PCSA TOOL DEVELOPMENT
PROGRESS REPORT II

Prepared for

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

Prepared by

B. Dasgupta
R. Benke
B. Sagar
R. Janetzke
A. Chowdhury

Center for Nuclear Waste Regulatory Analyses
San Antonio, Texas

September 2002

PREVIOUS REPORT IN SERIES

Name	Date
Development of a Tool and Review Methodology for Assessment of Preclosure Safety Analysis—Progress Report	September 2000
PCSA Tool Development—Progress Report	September 2001

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

FIGURES

FIGURES (continued)

FIGURES (continued)

Figure | Page

TABLES

Table | Page

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 views or regulatory position of the NRC.

The authors thank W. Patrick, G. Wittmeyer, and M. Smith for technical reviews and B. Sagar for programmatic review. The authors appreciate suggestions and contributions from M. Nataraja, B. Jagannath, and A. Henry of NRC. The Visual Basic coding for the PCSA Tool was written by A. Lozano and D. Stead; their contributions are greatly appreciated. Authors also thank K. Stiles and C. Patton for acceptance testing of the PCSA Tool Version 1.0.

The authors are also thankful to A. Ramos for skillfully typing and preparing the final report and C. Cudd, C. Gray, and J. Pryor for providing a full range of expert editorial services in the preparation of the final document.

QUALITY OF DATA, ANALYSES, AND COMPUTER CODES

DATA: No CNWRA-generated original data are contained in this report. Data used in this report are primarily equipment failure rate actuarial data from other sources. Each data source is cited in the report.

ANALYSES AND CODES: The PCSA Tool software is being developed following CNWRA Technical Operating Procedure–018, which implements the requirements of the CNWRA Quality Assurance Manual. The tool uses Microsoft® products and was developed to run on a personal computer using the Windows NT operating system. Hereafter, the term Microsoft will be used without the registered trademark symbol. The PCSA Tool is being developed using Visual Basic 6.0; Microsoft Access 97 SR–2; SAPHIRE Version 6.70; RSAC Version 5.2 codes; MELCOR Version 1.8.5; InstallShield Professional–Windows Installer Edition 2.0; CrystalReports Developer Edition; Component Chart 7.0; and a suite of utility codes. No other versions of the previously listed codes were used in this document. SAPHIRE and RSAC are distributed by Radiation Safety Information Computational Center, Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37381-6362. MELCOR is developed, supported, and distributed by Sandia National Laboratories, Albuquerque, New Mexico 87185. InstallShield Professional–Windows Installer Edition 2.0 is distributed by InstallShield Software Corporation, Schaumburg, Illinois 60173-5108. Crystal Reports Developer Edition Version 8.5 is distributed by Crystal Decisions, Inc., Palo Alto, California 94301-2413. Component Chart 7.0 is distributed by ComponentOne, Pittsburgh, Pennsylvania 15213. The suite of utility codes, which consists of PCSA_LHS Version 1.0, PCSA_LHS INP Version 1.0, PCSA_PROB Version 1.0, PCSA_COMBAN Version 1.0, and PCSA_RSACRD Version 1.0, were developed at CNWRA using the Lahey LF90 Fortran Compiler. An additional suite of utility codes, PCSA_IETCCDF Version 1.0, and PCSA_RISKCCDF Version 1.0, is being developed by CNWRA using the Lahey LF90 Fortran Compiler. Visual Basic 6.0, MSAccess 97, InstallShield, Component Chart, and Crystal Reports software packages do not conduct any computations and, hence, do not need to be put under CNWRA Configuration Control. The acquired computer codes SAPHIRE, RSAC, and MELCOR, which will not be modified, are under CNWRA Configuration Control.

InstallShield Professional–Windows Installer Edition 2.0 is used to create a PCSA Tool installation setup for Windows NT for distribution to the staff. The setup distribution installs SAPHIRE, RSAC, and MELCOR codes and the CNWRA-developed applications. Microsoft Access software will not be required on the user's computer.

REFERENCES

Gauntt, R.O., R.K. Cole, C.M. Erickson, R.G. Gido, R.D. Gasser, S.B. Rodriguez, M.F. Young, S. Ashbaugh, M. Leonard, and A. Hill. NUREG/CR–6119, "MELCOR Computer Code Manuals." Rev. 2. Washington, DC. NRC. October 2000.

Idaho National Engineering Laboratory. "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 6.0, Saphire Reference Manual." Idaho Falls, Idaho: Idaho National Engineering Laboratory. 1998.

Wenzel, D.R. "The Radiological Safety Analysis Computer Program (RSAC–5) User's Manual, WINCO–1123." Rev. 1. Idaho Falls, Idaho: Idaho National Engineering Laboratory. 1994.

EXECUTIVE SUMMARY

The proposed geologic repository at Yucca Mountain will be designed for the permanent disposal of approximately 70,000 MTU of spent nuclear fuel and high-level waste. During the preclosure period, the facility will receive and handle casks containing the waste in sealed disposal canisters or in the form of spent nuclear fuel assemblies. Using a series of remote operations, the waste will be transferred into disposal packages and transported underground for emplacement into drifts.

In its license application, the U.S. Department of Energy (DOE) will present a preclosure safety analysis of the proposed geologic repository operations area. This part of the license application must demonstrate compliance with the preclosure performance objectives outlined in 10 CFR 63.111 and the preclosure safety analysis requirements specified in 10 CFR 63.112.

The main hazards associated with the preclosure phase of the proposed repository arise from (i) a large inventory of radioactive wastes that will be progressively accumulated onsite; (ii) a large number of surface-processing operations that will have to be performed, many in parallel, to support the schedule; and (iii) subsurface operations that involve transportation and emplacement of waste packages.

The purpose of the preclosure safety analysis is to ensure that all relevant hazards that could result in radiological consequence have been evaluated and appropriate protective measures have been identified. The preclosure safety analysis also identifies the structures, systems, and components that are important to safety. Structures, systems, and components that are important to safety are defined as those whose failure would result in a radiological dose to a member of the public or a worker that exceeds the limits specified in 10 CFR 63.111(a) and (b).

This report documents the development, to date, of the preclosure safety analysis review methodology and PCSA Tool Version 2.0 Beta. The computer code, PCSA Tool, has been developed for use by the U.S. Nuclear Regulatory Commission (NRC) and the Center for Nuclear Waste Regulatory Analyses staffs to review the DOE preclosure safety analysis. The report formulates a risk-informed, performance-based methodology for performing the preclosure safety analysis and implement the procedures in Yucca Mountain Review Plan (NRC, 2002a). It also documents development of (i) a database consisting of appropriate information and data for site-specific, naturally occurring, and human-induced events from the review of referenced sources; (ii) a hazards analysis capability for surface and subsurface facility operations using standard qualitative methodology, including human reliability; (iii) an event sequence analysis capability based on quantitative methods; (iv) a capability for determining radiological consequences to the public with either point estimate or probabilistic calculations and to workers with a point estimate calculation; (v) a safety assessment capability based on the frequency and dose limits specified in 10 CFR Part 63; (vi) a capability to evaluate total aggregate risk as an additional option to gain risk insight, though not required to comply with the regulation; (vii) a capability to identify structures, systems, and components important to safety based on available information; and (viii) a failure rate, failure mode, and checklist databases from available literature on equipment and systems for operational hazard analysis. Additionally, the application of the tool has been demonstrated by conducting preliminary analyses of a selected area of the assembly transfer system in the proposed Waste Handling Building.

The PCSA Tool uses Visual Basic as the primary programming language to develop a graphical user interface to connect a set of diverse software and Microsoft Access to create the project database and the equipment failure rate database. Event tree and fault tree analyses are performed using SAPHIRE codes. The RSAC code is used to calculate the radiological consequence to a member of the public from the atmospheric release of radioactive material for radiological dose calculations.

The power of the PCSA Tool lies in enabling the user independently to evaluate and probe critical parts of the DOE preclosure safety analysis. Because the reviews can be performed for the entire system or a component of the system in an efficient and systematic manner, the PCSA Tool facilitates an expeditious and thorough review of DOE safety analysis. The tool enables the NRC to keep the analyses current with the evolving DOE design and, if the DOE is granted a construction authorization, to carry forward the review from the construction authorization to the receive and possess waste phase of licensing. The PCSA Tool will also be used to document and check that key safety features relied on by DOE in the design during the construction authorization phase are actually implemented in the receive and possess waste phase. Furthermore, the tool (appropriately updated) will be used to review the DOE safety analyses during the operation of the facility until its permanent closure.

Future work on the PCSA Tool will include modifications based on the verification and validation tests and suggestions by the users. The feasibility of incorporating software reliability analyses will be considered. A capability to review DOE analysis of seismic events will be incorporated, and addition of review capabilities for fire hazards and other external hazards (e.g., flood and tornado) in the PCSA Tool will be considered. As more repository design details become available, the failure rate database containing the failure rate of components will be expanded to include design-specific equipment, controls, and instruments. Improvements to the consequence analysis module will focus on the transfer of information from RSAC into the PCSA Tool interface to allow probabilistic calculations for the advanced RSAC input. In addition to the average boiling water reactor and pressurized water reactor characteristics of commercial spent nuclear fuel, bounding characteristics of other waste types may be added into the source term options. Possible inclusion of MACCS2 (MELCOR Accident Consequence Code System) into the PCSA Tool will be considered to allow comparisons with the RSAC results. Finally, the module for the structures, systems, and components important to safety will be modified based on the staff position on the review methodology.

1 INTRODUCTION

1.1 Background

As part of any application for a license to construct and, if a construction authorization is granted, any subsequent application for amendment for a license to receive and possess waste at the proposed geologic repository at Yucca Mountain, Nevada, the U.S. Department of Energy (DOE) must conduct and present a safety analysis of the proposed geologic repository operations area for the period until permanent closure. This preclosure safety analysis is necessary to demonstrate compliance with the preclosure performance objectives in 10 CFR 63.111 that meet the requirements specified in 10 CFR 63.112. A proper preclosure safety analysis requires a systematic examination of the site, design, and hazards stemming from natural phenomena and human-induced activities that have the potential for initiating event sequences during the preclosure period, and radiological dose consequences to the public and workers. An initiating event can be a natural or human-induced occurrence that causes an event sequence with the potential for a radiological dose. Natural events result from processes in nature and are normally external to the facility, such as seismicity, tornadoes, and floods. Human-induced events, on the other hand, are hazards caused by human actions either from the internal operations at the facility, such as a cask drop, or external to the facility, such as an aircraft crash. In addition, demonstrating compliance with the regulatory limits, another goal of the preclosure safety analysis is to identify structures, systems, and components important to safety. Detailed information about the site; the design of structures, systems, and components; operational methods; naturally occurring and human-induced initiating events; event sequences; consequences to public and workers from potential release of radiological material; and the role of structures, systems, and components to prevent or mitigate radiological dose are needed to identify structures, systems, and components important to safety.

The preclosure safety analysis considers the probability of event sequences, taking into account the uncertainty and variability in the data that support the probability calculations. Event sequences are identified based on well-established methods that may combine probabilistic and deterministic approaches. Potential doses to workers and the public are calculated for the identified event sequences. These calculated doses are compared to regulations dose criteria to determine compliance. The preclosure safety analysis also identifies and describes the controls necessary to prevent event sequences from occurring or to mitigate consequences of these event sequences, and it identifies measures necessary to ensure the availability of structures, systems, and components important to safety. In addition, the preclosure safety analysis also defines the design criteria and technical specifications necessary to ensure structures, systems, and components perform their intended safety functions. Structures, systems, and components important to safety are identified by importance analysis based on compliance criteria; structures, systems, and components important to safety also may be categorized based on their relative safety significance with risk-informed insights gained from the preclosure safety analysis. This categorization allows design and application of quality assurance controls to be applied through a graded quality assurance program. DOE currently plans to group structures, systems, and components into three categories based on safety and risk significance and to implement a graded quality assurance program based on this safety and risk significance (CRWMS M&O, 2000a; DOE, 2001a).

The preclosure safety analysis review philosophy is that (i) DOE must demonstrate, through a preclosure safety analysis, that the repository will be designed, constructed, and operated to meet the preclosure performance objectives (dose limits); (ii) the staff will focus the review on the structures, systems, and components important to safety and on whether the design meets the performance objectives; and (iii) the review will consider the safety and risk significance of structures, systems, and components important to safety.

The proposed geologic repository will be developed much like a large mine (Hossain, et al., 1997). It will combine two types of primary facilities: waste handling and temporary storage facilities constructed on the ground surface and underground disposal facilities constructed about 320 m [1,050 ft] beneath the Earth's surface. Surface facilities that include the waste handling and temporary storage facilities will be provided for receiving, preparing, and packaging nuclear wastes received at the site before sending them underground for disposal. The underground facilities include the underground structure; backfill materials, if any; and ramps, shafts, and boreholes, including seals. The surface facilities will be connected to the underground structure by ramps and shafts that (i) allow removal of excavated material from the underground drifts, (ii) provide access to conduct performance confirmation tests, (iii) provide access for staff and equipment, (iv) facilitate ventilation of the underground area, and (v) allow transfer of waste from the surface to the underground storage area and vice versa. After the repository has been filled with approximately 70,000 MTU of waste and the performance confirmation testing program has been completed, the surface facility will be decontaminated and decommissioned, and all ramps, shafts, underground drifts, and boreholes will be closed appropriately and decommissioned.

The waste isolation concept for a repository consists of multiple barriers, both natural and engineered, that act together to contain and safely isolate the waste. The engineered barrier subsystem includes the waste packages; engineered components and systems other than the waste packages (e.g., drip shields); the underground structure; backfill materials, if any; and openings that penetrate the underground structure (e.g., ramps, shafts, and boreholes, including seals). The waste package consists of the waste forms, either spent nuclear fuel or solidified high-level waste, and any containers, shielding, packing, and other absorbent materials immediately surrounding an individual waste container. The geological, hydrological, chemical, and geomechanical features of the high-level waste repository site constitute natural barriers to the long-term movement of radionuclides.

A comprehensive list of natural and human-induced events at the geologic repository operations area of the proposed high-level waste repository at Yucca Mountain needs to be prepared based on known or estimated geological, seismological, hydrological, geomechanical, geochemical, and meteorological characteristics of the site and surface, subsurface, and airborne activities that occurred in the past, are currently ongoing, or could potentially occur in the future. Yucca Mountain is located in the basin and range province of the western United States within the region known as the Great Basin. An overview of the characteristics of the Yucca Mountain site is provided by the DOE (1998). The generation of a comprehensive list of events from the facility operations will be dominated by the complexity of construction and operations in the geologic repository operations area. Contingent on U.S. Nuclear Regulatory Commission (NRC) issuance of construction authorization, construction will begin with developing initial portions of the surface and subsurface facilities. Following the initial construction, underground openings will be developed concurrently with waste emplacement operations (DOE, 1998). This establishment of underground openings will take place without interference with waste emplacement operations. Tunnel-boring machines will be used for most underground excavations. Other mechanical methods such as roadheader machines may be employed where use of a tunnel-boring machine is not feasible. Other construction-related activities will include installation of ground supports and transportation of excavated rock from the subsurface to the surface. The waste handling and emplacement operations include receiving transportation casks with spent nuclear fuel and vitrified high-level waste; transferring transportation casks to the Waste Handling Building; transferring waste from transportation casks to disposal containers, including blending of waste; transporting disposal containers underground; and emplacing waste using an emplacement gantry.

