Fundamentals of Probabilistic Risk Assessment (PRA)." DOE Contract No. DE–AC07–76ID01570. Idaho Falls, Idaho: EG&G Idaho, Inc. 1976.

Cheok, M.C., G.W. Parry, and R.S. Sherry. "Use of Importance Measures in Risk-Informed Regulatory Applications." *Reliability Engineering and System Safety.* Vol. 60. pp. 213–26. 1998.

CRWMS M&O. "Preliminary Preclosure Safety Assessment for Monitored Geologic Repository–Site Recommendation." TDR–MGR–SE–000009. Revision 00 ICN 01. Las Vegas, Nevada: CRWMS M&O. 2000a.

———. "Waste Handling Building System Document Description." SDD–HBS–SE–000001. Revision 00 ICN 01. Las Vegas, Nevada: CRWMS M&O. 2000b.

Dasgupta, B., R. Daruwalla, R. Benke, A. Chowdhury, and B. Jagannath. "Methodology for Assessment of Preclosure Safety for Yucca Mountain Project. Las Vegas, Nevada: Proceedings of the Ninth International Conference on High-Level Radioactive Waste Management, Las Vegas, Nevada, April 29–May 3, 2001. LaGrange Park, Illinois: American Nuclear Society. 2001.

Dasgupta, B., D. Daruwalla, R. Benke, and A.H. Chowdhury. "Development of a Tool and Review Methodology for Assessment of Preclosure Safety Analysis—Progress Report." San Antonio, Texas: CNWRA. 2000.

Emrit, R., R. Riggs, W. Milstead, J. Pittman, and H. Vandermulen. NUREG–0933, "A Prioritization of Generic Safety Issues." Washington, DC: NRC. June 2000.

Hollnagel, Erik. *Human Reliability Analysis—Context and Control.* San Diego, California: Academic Press. 1993.

Kemeny, J.G., Chairman "Report of President's Commission on the Accident at Three Mile Island—The Need for Change: The Legacy of TMI." New York: Pergamon. 1979.

NRC. SECY–00–0053, "NRC Program on Human Performance in Nuclear Power Plant Safety." Washington, DC: NRC. 2000a.

———. NUREG–1624, "Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)." Revision 1. Washington, DC: NRC. 2000b.

———. "Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants." Washington, DC: NRC. 2000c.

———. "Carolina Power & Light Company: H.B. Robinson Steam Electric Plant, Unit No. 2 Environmental Assessment and Finding of No Significant Impact." Docket No. 50-261. *Federal Register.* Vol. 64, No. 66. pp. 17019–17021. Washington, DC: U.S. Government Printing Office. 1999.

———. NUREG–1624, "Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)." Draft Report For Comment. Washington, DC: NRC. 1998a.

———. SECY–98–244, "NRC Human Performance Plan." Washington, DC: NRC. 1998b.

———. NUREG/BR–0184, "Regulatory Analysis Technical Evaluation Handbook." Washington, DC: NRC. 1996.

———. NUREG–1489, "A Review of NRC Staff Uses of Probabilistic Risk Assessment." Washington, DC: NRC. 1994.

———. NUREG/CR–2300, "PRA Procedure Guide. A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants, Final Report. Volumes 1 and 2." Washington, DC: NRC. 1983.

———. NUREG–0899, "Guidelines for the Preparation of Emergency Operating Procedures." Washington, DC: NRC. 1982.

———. NUREG–0799, "Draft Criteria for Preparation of Emergency Operating Procedures." Washington, DC: NRC. 1981a.

———. NUREG–0700, "Guidelines for Control Room Design Reviews." Washington, DC: NRC. 1981b.

———. NUREG–0835, "Human Factors Acceptance Criteria for the Safety Parameter Display System." Draft Report for Comment. Washington, DC: NRC. 1981c.

———. NUREG–0801, "Evaluation Criteria for Detailed Control Room Design Review." Draft Report. Washington, DC: NRC. 1981d.

———. NUREG–1280, "Power Plant Staffing." Washington, DC: NRC. 1980a.

———. NUREG–0731, "Guidelines for Utility Management Structure and Technical Resources." Washington, DC: NRC. 1980b.

Rogovin, M. and G.T. Frampton, Jr. "Three Mile Island: A Report of the Commissioners and to the Public." NRC Special Inquiry Group. Washington, DC: NRC. 1980.

Sandia National Laboratories. "Human Reliability Analysis." http://reliability.sandia.gov/Human_Factor_Engineering/Human_Reliability_Analysis/human_reliability_analysis.html. 2001.

Schneider, K.J. (coordinator). NUREG/CR–2873, "Nuclear Fuel Cycle Risk Assessment: Descriptions of Representative Non-Reactor Facilities." Volumes 1 and 2. Washington, DC: NRC. September 1982.

Smith, D.J. *Reliability, Maintainability and Risk.* 5th Edition. Oxford: Butterworth-Heinemann. 1997.

Swain, A.D. and H.E. Guttamann. NUREG/CR–1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." SAND 80-0200. Washington, DC: NRC. 1983.

Swain, A.D. "Comparative Evaluation of Methods for Human Reliability Analysis." GRS–71. Garching: Gesellschaft für Reaktorsicherheit. 1989.

Swain, A.D. NUREG/CR–4772, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure." Washington, DC: NRC. 1987.

Woods, D.D., E.M. Roth, and H. Pople. NUREG/CR–4862, "Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment." Volume 1. Washington, DC: NRC. 1987.