Because DOE has not finalized the design and operations of the proposed repository, including the waste package, a comprehensive hazards list based on site information and facility design is not available at this time. However, DOE developed a generic list of natural hazards and initiating events for the geologic repository operations area at Yucca Mountain (CRWMS M&O, 1999a; DOE, 2001a). Additionally, DOE developed a preliminary list of operational hazards associated with the preclosure operations (CRWMS M&O, 1999b,c; DOE, 2001a). These generic lists serve as the starting point to develop a comprehensive list of site- and facility-specific hazards that have potentials to initiate event sequences with radiological consequences. Only events that have a probability of 1×10^{-6} or more per year are included. This probability is based on the definition of Category 2 events in 10 CFR Part 63 and assumption of a 100-year preclosure period.

1.2 Objective and Scope

The overall objective of this activity is to develop a review methodology and PCSA Tool that can be used by the NRC and Center for Nuclear Waste Regulatory Analyses (CNWRA) staffs to evaluate the adequacy of the DOE safety case in demonstrating that preclosure performance requirements will be met, and to assess whether the identification of structures, systems, and components important to safety is acceptable.

The overall scope of this activity involves formulating a methodology for performing the preclosure safety analysis and developing a computer code, PCSA Tool Version 2.0 Beta, using existing integrated safety analysis methodology and available probabilistic risk analysis software packages, to assist in reviewing the DOE preclosure safety analysis. This report documents development of (i) a database consisting of appropriate information and data for site-specific, naturally occurring, and human-induced events from the review of referenced sources; (ii) a hazards analysis capability for surface and subsurface facility operations using standard qualitative methodology, including human reliability; (iii) an event sequence analysis capability based on quantitative methods; (iv) a capability for determining radiological consequences to the public with either point estimate or probabilistic calculations and to workers with a point estimate calculation; (v) a safety assessment capability based on the frequency and dose limits specified in 10 CFR Part 63; (vi) a capability to evaluate total aggregate risk as an additional option to gain risk insight, though not required to comply with the regulation; (vii) a capability to identify structures, systems, and components important to safety based on available information; and (viii) a failure rate, failure mode, and checklist database from available literature for the equipment and systems for operational hazard analysis. Additionally, the application of the tool has been demonstrated by conducting preliminary analyses of a selected area of the assembly transfer system in the proposed Waste Handling Building.

During fiscal year 2002, the major tasks performed were (i) improving and modifying all modules of the tool to make the code more efficient and user friendly, (ii) incorporating the human reliability analysis, and (iii) incorporating risk assessment methodologies. In addition, progress was made in testing of the PCSA Tool and related software. Acceptance testing of the functional behavior of the tool was conducted and code fixes were made based on test results. Testing of the consequence module resulted in several improvements to the PCSA Tool. The improvements included changes in functionality, correction of error messages, updates to default values, and modifications to window contents and their description. Validation of the MELCOR code, used in the consequence module, was completed. Validation of the RSAC code, used in the consequence module, will continue during fiscal year 2003.

1.3 PCSA Tool Overview

The computer code PCSA Tool has been developed for use by NRC and CNWRA staffs to implement procedures in the Yucca Mountain Review Plan (NRC, 2000a) to review the DOE preclosure safety analysis of the proposed geologic repository at Yucca Mountain. This tool provides a risk-informed, performance-based methodology for the review. The original version of the PCSA Tool was released in September 2000. Since then, PCSA Tool Version 1.0 Beta was released in September 2001, followed by PCSA Tool Version 1.0 in July 2002. PCSA Tool Version 2.0 Beta is scheduled for release in October 2002.

The tool provides the capability to review the DOE safety analysis through independent analyses of risk-relevant aspects. The tool applies the preclosure safety analysis review methodology, which is based on the requirements for the preclosure safety analysis of the geologic repository operations area in 10 CFR 63.112 and the preclosure performance objectives in 10 CFR 63.111. The PCSA Tool addresses the relevant sections of NRC (2002a), which is a site-specific review guidance document that implements site-specific, risk-informed, performance-based regulation at 10 CFR Part 63. NRC (2002a) applies a risk-informed, performance-based review philosophy that (i) considers the preclosure safety analysis as the main vehicle by which DOE would demonstrate that the repository will be designed, constructed, and operated to meet the specified performance objectives throughout the preclosure period; (ii) focuses the review on the design of the structures, systems, and components important to safety in the context of the capability of the design to meet the performance objectives; and (iii) further focuses the review of risk-significant structures, systems, and components important to safety.

The PCSA Tool has been structured in a modular fashion that allows selective use of various capabilities built into the tool. The PCSA Tool includes the following capabilities to aid in the review.

- Information storage and retrieval: information about the repository design, operations, and equipment based on DOE data and sources, and independent safety-related data on natural hazards, human-induced hazards, equipment reliability, and others.

- Qualitative and quantitative analysis tools: tools to guide reviewers in making qualitative findings related to completeness and adequacy of support for DOE findings, and tools to check quantitative findings produced by DOE.

- Documentation: review findings, rationale, support, and references.

The PCSA Tool modules address

- Segregation of the repository into functional areas and subareas and storage of relevant data for each subarea

- Identification of naturally occurring and human-induced, and operational hazards initiating events based on several qualitative hazard analysis techniques

- Quantification of event sequence frequencies evaluation of radiological doses to the members of the public and facility workers

- Safety assessment of the repository assessment of repository operations to determine compliance with performance objectives

- Identification of structures, systems, and components that would be relied on to meet regulatory performance objectives

Although the PCSA Tool addresses acceptance criteria and review methods related to the preclosure safety analysis described in Section 4.1.1 of NRC (2002a), not every element of the review has a counterpart in the PCSA Tool. Some acceptance criteria and review methods delve into details of the site and the design of structures, systems, and components that are beyond the scope of the PCSA Tool. Table 1-1 describes the relationship of various PCSA Tool modules to different sections of NRC (2002a) and particular acceptance criteria and review methods.

The tool combines useful components of the integrated safety analysis methodologies used in the chemical industry (NRC, 2001) and the probabilistic risk assessment capabilities used in safety assessment of nuclear power reactors (Hickman, et al., 1983). The PCSA Tool has been designed to serve three purposes: (i) store and retrieve data and information in a database, (ii) perform confirmatory analyses using off-the-shelf and specially designed software, and (iii) documentation of review results. The PCSA Tool uses Visual Basic as the primary programming environment to develop a graphical user interface for the databases and for analytical tools. Some of the software packages incorporated in the tool include (i) the SAPHIRE code for event sequence analyses and quantitative frequency evaluations using event tree and fault tree models, (ii) the RSAC code to calculate the radiological consequences to a member of the public from an atmospheric release of radioactive material using deterministic and probabilistic approaches, and (iii) the MELCOR code to estimate building discharge fractions. The project database allows segmenting the repository into several functional areas for the creation of input data for and storage of output data from model analyses using acquired software, displaying graphical results, and generating reports for each functional area. In addition, the tool contains static databases that include the component failure rates obtained from actuarial data and literature citation for source of the data and other information such as checklist of failure modes for assisting in hazard analysis.

Table 1-1. Crosswalk of PCSA Tool*			
PCSA Tool Functions	**Yucca Mountain Review Plan**	**Review Method**	**Acceptance Criteria**
Functional area database	Section 4.1.1.2 Section 4.1.1.7	1,2,3,4,5,6 1	1,2,3,4,5,6 1
Hazard analysis and identification of initiating events	Section 4.1.1.3.3	2,3,4,5	2,3,4,5
Event sequence frequency analysis	Section 4.1.1.4.3	2	2
Public and worker dose analysis	Section 4.1.1.5.1.3 Section 4.1.1.5.2.3	1,2 1,2	1,2 1,2
Safety assessment	Section 4.1.1.5.1.3 Section 4.1.1.5.2.3	3 3	3 3
Identification of structures, systems, and components	Section 4.1.1.6.3	1	1
*NRC. NUREG–1804, "Yucca Mountain Review Plan—Draft Report for Comment." Revision 2. Washington, DC: NRC. March 2002.			

The PCSA Tool allows the NRC and CNWRA staffs to conduct and document independent and confirmatory analyses for part or the entire repository system. The tool provides the flexibility to review in detail all aspects of the safety analysis (e.g., hazard analysis, event frequency analysis, consequence analysis) in a functional area or only a selected aspect of the safety analysis. The tool, however, uses information from all the functional areas for the overall repository safety assessment and the identification of structures, systems, and components. The modules in the tool allow the staff to perform independent review analyses and to store results of these reviews in a structured and systematic manner. Results of a review may be abstracted, as appropriate, for use in other modules of the tool. Alternatively, the modules can also work independently. The abstraction of review results and input to another module are not necessarily automatic; rather, the appropriate information is generally input manually into another module to enable a tailored review. The tool can be used to conduct are in-depth review by confirmatory analysis of event frequency and consequence analyses applying either point estimate or probabilistic approaches. The database permits storage of alternative analyses for safety assessment and the identification of structures, systems, and components important to safety. In addition, the database structure in the PCSA Tool handles updated reviews of the DOE safety analysis throughout the licensing process (i.e., through the construction authorization, receipt and possession of waste, and permanent closure phases).

1.4 Report Organization

This report presents the formulation of a risk-informed, performance-based methodology for reviewing the DOE preclosure safety analysis and documents the development of computer code PCSA Tool Version 2.0 Beta. This report is the third in a series of progress reports on the PCSA Tool development (Dasgupta, et al., 2000, 2001a). With the intention to formalize the overall layout of the report and to serve as a manual for PCSA Tool, chapters in this progress report have been rearranged and organized in a sequence maintaining consistency with the applicable sections in preclosure safety analysis in NRC (2002a). Features and capabilities, when added in the future versions of the tool, will be accommodated with this framework. Some chapters from Dasgupta, et al. (2001a) have been modified to report additional features in the respective modules and some chapters (especially 5 and 10 and related appendices) have not been changed.

Chapter 2 discusses the preclosure safety analysis methodology including preclosure requirements from relevant sections of 10 CFR Part 63 and applicable guidance acceptance criteria in NRC (2002a). This chapter also addresses implementation of the methodology in the PCSA Tool including the overall structure of the tool and its functionality. The hazard analysis methodology for naturally occurring external hazards and operational hazards is discussed in Chapter 3. This chapter presents a generic list of naturally occurring external hazards and a set of criteria to identify hazards that may potentially cause release of radioactive material from the repository. Four qualitative hazard analysis techniques—failure modes and effects analysis, what-if analysis, energy method, and human-reliability—are discussed to identify hazards related to facility operations. The PCSA Tool functions to conduct hazard analysis are described. In addition, the chapter also addresses the identification of initiating events for further safety analysis. The text in Chapter 5, which deals with the failure of components and equipment, has not been modified for this progress report; however, the failure rate database will be reviewed in fiscal year 2003. Chapter 6 explains the quantitative analyses techniques, event tree, fault tree, and human reliability tree. The tool is used to conceptualize event scenarios for fault tree and event tree analysis in a systematic manner and record results from analysis using SAPHIRE software. The tool functions in this module have been substantially modified for increased efficiency. Discussion of quantitative human reliability analysis has been added in this chapter, although the tool capability will be supplemented later. Chapter 7 describes the radiological dose consequence analysis for workers and public. The tool develops input data, executes, and displays output from RSAC software for calculating public dose. In addition, the tool offers a similar functionality to estimate building discharge using MELCOR software. The tool has the capability to conduct point estimate and probabilistic analysis of public dose. The worker dose analysis is currently performed through an in-built spreadsheet calculation. Chapter 8 describes the compliance assessment methodology and tool functionality. The tool conducts safety assessment by evaluating the capability of the proposed repository to meet regulatory performance objectives defined in 10 CFR 63.111 by comparing (i) annualized frequency-weighted dose and combination of event sequences for Category 1 event sequences, and (ii) individual event sequence dose for Category 2 event sequences. In addition, the tool evaluates total aggregate risk using point estimate and probabilistic approach. DOE is not required to demonstrate compliance by evaluating total risk. This feature is an additional one incorporated in the tool to gain risk insight. Chapter 9 describes a conceptual methodology to identify structures, systems, and components important to safety. Use of all modules and features of PCSA Tool is demonstrated through example problems in Chapter 10, the text of which has not been modified for this progress report. Chapter 11 describes the future work, and Chapter 12 outlines the conclusions.

2 DESCRIPTION OF PRECLOSURE SAFETY ANALYSIS

The objective of the PCSA Tool is to provide an independent capability to the U.S. Nuclear Regulatory Commission (NRC) and Center for Nuclear Waste Regulatory Analyses (CNWRA) staffs to review the U.S. Department of Energy (DOE) preclosure safety analysis. The main features of the PCSA Tool are its capabilities to (i) perform safety analyses for the entire operation or selected operations; (ii) systematically identify structures, systems, and components important to safety; (iii) accommodate changes in the design and related site characteristics; and (iv) maintain continuity of safety analyses from the construction authorization phase through the receipt and possession of waste phase of the license application review. Furthermore, the tool can be used to review the DOE safety analysis during the operation of the facility until its permanent closure. This chapter describes the preclosure safety analysis methodology and PCSA Tool modules and structure.

2.1 Requirements of 10 CFR Part 63

The risk-informed, performance-based regulation 10 CFR Part 63 provides the general scope, requirements, and objectives of the preclosure safety analysis to ensure safety of the public and workers during the operational phase of the repository until permanent closure. As required in 10 CFR 63.21(c)(5), the DOE must include a preclosure safety analysis in its license application and demonstrate compliance with the performance requirements in 10 CFR 63.111(a), (b), and 63.204. As defined in 10 CFR 63.2 and 63.102(f), preclosure safety analysis is a systematic examination of the repository site and the facility design, and evaluation of potential hazards, initiating events, event sequences, and dose consequences to workers and the public. Other terms associated with preclosure safety analysis, such as initiating event, event sequence, important to safety, and Category 1 and 2 event sequences are also defined in 10 CFR Part 63. The requirements for preclosure safety analysis are specified in 10 CFR 63.112.

An important purpose of the preclosure safety analysis is to identify structures, systems, and components important to safety. The structures, systems, and components important to safety, as defined in 10 CFR 63.2, are those engineered features of the geologic repository operations area whose function is to (i) provide reasonable assurance that high-level waste can be received, handled, packaged, stored, emplaced, and retrieved without exceeding the requirements of 10 CFR 63.111(b)(1) for Category 1 event sequences; or (ii) prevent or mitigate Category 2 event sequences that could result in radiological exposure exceeding the values specified in 10 CFR 63.111(b)(2) to any individual located on or beyond any point on the boundary of the site. The regulation at 10 CFR Part 63 does not require any particular methodology to be used, allowing DOE flexibility in structuring its preclosure safety analysis.

2.2 Yucca Mountain Review Plan

The Yucca Mountain Review Plan (NRC, 2002a) provides staff with guidance for determining whether the facility can be constructed and operated in compliance with the applicable NRC regulations to ensure repository safety before and after permanent closure. The Yucca Mountain Review Plan will be used by the staff to review any license application for construction authorization and, if a construction authorization is granted, any license to receive and possess waste.

The Yucca Mountain Review Plan (NRC, 2002a) implements the site-specific, risk-informed, and performance-based regulation, of 10 CFR Part 63. It outlines a risk-informed, performance-based review philosophy that (i) requires DOE to demonstrate through its preclosure safety analysis that the repository will be designed, constructed, and operated to meet the specified performance objectives throughout the preclosure period; (ii) enables NRC staff to focus the review on the design of the structures, systems, and components important to safety in the context of the capability of the design to meet the performance objectives; and (iii) permits NRC staff to proportionately focus its review on high-risk-significant structures, systems, and components important to safety.

Each section on preclosure safety analysis in the Yucca Mountain Review Plan (NRC, 2002a) provides guidance on information to be reviewed by NRC, the review basis, how the review is accomplished, acceptable means to demonstrate compliance with regulations, and the potential conclusions regarding applicable sections in 10 CFR Part 63. A sequence of evaluations leading from site characterization to compliance with 10 CFR Part 63 preclosure performance objectives including identification of structures, systems, and components is addressed in Section 4.1.1 of Yucca Mountain Review Plan (NRC, 2002a)

The Yucca Mountain Review Plan (NRC, 2002a) does not require any specific process or methodology for preclosure safety analysis. The DOE is allowed flexibility in how it chooses to meet the performance-based regulation and how to demonstrate compliance. In addition, the licensing review is intended to focus its evaluation on aspects of facility operations and design that have high risk significance. The PCSA Tool, which implements the review methodology of the Yucca Mountain Review Plan, provides risk-informed review capabilities to facilitate staff identification of safety-related structures, systems, and components for detailed review, and staff determination of whether the DOE preclosure safety analysis demonstrates compliance with the performance objectives in 10 CFR Part 63.

2.3 Preclosure Topics

To facilitate review and technical discussions with DOE on its use of methodologies, assumptions, data, evaluations, and conclusions for preclosure safety analysis, NRC has divided the preclosure area into 10 topics.[1] In parallel with the outline of the preclosure portion of the Yucca Mountain Review Plan, the ten preclosure topics are listed below.

(1) Site Description As It Pertains to Preclosure Safety Analysis

(2) Description of Structures, Systems, Components, Equipment, and Operational Process Activities

(3) Identification of Hazards and Initiating Events

(4) Identification of Event Sequences

(5) Consequence Analyses

---

[1]Reamer, C.W. "U.S. Nuclear Regulatory Commission and U.S. Department of Energy Technical Exchange in Pre-Closure Issues." Letter (April 27) to S. Brocoum, DOE. Washington, DC: NRC. 2001.

(6) Identification of Structures, Systems, and Components Important to Safety; Safety Controls; and Measures to Ensure Availability of the Safety Systems

(7) Design of Structures, Systems, and Components Important to Safety and Safety Controls

(8) Meeting the 10 CFR Part 20 As Low As Is Reasonably Achievable Requirements for Normal Operations and Category 1 Event Sequences

(9) Plans for Retrieval and Alternate Storage of Radioactive Wastes

(10) Plans for Permanent Closure and Decontamination, or Decontamination and Dismantlement of Surface Facilities

Preclosure Topics 3–6 are addressed in the PCSA Tool using standard methodologies and techniques from integrated safety analysis and probabilistic risk assessment. Topic 1 pertains to site-specific information, and Topic 2 involves details of the facility design, operations, human activities, and waste characterization. Topics 1 and 2 and design information from Topic 7 provide input to the preclosure safety analysis. Topics 3 and 4 deal with the determination of potential hazards, identification of initiating events, definitions of frequencies or probabilities taking into account associated uncertainties for initiating events and subsequent system failures, and event sequence frequency analysis. Topic 5 relates to determination of radiological consequence to the members of the public and facility workers. The results from the safety analysis in Topics 3–5 would be used to (i) demonstrate that the facility design is in compliance with the regulatory requirements; (ii) identify structures, systems, and components that are important to safety (Topic 6); and (iii) develop and modify design bases and design criteria for the structures, systems, and components (Topic 7). Because the preclosure safety analysis is an iterative process, Topic 7 not only represents the results of the preclosure safety analysis but is also part of the input for the next iteration of the preclosure safety analysis.

2.4 Preclosure Safety Analysis Review Methodology

The preclosure safety analysis examines the processes, equipment, structures, and operational activities during the preclosure period of geologic repository operations (i.e., the period before permanent closure and decontamination or permanent closure, decontamination, and dismantlement of surface facilities as defined in 10 CFR 63.102). The preclosure safety analysis identifies the hazards, potential event sequences, and consequences. It considers the structures, systems, and components, equipment, and operational activities of the facility staff that are relied on for safety. The purpose of the preclosure safety analysis is to ensure that all relevant hazards that could result in unacceptable consequences have been evaluated and appropriate protective measures have been identified and implemented. The DOE preclosure safety analysis methodology is discussed in Bechtel SAIC Company, LLC (2002).

The preclosure safety analysis review methodology can be illustrated using the flow chart in Figure 2-1. This flow chart is consistent with the regulatory requirements of 10 CFR Part 63

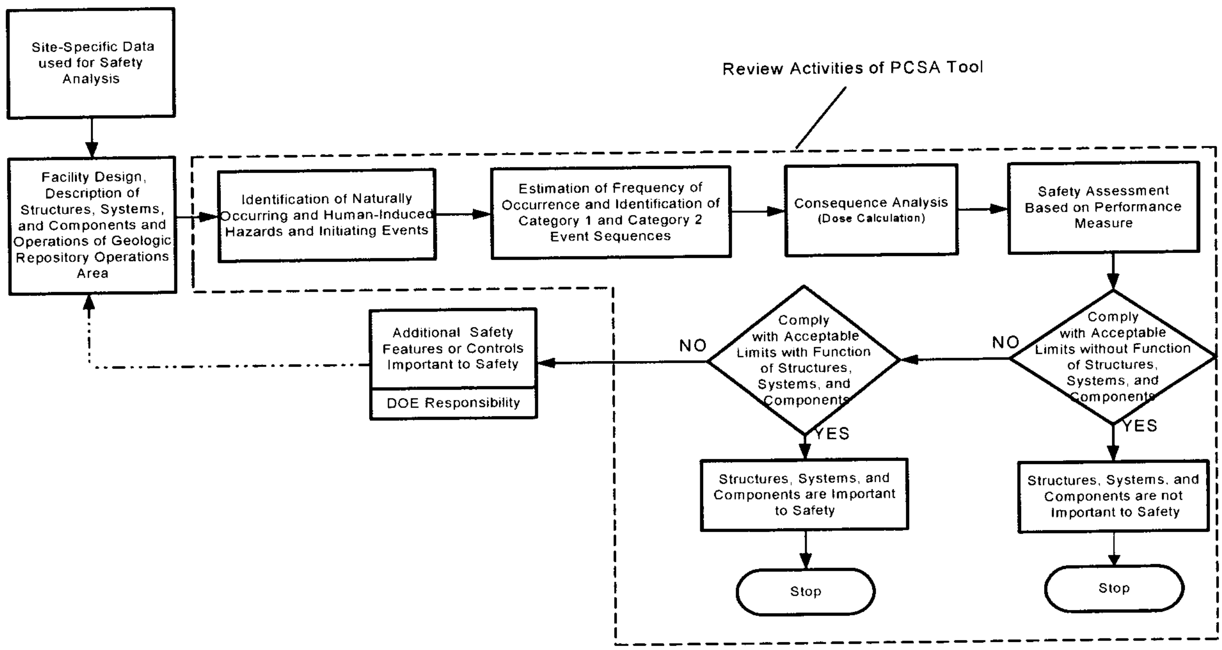


Figure 2-1. Preclosure Safety Analysis Review Methodology Flow Chart

and applicable review methods included in the Yucca Mountain Review Plan (NRC, 2002a). The preclosure safety analysis methodology is based on the requirements for preclosure safety analysis of the geologic repository operations area in 10 CFR 63.112 and the preclosure performance objectives in 10 CFR 63.111. The steps involved in the preclosure safety analysis evaluation include review of:

- Site-specific data used for safety analysis
- Description of structures, systems, components, equipment, operations, and process activities at the geologic repository operations area
- Identification of hazards and initiating events resulting from the naturally occurring and human-induced hazards
- Estimation of frequency of occurrence and identification of potential Category 1 and Category 2 event sequences
- Evaluation of radiological dose consequences to the public and to the workers for Category 1 and Category 2 event sequences
- Safety assessment based on the performance requirements of Category 1 and Category 2 event sequences in 10 CFR Part 20 and 10 CFR 63.111(a) and (b)
- Identification of structures, systems, and components important to safety

The DOE is responsible for conducting a satisfactory preclosure safety analysis. Although the NRC will review each aspect of the DOE analysis, some steps in the process are sufficiently important that NRC staff anticipate confirming the DOE results through independent calculations, as indicated above. For example, staff will independently identify (confirm or raise concerns about) potentially hazardous events. In addition, staff will use the tool to confirm, verify, or test adequacy of the analysis DOE is using to screen events out by probability.

The flow chart in Figure 2-1 shows that the structures, systems, and components important to safety are identified by comparing the consequences of the event with the acceptable dose limits, with and without the function of the structures, systems, and components. If the frequency and consequences from the event sequences are within the acceptable limits without the safety features and controls, those structures, systems, and components are not important to safety. On the other hand, if the frequency or consequences from event sequences are within the acceptable limits only if the safety features and controls are in place, those structures, systems, and components are important to safety. Finally, if the frequency or consequences from event sequences exceed the acceptable limits even with the safety features and controls in place, DOE has the responsibility of imposing additional safety features and controls to ensure that the consequences do not exceed acceptable limits. The activities discussed in this report are those highlighted by the dashed box in Figure 2-1.

2.5 Description of the Structure and Modules of the PCSA Tool

The PCSA Tool structure is modeled after the safety analysis review methodology shown in Figure 2-1. Activity under each section is divided into several modules, and the tool functions through these modules. The main modules parallel the review methodology. Each module has submodules, as shown in Figure 2-2(a,b). The modules in the tool allow the staff to perform independent review analysis and store data and results of the review in a structured and systematic manner. Results of the review are abstracted, as appropriate, for use in other modules of this tool. The abstraction and input to the next module are not fully automatic; rather, the needed information can be manually input into the next module to enable a tailored review. The modules under each section of the preclosure safety analysis review methodology are described in detail in the next paragraphs.

2.5.1 Review of Site and Facility Description

This section, which addresses the first two boxes in Figure 2-1, does not have a corresponding module in the tool. Staff will identify and verify that sufficient information is available to review and perform independent preclosure safety analysis. Site-specific data are primarily about meteorology, geology, and human activities (e.g., seismicity and faulting, winds and tornado, volcanic activity, slope stability, soil and rock characterization, aircraft flight information, industrial activities, regional demography, and such). The facility data include description and design details of structures, systems, and components; characterization of waste and source terms; and description of geologic repository operations area operational processes and procedures with an adequate understanding of the component and facility functions and sequence of operations. Chapter 3 provides further details on the site-specific and facility data.

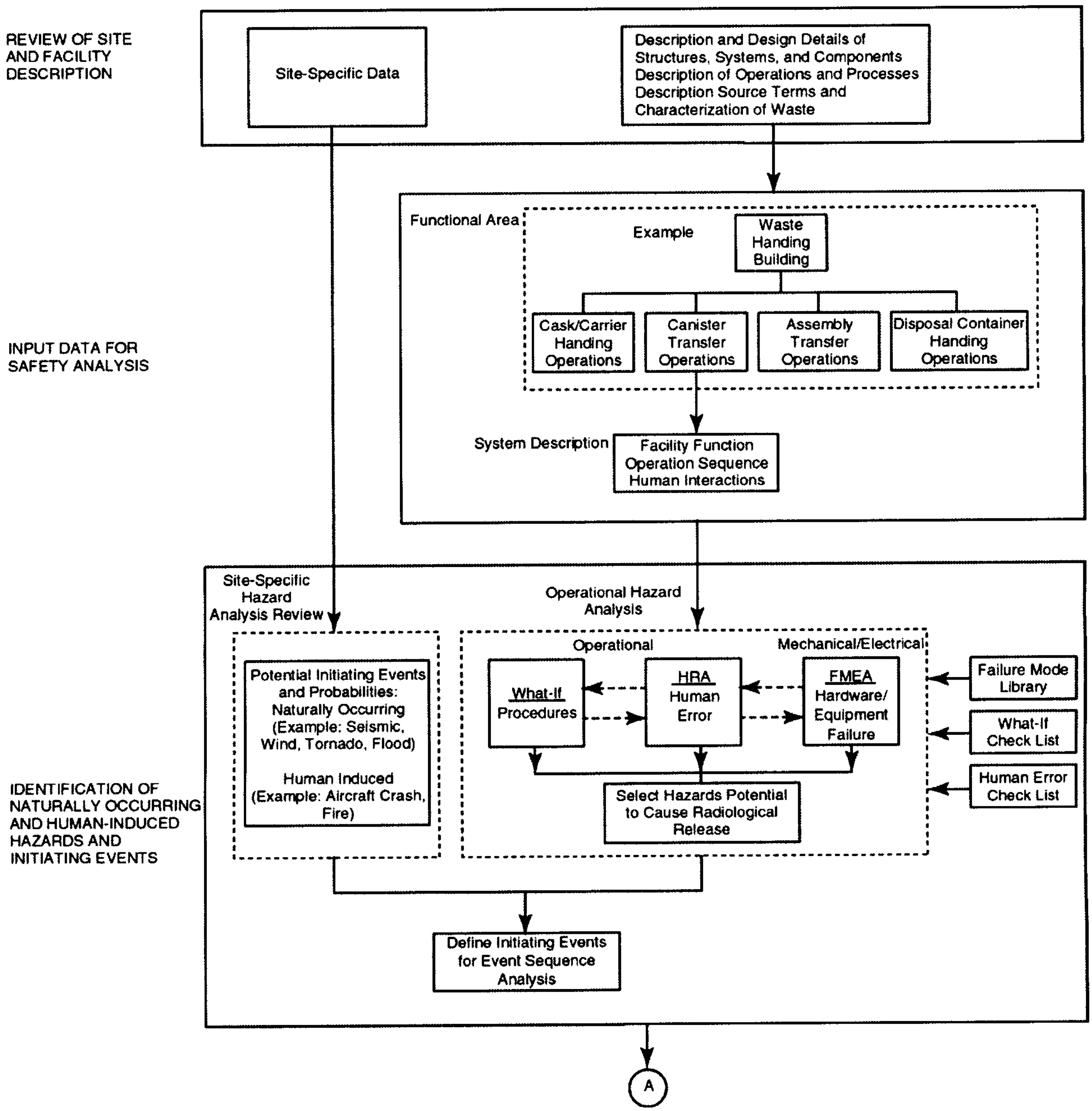


Figure 2-2(a). PCSA Tool Modules and Data Flow Design

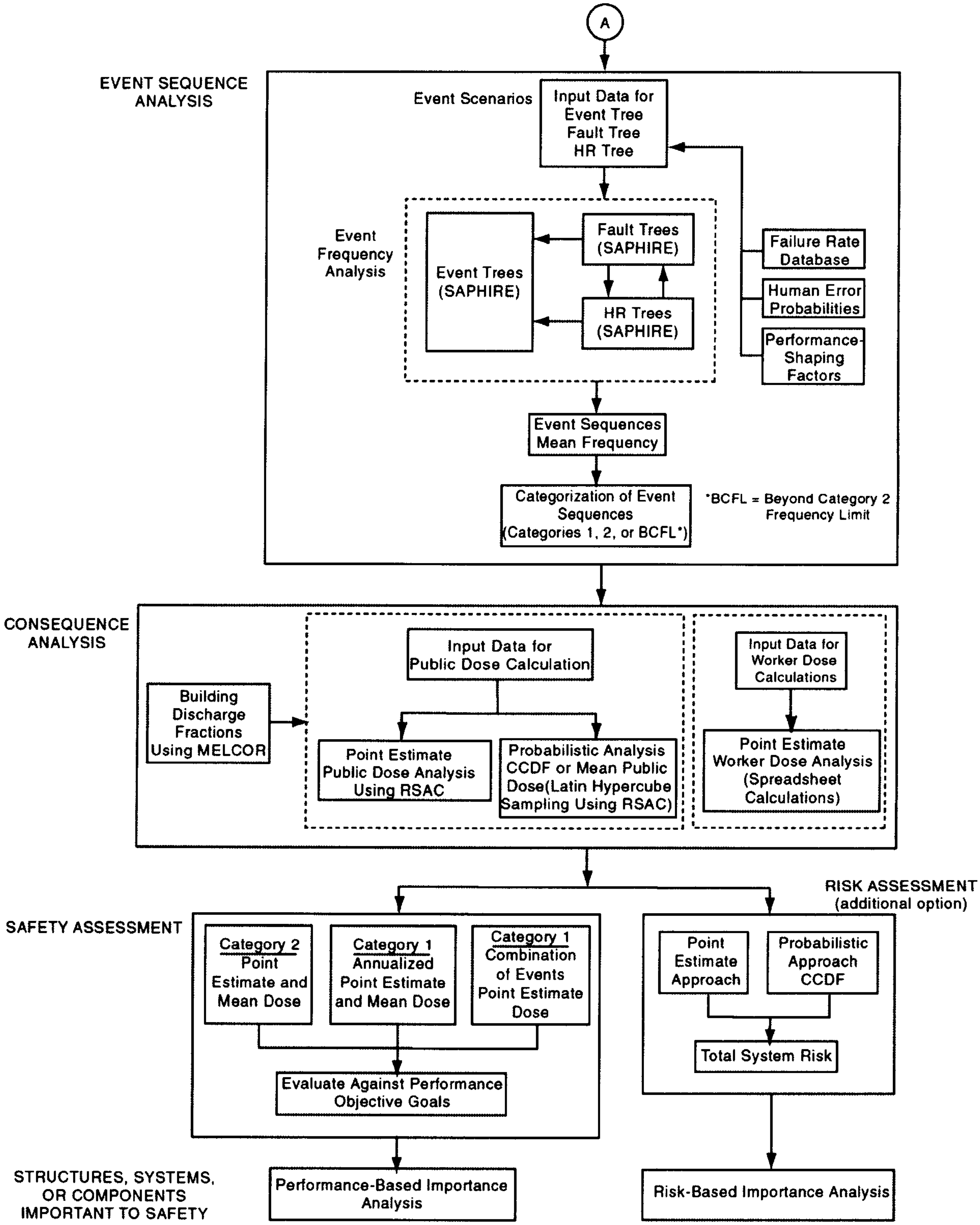


Figure 2-2(b). PCSA Tool Modules and Data Flow Diagram

2.5.2 Input Data for Safety Analysis

2.5.2.1 Functional Area

The facility and operations in the geologic repository operations area can be divided into functional areas by specific function or physical area of the facility, or by process. In this module, the functional area is identified to define the physical boundary of the safety analysis. For example, as shown in Figure 2-2(b), the canister transfer operation in the Waste Handling Building is selected as a functional area for safety analysis. Design information consisting of system description, process flow diagram, mechanical flow diagram, and conceptual description of the operations in this functional area will be used for the safety analysis.

2.5.2.2 System Description

Information required for safety analysis is compiled in this submodule. Descriptions include structures, systems, and components, and their functions, detailed operation sequences, and human actions. Nuclear material (e.g., inventories of cask and canisters) handled in this part of the operations is also identified and documented. Further discussion on functional area and system description is provided in Chapter 3.

2.5.3 Naturally Occurring and Human-Induced Hazards and Initiating Events

This section addresses two code submodules: (i) site-specific, naturally occurring, and human-induced hazard analysis; and (ii) operational hazard analysis as shown in Figure 2-2(a). The end result of the module is to identify the initiating events that may lead to a potential radiological dose to the public or workers. Details on this module are discussed in Chapter 4.

2.5.3.1 Site-Specific Hazard Analysis Review

The naturally occurring events and human-induced events external to the facility are identified in this submodule. The naturally occurring events consist of seismic, tornado, wind, flood, and other such events, while site-specific, human-induced events include aircraft crash, fire, and other such events. Extensive analyses for identification of naturally occurring events and their occurrence frequencies will be produced by the DOE. These analyses will be reviewed, and, if required, independent analyses will be made outside the tool. The module in the tool will record the results of the staff review and identify the site-specific events that may initiate event sequences in the facility based on their frequencies of occurrence.

2.5.3.2 Operational Hazard Analysis

Events resulting from the facility operations are analyzed for each functional area in this submodule. In addition, the failure checklist database is a submodule that provides input to this module.

2.5.3.2.1 Hazard Analysis

Hazard analysis is performed in this submodule using what-if analysis, failure modes and effects analysis, energy method, and human reliability analysis. The what-if analysis technique can be used for identification of process hazards, the failure modes and effects analysis addresses the hardware and equipment failures, human reliability analysis determines the possible human errors and actions, and the energy method seeks to find possible release of energy (e.g., kinetic, chemical, thermal) from the system that may result in radiological consequences.

2.5.3.2.2 Failure Checklist

A failure mode checklist, what-if checklist, and human error checklist database library would be used to assist in hazard analysis. The database library would contain the modes of equipment failure and list of possible internal events. Development of these checklist databases is in progress.

2.5.3.3 Initiating Events

In this submodule, initiating events that have the potential for radiological consequences are selected based on naturally occurring and human-induced and operational hazard analyses. In addition, the preclosure period is specified, and frequency of initiating event is evaluated.

2.5.4 Event Sequence Analysis

This section addresses code submodules: development of an event scenario and event frequency analysis as shown in Figure 2-2(b). Details on this module are discussed in Chapter 6.

2.5.4.1 Event Scenarios

In this submodule, the scenarios are developed based on postulated initiating events and subsequent system and operation failures that may result in a radiological release. Frequency of occurrence for initiating events and probability of failure of safety systems that lead to subsequent event are assigned. This submodule develops input data for event tree and fault tree analyses in the event frequency analysis module and stores the result after SAPHIRE analysis. This submodule will be updated to accommodate input data for human reliability tree analysis in the next version. Details on this submodule are discussed in Chapter 6.

2.5.4.2 Failure Rate Database

This module contains a comprehensive library of failure rates of equipment from actuarial data. The data on a particular component were obtained with the help of a taxonomy tree structure or built-in search capability. Each failure rate datum lists the unit associated with it (e.g., per demand or per hour). The primary and secondary reference for the data source and any statistical information available on the data are also provided. A separate database for human errors and performance-shaping factors required for human reliability tree analysis will be introduced in the PCSA tool in the next version.

2.5.4.3 Event Frequency Analysis

Event trees and fault trees are used in this module to estimate the frequencies of the event sequences. The tool uses SAPHIRE Version 6.07 to model and analyze the event trees and fault trees.

2.5.4.4 Event Sequences and Categorization

The results from the event tree analysis from SAPHIRE analysis are stored in this submodule. All event sequences are given unique identification numbers. The frequency and end state (i.e., qualitative assessment of consequence) for each event sequence are entered in this submodule.

Based on the frequency of occurrences, event sequences are categorized in this submodule as Category 1 or Category 2. Based on definition of 10 CFR 63.2, Category 1 event sequences are those natural and human-induced event sequences that are expected to occur one or more times before permanent closure. Category 2 event sequences are other natural and human-induced event sequences that have at least 1 chance in 10,000 of occurring before permanent closure. In this submodule, the event sequence frequencies are automatically categorized to Category 1, Category 2, or below category frequency limit based on the preclosure period assigned to the initiating events. Below Category 2 frequency (BCFL) limit are those with frequencies of occurrence of less than the Category 2 frequency limit.

2.5.5 Analysis of Consequence

The consequence analysis module calculates the radiological dose to the members of the public and workers. This section addresses the two main code submodules: public dose and worker dose. These modules supplied information through an input data module. Point estimate or probabilistic calculations can be performed for the public dose determination. Point estimate calculations of the worker dose are also available. Details in this module are provided in Chapter 7.

2.5.5.1 Input Data

This module prepares data required for public dose calculations by deterministic and probabilistic approaches. Dose calculation requires the inventory of radionuclides, meteorological data, and other parameters. For probabilistic analysis, the distributions of sampled parameters are provided in this module.

2.5.5.2 Public Dose

The point estimate calculations of public dose are performed using RSAC software. The probabilistic calculations are based on Latin Hypercube Sampling of RSAC input parameters. RSAC is executed once for each sampled set of input parameters to determine the dose from that realization. The results from the simulations and dose calculations are processed and displayed in this module. The tool provides a separate module for generating input data for calculating building discharge fractions using MELCOR software.

2.5.5.3 Worker Dose

The worker dose option performs a spreadsheet calculation to estimate dose to the facility workers. A single screen provides the user interface for the input and output of the worker dose calculations.

2.5.6 Safety Assessment

The safety assessment module integrates and analyzes the results obtained in the various tasks for safety assessment. This integration includes, among other things, the tabulation of frequencies for event sequences and consequences. The results are analyzed to assess safety by comparing the dose with performance objectives for Category 1 and 2 event sequences stipulated in 10 CFR 63.111. For Category 1 event sequences, the two approaches for safety assessment used in this module are annualized dose and combination of events. For Category 2 event sequences, each event sequence is compared with Category 2 dose limits. Chapter 8 discusses the capabilities and tool function for safety assessment.

2.5.7 Risk Assessment

The risk assessment module evaluates aggregate risk from a potential repository during the preclosure period. Estimation of aggregate risk is not required by the NRC regulation in 10 CFR Part 63 (66 Federal Register 55732) and will not be used directly in compliance determination. However, estimation of aggregate risk is incorporated in the PCSA Tool for completeness sake and will be used for gaining risk insights. Additionally, the risk assessment can also be used to evaluate the reliance on structures, systems, and components important to safety. The details in risk assessment are discussed in Chapter 8.

2.5.8 Structures, Systems, and Components Important to Safety

The structures, systems, and components important to safety will be identified using a performance-based importance analysis. This module is not fully developed. The approach and current state of development, however, are discussed in Chapter 9.

2.6 PCSA Tool Code Structure

The preclosure safety analysis methodology discussed in Section 2.5 is implemented in the PCSA Tool. The purpose of the PCSA Tool is to conduct selected independent safety analyses to review the DOE preclosure safety analysis. The tool will be used to conduct systematic hazard analyses, event sequence analyses, consequence analyses, and safety assessments. The PCSA Tool has been designed to satisfy the primary objective as a review tool with the capability to analyze the entire operation or selected operations. The PCSA Tool is intended to keep track of all phases of review activity from system description to safety assessment. Further, the tool can be applied to all or selected components of the safety analysis, such as hazard analysis, event tree, fault tree analyses, human reliability analysis, or consequence analyses using the independent modules as described in Section 2.5.

2.6.1 Computational Approach

The PCSA Tool serves two primary purposes: store data in a database and perform analyses. The structure of the PCSA Tool is schematically illustrated in Figure 2-3. The figure shows that the graphical user interface, developed using Visual Basic 6.0, controls the functions of the tool by independently linking to databases and other software packages. The project database and probability database were created using Microsoft Access database software. The failure rate database contains the component failure rates obtained from actuarial data and other information such as literature citation for source of the data. The failure rate and other checklist databases can only be viewed through the graphical user interface for reference and cannot be modified by the user. The project database is the workbench for the tool, and it has been designed to perform specific data management tasks that allow safety analyses to be conducted in a systematic manner. The input data and output data to and from other software packages are also managed by this database. As seen in Figure 2-3, the project data are handled through several tables in the Microsoft Access database for (i) entering or gaining access to data, (ii) sorting and filtering data, and (iii) creating reports.

The PCSA Tool incorporates SAPHIRE, RSAC, and MELCOR codes, which are based on mathematical models described in Russel, et al. (1993), Wenzel (1994), and (Gauntt, et al., 2000c), respectively. The SAPHIRE software conducts fault tree and event tree analyses, and the RSAC software performs dose calculations from atmospheric release of radiological material. Both programs are distributed by Radiation Safety Information Computational Center, Oak Ridge National Laboratory, Oak Ridge, Tennessee. Developed by Sandia National Laboratory, MELCOR is used to estimate the building discharge fraction (i.e., the fraction of radionuclide released into the building air that is transported through the building ventilation and discharged into the atmosphere).

The PCSA Tool is developed to operate on an IBM-compatible computer installed with Windows NT 4.0 or higher. The estimated disk space required is 256 megabytes maximum. This program is currently developed on a Pentium II—256 megahertz with 256 megabytes of random access memory. A setup package InstallShield Professional–Windows Installer Edition 2.0, was used to create a PCSA Tool installation setup for Windows NT for distribution to prospective users. The setup distribution will also install SAPHIRE, RSAC, and MELCOR codes, application packages, and the CNWRA-developed applications. Microsoft Access database software is not required to be resident in the user's computer.

2.6.2 PCSA Tool Functions

The computer program is described here in the context of the functions of the PCSA Tool. When the program is first executed, a startup title form is displayed to the user (Figure 2-4). This form contains an artistic rendering of the proposed Yucca Mountain repository (CRWMS M&O, 1996b). The startup page displays five buttons: About PCSA, Disclaimer, Open Project, Create Project, and Exit. The About PCSA describes the tool and the project. The Open Project button will open an existing project, and the Create Project button will enable the user to create a new project. Both buttons open a dialog box as shown in Figure 2-5. The dialog box has features similar to other standard Windows application packages (e.g., the Browse Control button enables searching a project file, or storing a project file in the directory structure). The tool will create and open database files with the extension*.mdb*. After

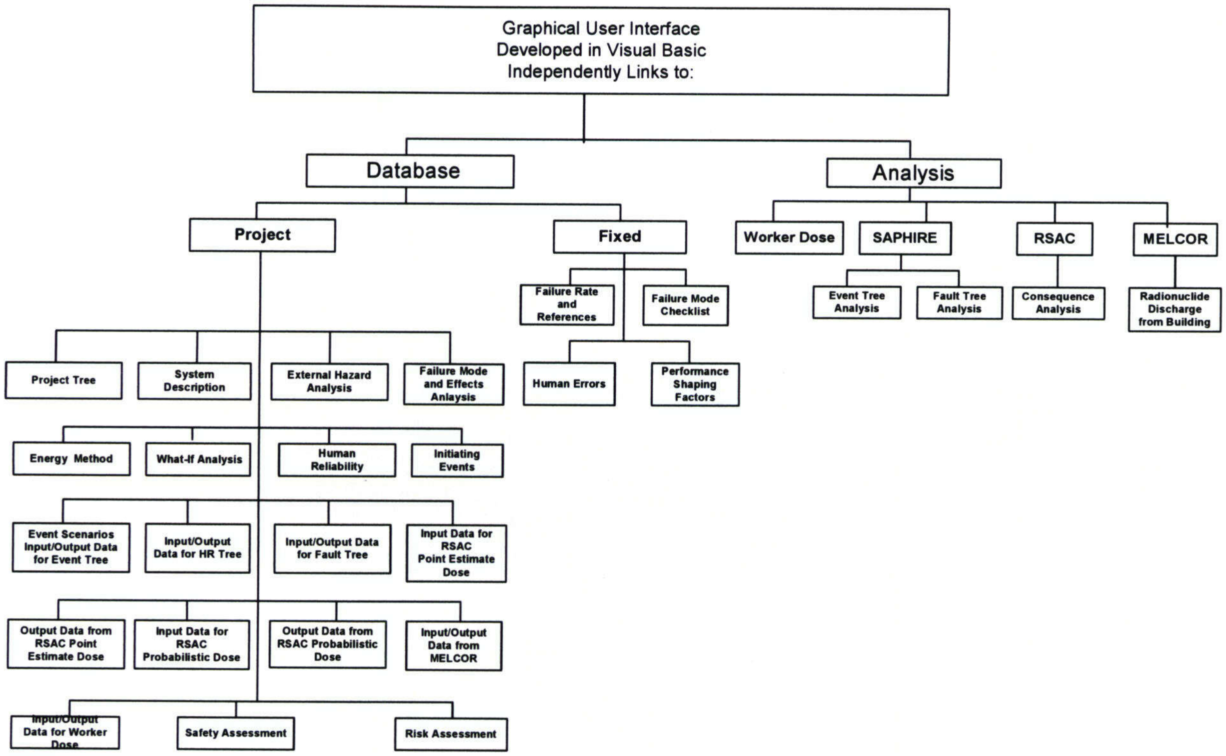


Figure 2-3. Structure of PCSA Tool

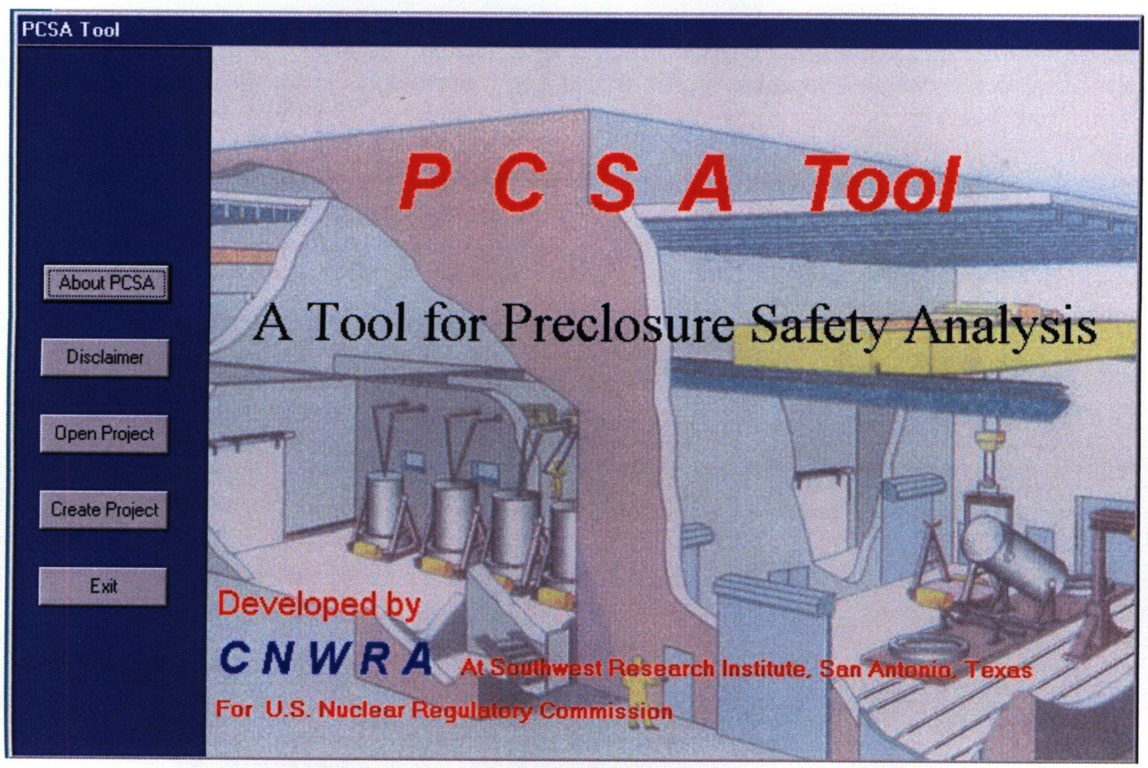


Figure 2-4. Display of Startup Screen from PCSA Tool

Figure 2-5. Open Project Dialog Box to Open an Existing Project

selecting a file or creating a new file, PCSA Tool opens the main tool window with a menu bar at the top. In the PCSA Tool, the term project represents a single specific database. The menu bar lists various functions and categories into which the tool allows the entry of data or further actions. The top-level menu list on the menu bar is shown in Figure 2-6. After clicking on the menu bar, the user is given more specific options. Many of these options have subsets, which may have further subsets. The sublevels and further levels of the menu are shown in Figure 2-7. By clicking on the various options, the user is able to navigate through various programs, forms, tables, and reports. The user can then enter data into the selected table or form and recall the data at a later time. The last level of the menu opens a dialog box that provides further actions through button controls. The functions of each menu are schematically represented and described as follows:

- File Menu: On the Main form, a single menu bar is displayed at the top with an artistic rendering of the Yucca Mountain Project waste handling system in the background. The first menu is File, which performs functions similar to every other file menu in Windows applications (i.e., new, open, save, save as, and exit). Data entered using forms are not saved in the database until the Save menu is pressed.

- Project Tree: The Project Tree menu displays an expandable and collapsible tree view of the functional area. Project Tree is used to show and develop the organization of functional area as a tree structure. This menu helps to manage data from the facility hazard analysis in a systematic manner. The data for each node of the tree can be expanded to three levels, allowing three levels of subsections of each functional area. When the lowest level of the functional area is selected, a graphical user interface opens the database, and activates the System menu, Internal Event menu,

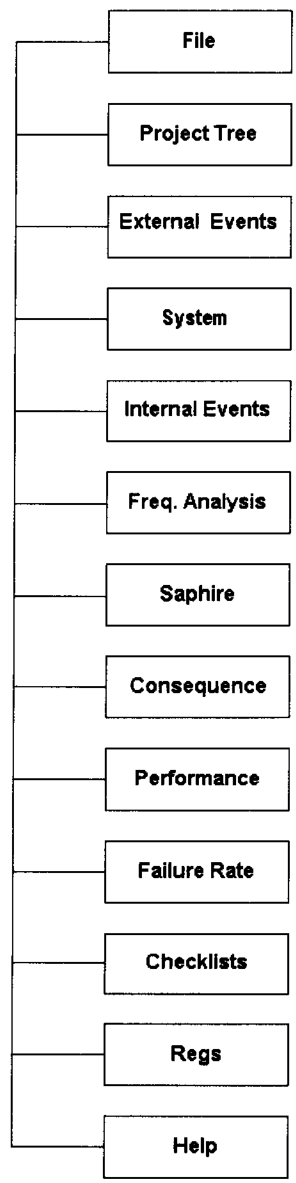


Figure 2-6. Main Menus on PCSA Tool Menu Bar

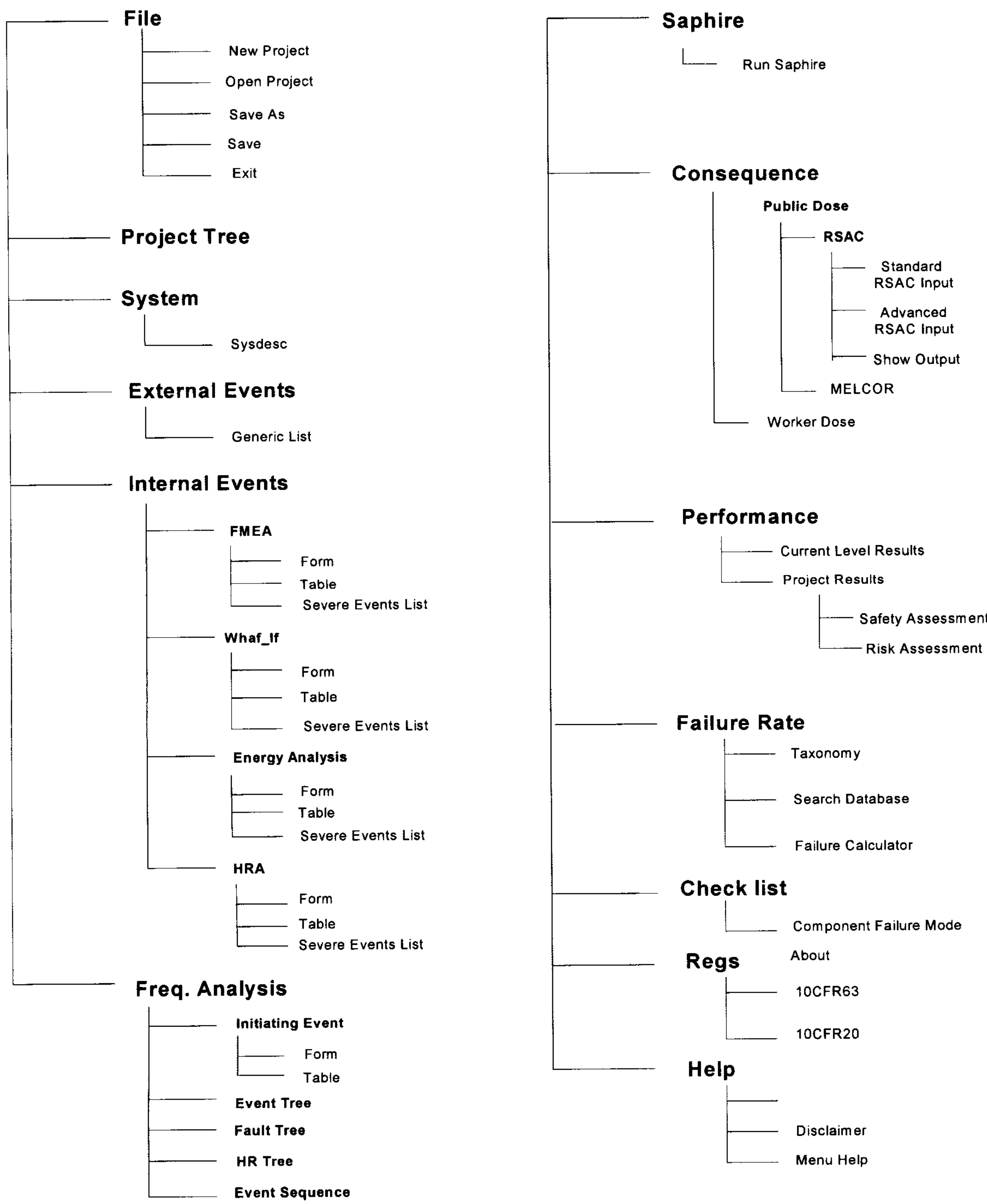


Figure 2-7. Tree Diagram Showing Layout of Menus and Submenus

Freq. Analysis menu, and Current Level Results submenu under the Performance menu to store data at that level. The actions under this menu, such as opening forms and dialog boxes, and further operations through button controls are shown in Figure 2-8. The details on the functions and operations of project tree are discussed in Chapter 3.

- External Events Menu: The External Events menu contains a submenu, Generic List, which leads to a database with tables containing a generic list of naturally occurring and human-induced external events. The table shows the four categories of screening processes, and the applicability of an event for each category is indicated by yes or no for negative outcome. One column header in the table is Frequency, in which the frequency of occurrence of the event is entered. The event screening process is based on an indepth review of DOE reports. The outcome of the review for each screening category can be stored in the database by double clicking on the event. Details on the natural and human-induced hazard analysis external to the facility are discussed in Chapter 4.

- System Menu: Under the System menu, a Sysdesc submenu appears. The Sysdesc is used to create a system description detailing all necessary information on the functional area and system. Sysdesc includes the initial information, functions, detailed operations sequence, equipment used, human actions, and nuclear material handled. To activate this menu, a functional area should be selected under System menu. The menu launches a dialog box with a form to help input data in the database. Further actions in the dialog box are accomplished through button controls. The details on the functions and operations of the System menu are discussed in Chapter 3.

- Internal Events Menu: Facility hazard analysis is performed under this menu. To activate this menu, a functional area must be selected under the Project Tree menu. Included in the Internal Events menu are four options: FMEA, What_If, HRA, and Energy Method submenus. Analyses of the hazards resulting from the operations of the facility are performed using failure modes and effects analysis, what-if analysis, human reliability analysis, and energy analysis methods. The hazard analysis techniques are usually qualitative in nature. The tool uses the standard format for these techniques with minor modifications to suit the review process. In all the hazard analysis methods, the data are entered into a database using a data entry form. The data can then be viewed in a tabular form that can be used to edit data, introduce additional data, and generate reports. DOE facility hazard analysis is based on the energy analysis method structured for the repository operations (Bechtel SAIC Company, LLC, 2002, CRWMS M&O, 1999b). The energy analysis in the tool is modeled after the DOE method. This technique was introduced to allow a direct comparison of DOE identification of operational hazards. Further actions in the dialog box are performed through button controls. The details on the functions and operations of the Internal Events menu are discussed in Chapter 4.

- Freq. Analysis Menu: To activate this menu, a functional area must be selected under the Project Tree menu. The Freq. Analysis (frequency analysis) menu contains submenus: Initiating Event, Event Tree, Fault Tree, HR Tree, and Event Sequence. An initiating event could result from (i) a naturally occurring, human-induced event external to the facility identified through site-specific hazard analysis; or (ii) a failure of a component or equipment in a system or human actions during facility operations

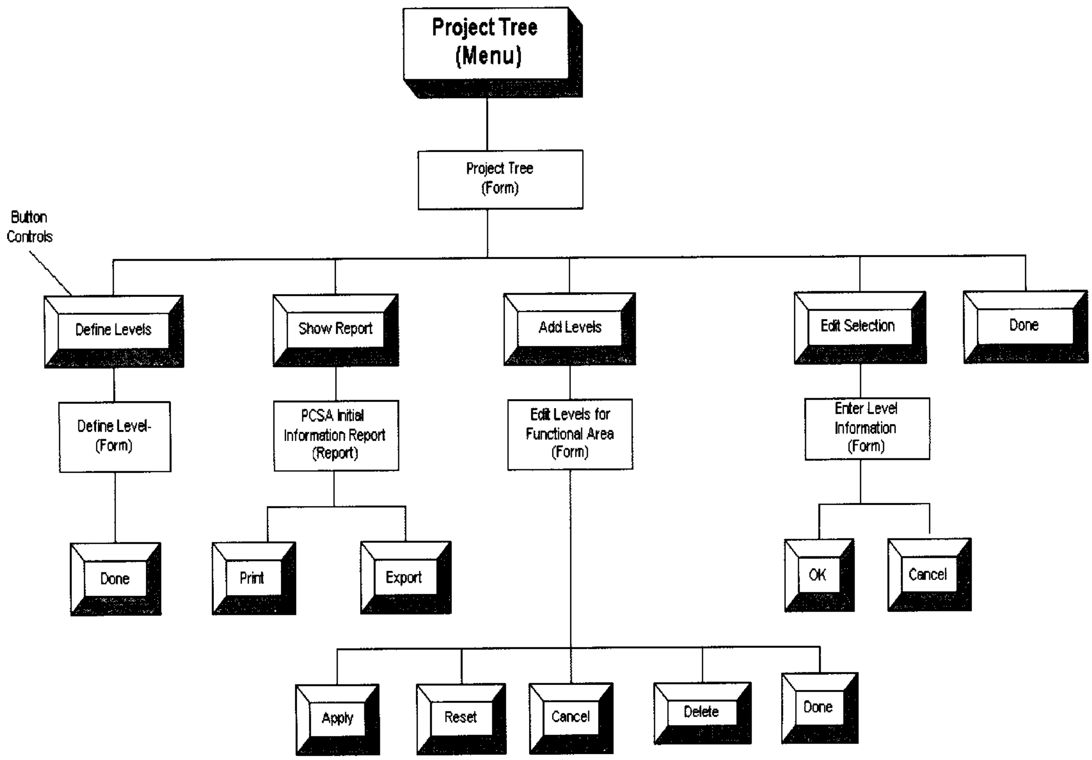


Figure 2-8. Example of Typical Action Buttons under Each Menu

identified through operational hazard analysis. The initiating events identified based on PCSA Tool hazard analysis or DOE analysis are entered into the database from the Initiating Event submenu. All potential initiating events identified must be examined and frequencies of occurrence evaluated even if the initiating event may not develop into a scenario because of certain mitigating features. The reason for inclusion or exclusion of initiating events for further preclosure safety analysis should be recorded. The Event Tree submenu leads to an Event Tree Form that allows the user to develop event scenarios resulting from an initiating event for event tree analysis. Event scenarios are generated by postulating subsequent events caused by failure of safety features to mitigate the event and probability of failure for the safety features. For a single component failure, the probability of failure is obtained from the failure rate database; however, for a multicomponent system, the probability of the failure is estimated using fault tree analysis. The fault tree and event tree analyses are performed using SAPHIRE code. The Event Sequence menu contains a form to store the results from the event tree analysis (i.e., event sequences and the frequencies) for each postulated scenario in the database. Similarly, the results from the fault tree analysis and human reliability tree analysis are stored in the database under the Fault Tree submenu. Further actions in the dialog box are performed through button controls. Details on the functions and operations of the Freq. Analysis menu are discussed in Chapter 6.

- SAPHIRE Menu: Next on the PCSA Tool is a menu containing SAPHIRE to run SAPHIRE Version 6.70 code (Idaho National Engineering Laboratory, 1998). Clicking on this button launches the application for the user. Currently, there is no exchange of data between the tool and the SAPHIRE code program. Consequently, data required to run SAPHIRE code must be separately entered, and the user must be familiar with the software package. SAPHIRE code is used for event tree and fault tree analyses.

- Consequences Menu: The Consequences menu contains two calculation options: public dose and worker dose. The Public Dose menu displays RSAC and MELCOR submenus. The RSAC further displays Standard RSAC Input, Advances RSAC Input, and Show Output.

  The Input submenu leads to input data menus displayed as folder forms for a variety of input data categories: Fuel Selection/Assemblies Breached, Release Fraction by Group, View Source Term, Meteorological Data, Inhalation Dose, Ingestion Dose, Submersion Dose, Ground Surface Dose, and HEPA Bldg Discharge, and Other. The input data are stored in a text file in a format that will serve as input for RSAC execution. For public dose calculations, RSAC is executed by clicking on the Run RSAC menu. The results from the RSAC run are seen under the Show Output submenu. The total effective dose equivalent from each pathway (inhalation, ingestion, ground surface, and submersion) is displayed along with the sum of the four pathways. Organ dose equivalent from inhalation, ingestion, and ground surface pathways are also tabulated. The details of the consequence analysis, including its functions and operations, are discussed in Chapter 7.

  The Worker Dose menu opens up a form to calculate worker dose. The input data, calculation of worker dose, and display of results are all performed under this option. Details about the worker dose calculation are provided in Chapter 7.

- Performance Menu: The Performance menu has two submenus: Current Level Results and Project Results. The Project Results submenu has further submenus, Safety Assessment and Risk Assessment. Selecting Current Level Results menu opens a dialog box that shows the integrated results from event frequency analysis and dose consequence analysis in tabular form. To activate the Current Level Results menu, a functional area must be selected under the Project Tree menu. The frequency data for event sequences for the functional area entered in the Event Sequence Form are automatically brought into this form and dose consequence results for point estimate (deterministic) and probabilistic cases for each event sequence are entered. In addition, the directory path at which the consequence analysis results exist is also entered.

  The System Assessment submenu under Project menu displays a grid form showing results (i.e., frequencies and consequences from all functional areas). Data cannot be entered or edited in this form. The safety assessment for Category 1 and Category 2 event sequences and identification of structures, systems, and components important to safety are conducted by clicking on the Safety Assessment and SSCIS buttons. The Risk Assessment menu allows evaluation of total aggregate risk based on the frequencies and consequences of event scenarios from all functional areas. This calculation is not required by the regulation; it is an additional option to gain risk-insight. Detailed operations of all the features under the Performance menu are discussed in Chapters 8 and 10.

- Failure Rate Menu: The Failure Rate menu contains View Taxonomy, Search Database, and Failure Calculator submenus. A database has been developed that contains failure rates of several components based on the actuarial data. A user can search for the data using either View Taxonomy or Search Database submenus. These data have been categorized in an industry standard taxonomical structure. The View Taxonomy submenu opens a dialog box that contains a taxonomy tree view that shows a listing of all current components and categories. After expanding the nodes of the tree, the user can search for the component. The component will bring forward a dialog box that contains the failure rate for that component, the references from where the data were acquired, and a brief description of the available statistical basis. The Search Database menu brings up a dialog box in which the user can type the component name for a faster search.

  When clicked, the Failure Calculator menu opens a dialog box allowing entry of a component name, failure rate, and number of operating hours or demands, which will compute the expected frequency of failures and has the capability to save the results to an output file.

  Further actions in the dialog box are accomplished through button controls. Details on the functions and operations of the probability database are discussed in Chapter 6.

- Checklists Menu: The Checklist menu contains the component failure mode checklist, which displays a checklist of component failure modes. The checklist may be used during failure modes and effects analysis. The user can browse through the entire database or use the search option for a component.

- Regulation Menu: The Regulation menu displays two submenus, 10 CFR Part 63 and 10 CFR Part 20. The 10 CFR Part 63 menu displays the 10 CFR Part 63: Disposal of High-Level Wastes in a Geologic Repository at Yucca Mountain, Nevada. Similarly, the 10 CFR Part 20 menu displays 10 CFR Part 20: Standards for protection against radiation. Both regulations have been stored as hypertext markup language files, and the respective menus display the regulations through the web browser Netscape Navigator. An html file allows the user to browse through the document with ease using the hypertext links. Both 10 CFR Part 20 and 10 CFR Part 63 were downloaded from the NRC web site (www.nrc.gov).

- Help Menu: The Help menu displays About, Disclaimer, and Menu Help submenus. The Menu Help submenu is not currently active.

3 DESCRIPTION OF YUCCA MOUNTAIN SITE, FACILITY, AND OPERATIONS

To comply with the requirements for the preclosure safety analysis in 10 CFR 63.112, adequate information on the site and the facility in the U.S. Department of Energy (DOE) license application would be required for evaluation of preclosure safety. Sections 4.1.1.1 and 4.1.1.2 of the Yucca Mountain Review Plan (NRC, 2002a) define the acceptance criteria and review methods to be used for evaluating adequacy of information on the repository site, facility, and operational processes and for conducting and reviewing the preclosure safety analysis. This chapter provides a brief description of the site, facility, and operations of the proposed repository. The DOE design for the facility is being continually revised, and the information provided in this chapter is based on information available from the Viability Assessment Design and Enhanced Design Alternative II (DOE, 1998; DOE, 2001b). Additionally, this chapter describes the organization in the PCSA Tool for abstraction of information from review of the description of the site, structures, systems, components, processes activities, sequence of operations, and human actions.

3.1 Yucca Mountain Site Description

Review of the DOE description of the Yucca Mountain site will provide input to the preclosure safety analysis through facilitation of the identification of naturally occurring and human-induced external events. The site description in DOE documents should provide sufficient understanding of the site to identify potential naturally occurring and human-induced hazards and event sequences. The Yucca Mountain Review Plan (NRC, 2002a) provides guidance for reviewing the Yucca Mountain site description in Section 4.1.1.1. The review methods and acceptance criteria encompass the description of site geography, regional demography, local meteorology and regional climatology, regional and local surface and groundwater hydrology, site geology and seismology, igneous activity, site geomorphology, and site geochemistry. NUREG–1762 (NRC, 2002b) summarizes the current understanding of the U.S. Nuclear Regulatory Commission (NRC) based on the acceptance criteria of the Yucca Mountain Review Plan (NRC, 2002a), of the status of the description of Yucca Mountain as provided by the DOE. This section provides a summary of the NRC assessment as provided in NUREG–1762 (NRC, 2002b).

The information given by the DOE on site geography may need to be updated for site location and site map to be consistent with the U.S. Environmental Protection Agency Standard and design for an expanded repository (DOE, 2001b). The regional demographic information needs to be updated to include fiscal year 2000 census data. Regarding regional and local surface and groundwater hydrology, additional information is needed to evaluate potential water and debris flows, siting criteria or ventilation shafts, maximum versus 100-year flood, 100-year flood design considerations, storage in Midway Valley, transportation across active drainages, and water influx along faults. Additional information is also necessary for proposed alternative design for expanded repository (DOE, 2001b). The information provided by the DOE on regional geologic and tectonic setting as well as site stratigraphy is sufficient for conducting a safety analysis. Additional information may be necessary for proposed alternative design for expanded repository. The DOE has agreed to provide information on site soil data necessary for seismic response models and site design, on rock properties, and additional information on probabilistic seismic and fault displacement hazard assessments. To date, the DOE has not provided adequate technical bases for evaluation of tephra deposition at the site. Staff review of DOE information on local meteorology and regional climatology, site geomorphology, and preclosure aspect of geochemistry is incomplete at this time.

3.2 Description of Structures, Systems, and Components; Equipment; and Operational Process Activities

Comprehensive identification of hazards and initiating events depends on details of facility design and processes. The DOE has indicated that its License Application for construction authorization would be based on a preliminary layout and functional description, and conceptual design (Bechtel SAIC Company, LLC, 2002). Thus, DOE preclosure safety analysis and identification and quality level classification of structures, systems, and components important to safety would be based on "limited design detail." Although all the design information may not be needed for the license application for construction authorization, the level of detail must be sufficient to demonstrate compliance based on an acceptable preclosure safety analysis. DOE identification of structures, systems, and components important to safety and their further quality level categorizations must be based on results of a robust preclosure safety analysis.

Review of the DOE description of structures, systems, and components and operational process activities will provide input to the preclosure safety analysis. The description of structures, systems, and components and operational process activities in DOE documents should provide sufficient understanding of the design of geologic repository operations area facilities to identify hazards and event sequences. In addition, adequate description of the characterization of high-level waste and operating schedules should be available for the preclosure safety analysis. The Yucca Mountain Review Plan (NRC, 2002a) provides guidance on the staff review in Section 4.1.1.2 that addresses the description of (i) the location of surface facilities and their functions, including structures, systems, and components and equipment; (ii) design details of structures, systems, and components, equipment, and utility systems of surface and subsurface facilities; (iii) high-level waste characteristics and description of engineered barrier system components; and (iv) process activities, and procedures, including interfaces and interactions between structures, systems, and components. Descriptions of the facility, as available from DOE documents based on DOE's current design, and abstraction of this information in the PCSA Tool to review and conduct the preclosure safety analysis are discussed next.

3.2.1 Description of Facility and Their Functions

3.2.1.1 Surface Facility

The primary safety function of the surface facilities is to prevent accidental release of radioactive materials during operations. The surface facilities will be used to receive spent nuclear fuel and high-level waste shipments, temporarily store them, and prepare and package the wastes for underground emplacements (DOE, 1998). The surface facilities consist of three primary functional areas: (i) the waste receiving and inspection area, where incoming trucks and rail cars arrive and are inspected; (ii) the surface portion of the waste operations area, which includes all buildings in which radioactive material is handled for packaging; and (iii) the general support facilities, consisting of administrative buildings, security stations, and warehouses.

The North Portal surface facilities would consist of a radiologically controlled area, the Balance of Plant area, and the site service area as shown in Figure 3-1 (DOE, 2001b; CRWMS M&O, 1999d). The radiologically controlled area would contain the nuclear facilities and systems that receive spent nuclear fuel from the off-site transportation system, place the waste in disposal containers, ship the empty transportation carriers, and collect and package site-generated, low-level waste for disposal. The radiologically controlled area comprises systems, equipment, and facilities that are required to receive, transfer, package, and emplace waste in the repository. These facilities include (DOE, 2001b; CRWMS M&O, 1999b) (i) the Carrier Preparation Building, where rail and truck carriers are prepared for receiving and shipping; (ii) the Waste Handling Building, where shipping casks are unloaded, and the waste is transferred and placed in disposal containers for emplacement; (iii) the Waste Treatment Building, where liquid and solid low-level waste is processed and packaged for off-site shipment; and (iv) the Transport Maintenance Building, where the site prime movers and underground transporters are serviced. Additionally, the surface facilities will also provide radiological protection, utilities, ventilation for the underground facilities, and other supporting functions. The balance of plant facilities provides nonradiological support to the surface and subsurface operations comprising general infrastructure facilities such as management and administration, warehousing, maintenance, fire-fighting equipment, medical facilities, utility (including fuel and steam generation), security, markup, and testing. The site services include general parking and a visitor center.

The major radiologically controlled area facilities would be the Carrier Preparation Building and the Waste Handling Building. The Carrier Preparation Building would house the carrier preparation material handling system to receive, inspect, and prepare the incoming carriers and casks for unloading at the Waste Handling Building. The Carrier Preparation Building is a one-story, steel-framed structure with an approximate floor size of 58 m [190 ft] long, 37 m [121 ft] wide, and 14 m [45 ft] high. Inside, there would be two identical carrier bays accommodating four parallel rail tracks and roadways for the passage of carriers. The two outer tracks serve the incoming carriers, and two inner tracks serve outgoing carriers. The transportation carriers enter and exit the building through one of eight remotely operated doors.

The Waste Handling Building would provide the structures, controlled areas, and accesses required to house and operate the waste preparation systems, protect operating personnel, and maintain radiological confinement. The multilevel Waste Handling Building is approximately 180 m [593 ft] wide and 214 m [703 ft] long. Integral to the facility structure are the essential waste preparation systems, including the carrier/cask handling system, assembly transfer system, canister transfer system, disposal container handling system, and waste package remediation system as shown in Figures 3-2 and 3-3 (DOE, 2001b). The associated operating and equipment areas for these systems are described in subsequent sections. Essential support systems include an electrical power system, a fire protection system, a radiation monitoring and control system, a ventilation system, a treatment and cooling system, a leak detection system, a water-level management system, and a supplemental water system for pool water.

The structural system of the building that would house waste handling primarily consists of a structural-steel frame with metal-clad siding and reinforced concrete hot cells. The waste handling process areas use concrete walls and a roof slab for radiation shielding. Lower-level radiation areas, such as carrier preparation, air lock, and such will have wall

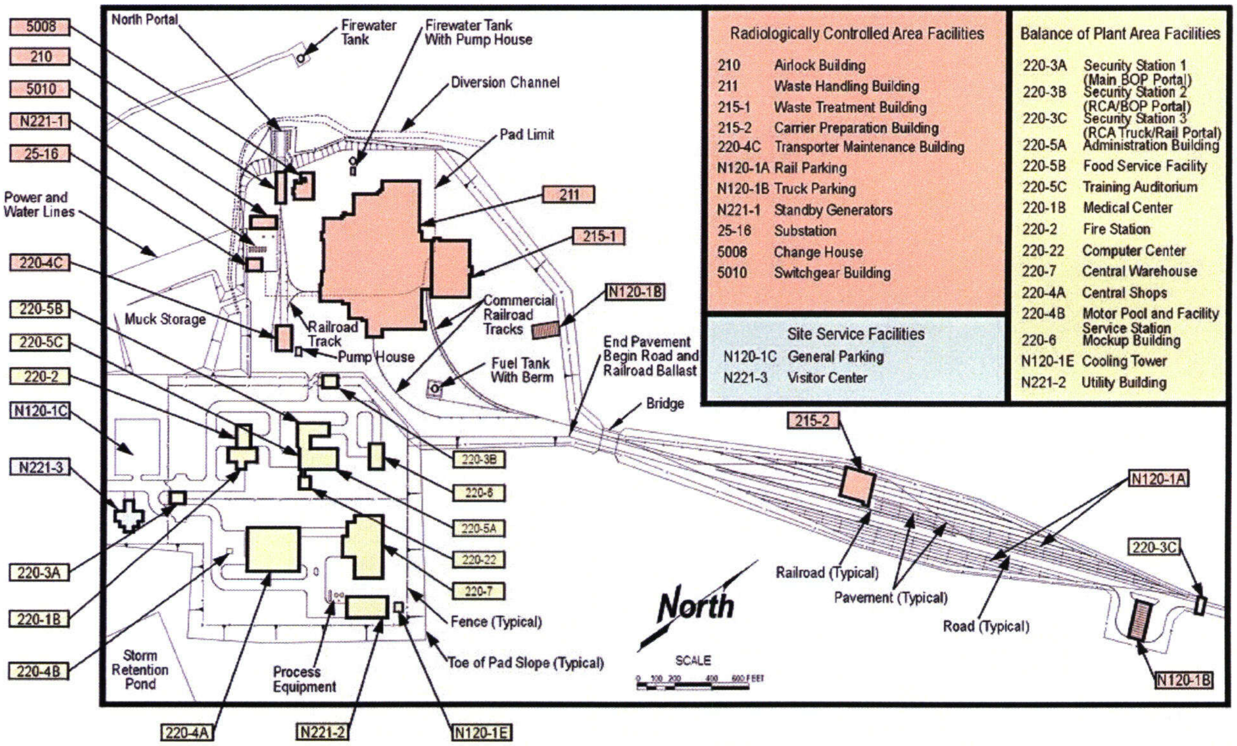


Figure 3-1. Layout of North Portal Surface Facilities (DOE, 2001b)

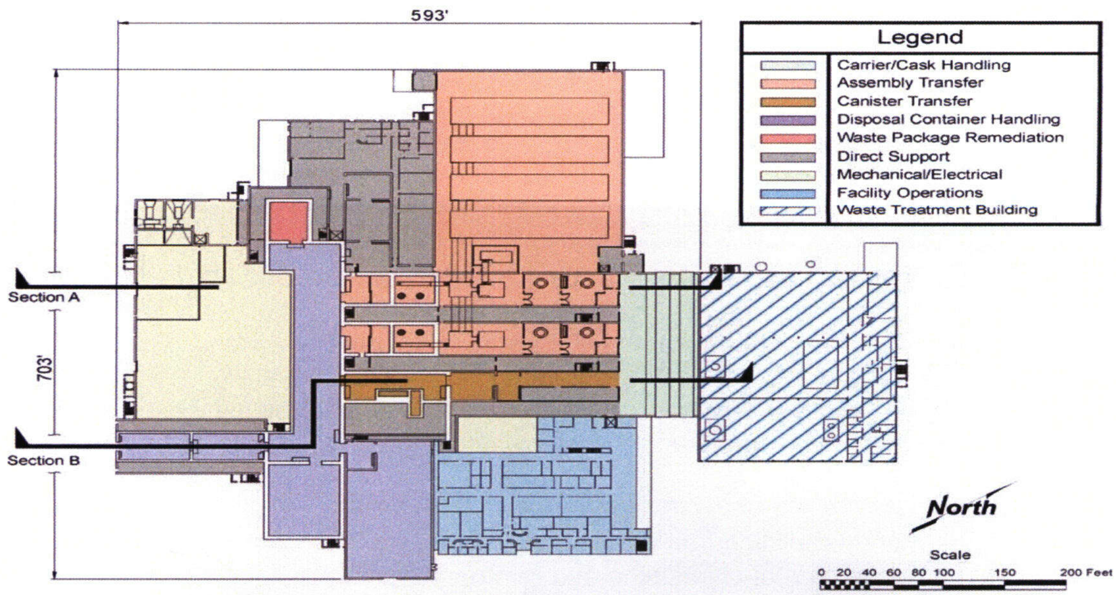


Figure 3-2. Waste Handling Building (DOE, 2001b)

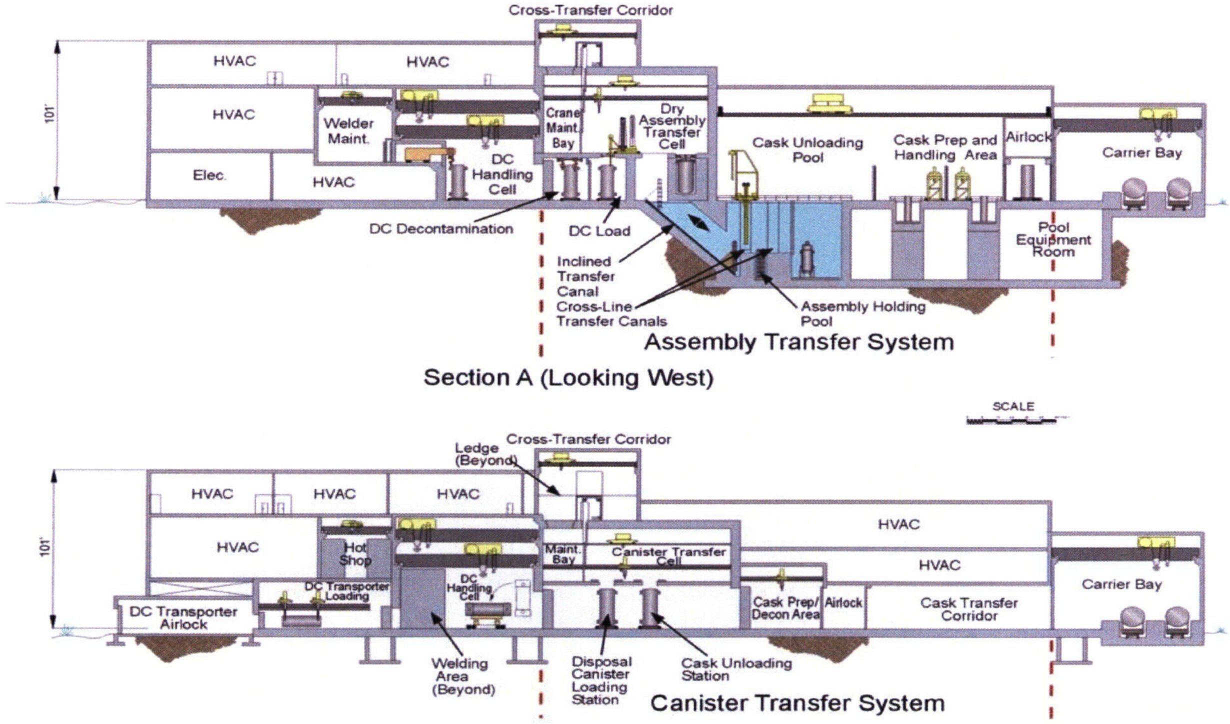


Figure 3-3. Sections A and B of Waste Handling Building (DOE, 2001b)

thicknesses varying from 0.3 to 0.9 m [1 to 3 ft], while the dry transfer area, assembly cells, disposal container load and decontamination, and disposal container welding and staging areas will have a concrete wall thickness of 1.5 m [5 ft]. The roof structures will be concrete slabs 20–25 cm [8–10 in] thick supported by steel beams and concrete walls. Other factors that affect the building structure and foundation loads are heavy-duty overhead cranes, with capacities of up to 160 tons and concentrated loads on the operating floor from casks and disposal containers on the transfer cart. Radiological areas will have 1.5-m [5-ft] thick floors.

The restricted-access area for waste-handling and packaging facilities will include buildings and equipment for receiving and packaging all incoming wastes. The surface plant also will include a waste treatment facility for processing all the radioactive wastes generated by onsite operations (e.g., protective clothing, decontamination fluids, and ventilation filters). Support facilities for the repository will include offices for administrative, management, and engineering staff; a firehouse; medical, training, and computer centers; a vehicle maintenance and repair shop; security buildings; a machine and sheet metal shop; and an electrical shop. Warehouses will be needed to store bulk materials, equipment, spare parts, and supplies.

Facilities for environmental measurements and instrument laboratories will also be required. Surface facilities in support of the underground operations include staff changing rooms and showers, as well as space to store mining equipment and vehicles. Electric transmission lines will be extended to the repository facilities from existing local utility lines, and a new substation will be provided at the site. Utilities that support the repository will include an electric power building with emergency electrical-generating equipment, steam-generating equipment, compressor and chiller systems, and cooling towers with water-treatment equipment. A system for treating and distributing potable water and water for fire protection also will be required. New wells or storage tanks may be needed to supply the water required during construction and operation of the repository. Finally, stations for dispensing gasoline and diesel fuel will be required at the site. Various DOE reports provide further description of the repository surface facilities (DOE, 1998, 2001b; CRWMS M&O, 1999d).

3.2.1.2 Subsurface Facility

The subsurface facility includes (i) the infrastructure, (ii) systems for transport and handling and emplacements of waste packages, (iii) a system for controlling and monitoring such operations, and (iv) systems to maintain and monitor the performance of the infrastructure and waste packages throughout the preclosure phase (DOE, 2001b; CRWMS M&O, 1997).

The repository subsurface facilities consist of portals and access ramps, access mains, emplacement drifts, openings to support the subsurface ventilation, and openings to support monitoring and performance-confirmation testing (CRWMS M&O, 1998b). The waste packages will be emplaced in the repository siting volume (DOE, 1998). The repository host horizon is located above the water table in the unsaturated zone, consisting of volcanic tuff. The repository emplacement drifts and perimeter main drifts will be located entirely within this siting volume. The layout of the subsurface portion of the repository for the high-temperature operating mode is shown in Figure 3-4. Principal features identified in the figure include the North and South Ramps, the east and west main drifts, the exhaust main drift located between and below the east and west drifts, and the emplacement drifts. The physical location and general arrangement of the subsurface facility in the unsaturated zone above the water table take advantage of the natural geologic barriers and other attributes as part of the overall waste containment strategy. Another design consideration was locating the emplacement drifts away from major faults. A detailed description of the repository subsurface facilities is available in various DOE reports (DOE, 1998, 2001b; CRWMS M&O, 1999e, 2000b,g).

The subsurface facility infrastructure includes tunnels, a shaft, a rail, and a support system, including the subsurface ventilation system and the electrical power system. The primary tunnels, North Ramp, North Ramp Extension, Main Access Drift, and turnouts provide pathways for transport of waste packages to the emplacement drifts as shown in Figures 3-5 and 3-6 (DOE, 1999). The portal and access ramps (north portal, south portal, north ramp, and south ramp) of the existing exploratory studies facility will be integrated into the proposed repository and would connect the surface and subsurface facilities through the access mains. The access mains are network of tunnels that define the perimeter of, and provide access to, the proposed emplacement area. The access mains comprise the north-south trending east main and west main, which are interconnected through other shorter tunnels, such as the north and south mains, and to the surface facility through the access ramps (CRWMS M&O, 2000b). The access mains have a nominal diameter of 7.62 m [25 ft] and are provided with rail lines, installed on concrete invert, and a trolley cable suspended from the crown, to support the transportation of the waste packages to and from the emplacement area. The North Ramp has a downward grade of 2.15 percent. The east and west mains will also conduct intake ventilation air to the emplacement area (CRWMS M&O, 2000c). The emplacement drifts will be an array of horizontal tunnels trending approximately east-northeast-west-southwest

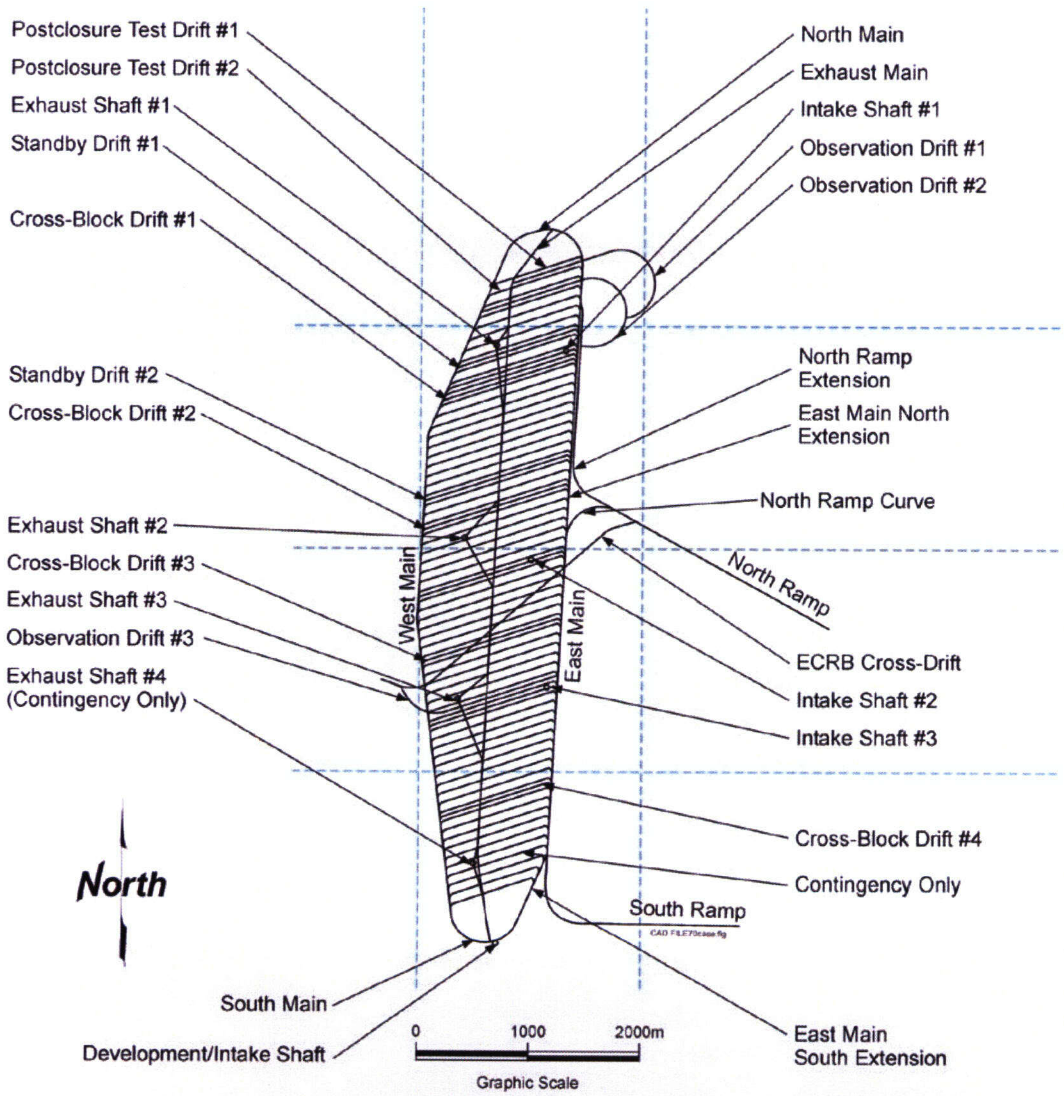


Figure 3-4. Proposed Repository Subsurface Layout for High-Temperature Operating Mode (DOE, 2001b)

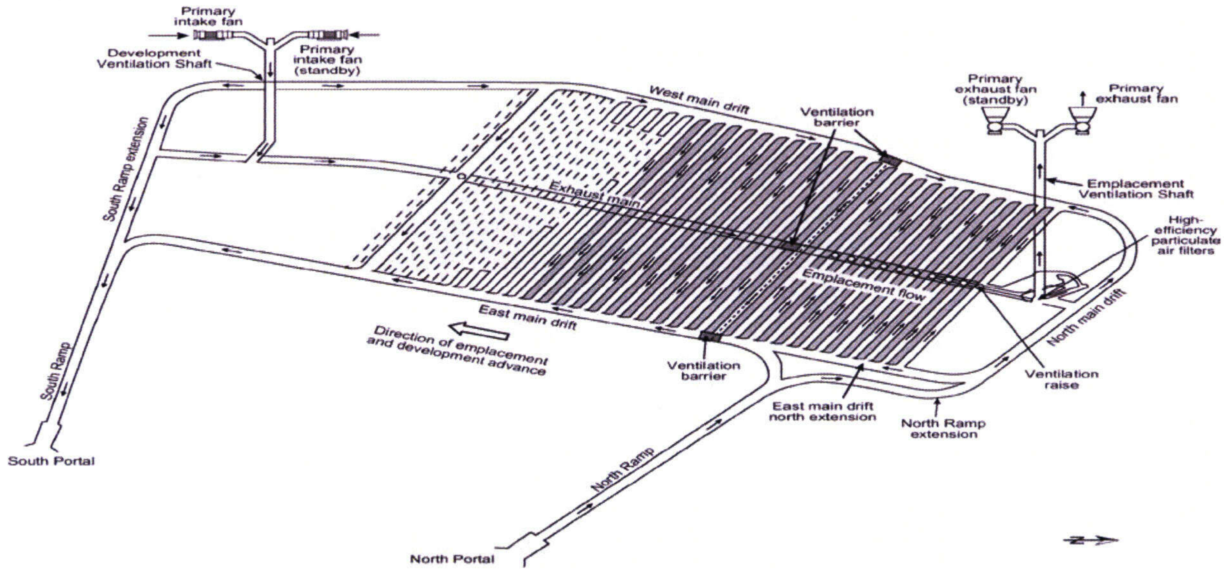


Figure 3-5. Subsurface Conceptual Design during Operations and Construction (DOE, 1999)

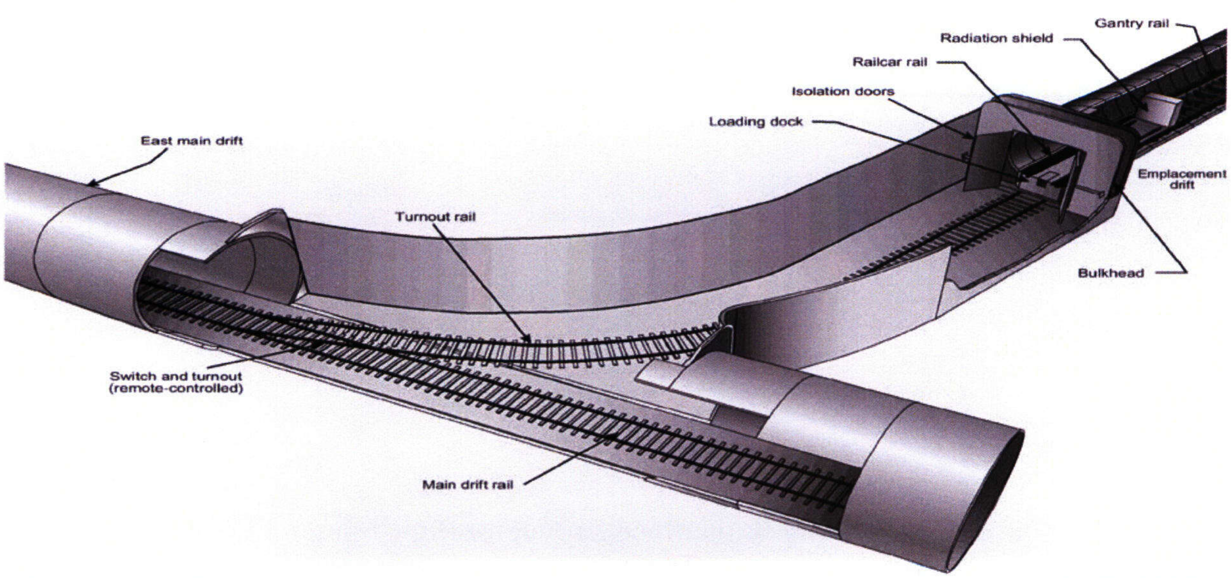


Figure 3-6. Emplacement Drift Branching from Main Drift and Rail System (DOE, 1999)

(252 azimuth) between the east and west mains. Each drift will have a diameter of 5.5 m [18.5 ft] and will be separated from the adjacent drifts by a center-to-center distance of 81 m [265.7 ft]. The concrete invert in emplacement drifts will support rails and pedestals that receive and support waste packages. The waste packages will be placed axially over the entire length of each emplacement drift, with spacing between packages to control the temperature of the rock mass, waste form, and waste package components. The transition from the east and west mains to the emplacement drifts (which are nearly perpendicular to the mains) will be provided through the emplacement-drift turnouts. A pair of isolation doors located near the emplacement-drift and access-main ends of each turnout will help control airflow into the emplacement drifts and protect the access mains from radiation from the waste packages in the emplacement drifts. The ground-support system for the emplacement drifts will consist of steel sets and wire mesh, with occasional rock bolts installed in the roof area during construction, if considered necessary. The ground support will be of carbon-steel material and will be designed for an operational life of up to 175 years with possible extension to 300 years (CRWMS M&O, 2000d,g).

The other openings that constitute the underground facility include the north-south trending exhaust main located below the emplacement drifts; ventilation raises (i.e., shafts excavated from the floor of the emplacement drifts to the roof of the exhaust main); the intake and exhaust shafts; and other drifts within the emplacement block that will be used for various purposes other than waste emplacement. The ground-support system for the nonemplacement openings (including the access mains) will initially consist of pattern rock bolts and welded wire fabric, and, where necessary, shotcrete or steel sets. A final ground support consisting of a cast-in-place concrete lining will be installed to provide long-term support of the openings during the preclosure period.

3.2.2 Description of Surface Systems and Operations

3.2.2.1 Surface Systems and Operations

During the operations phase of the repository, the two main activities of the surface operations are receiving and preparing waste. The primary system and the subsystems associated with receiving and handling operations in surface facilities are (DOE, 2001a,b; CRWMS M&O, 1999d,f)

- Cask/Carrier Shipping and Receiving System
  —cask/carrier transport system
  —carrier preparation material handling system
- Waste Preparation System
  —carrier/cask handling system
  —canister transfer system
  —assembly transfer system
  —disposal containers handling system
- Essential Support Systems
  —electrical power system
  —fire protection system
  —radiation monitoring and control system
  —ventilation system

—treatment and cooling system for pool water
- –water treatment system
- –leak detection system
- –water level management system
- –supplemental water system to control water temperature

3.2.2.1.1 Cask/Carrier Shipping and Receiving System

The cask/carrier shipping and receiving system consists of the cask/carrier transport system and the carrier preparation material handling systems. The transportation casks containing spent nuclear fuels and vitrified high-level waste would be transported from waste-generating sites by rail or road to the North Portal area. After security verification and inspection of the cask, the carrier would enter the radiologically controlled area and be stationed in parking areas until scheduled for processing. The cask/carrier transport system would move the cask and the carrier inside the facility.

Carrier/cask transport system. The carrier/cask receiving system receives casks by rail and truck and provides parking for carriers and prime movers. Incoming shipments are inspected, and off-site transporters are parked. The off-site transporters are disengaged from the carriers, and site prime movers are engaged to transport to the Carrier Preparation Building and then from the Carrier Preparation Building to the Waste Handling Building. The sequence of operations is schematically shown in Figure 3-7 (CRWMS M&O, 1999a).

Carrier preparation material handling system. The operations in the Carrier Preparation Building, schematically shown in Figure 3-8 (DOE, 2001b), include moving a loaded carrier/cask into an available preparation bay using the site prime mover, removing the personnel barriers, retracting impact limiters, surveying cask surface for radiation, decontaminating cask surface (if necessary), measuring cask temperature, and installing any required special tools or devices. The carrier preparation system uses one 10-ton capacity remotely operated overhead bridge crane and one remotely operated manipulator in each pair of preparation lines. The system supports both manual and remote handling of carrier/cask materials. The prepared carrier/cask will then be taken to the carrier parking area to await movement to the Waste Handling Building pending clearance.

3.2.2.1.2 Waste Preparation System

The waste preparation system housed in the Waste Handling Building consists of the carrier/cask handling system, the canister transfer system, the assembly transfer system, and the disposal canister handling system.

Carrier/cask handling system. The carrier/cask handling system unloads casks and dual-purpose canister overpacks from the truck and rail carriers in the carrier bay of the Waste Handling Building. The mechanical flow diagram of the carrier/cask handling system is shown in Figure 3-9 (DOE, 2001b). The truck or rail carrier is towed into the Waste Handling Building by the on-site transporter site prime mover after a water washdown at the carrier washdown station. A 160-ton capacity bridge crane reorients the cask from horizontal to vertical, lifts it off the carrier, and places it on a cask transfer cart. The transfer cart, operated remotely, carries the cask to either the canister transfer system or the assembly transfer system.

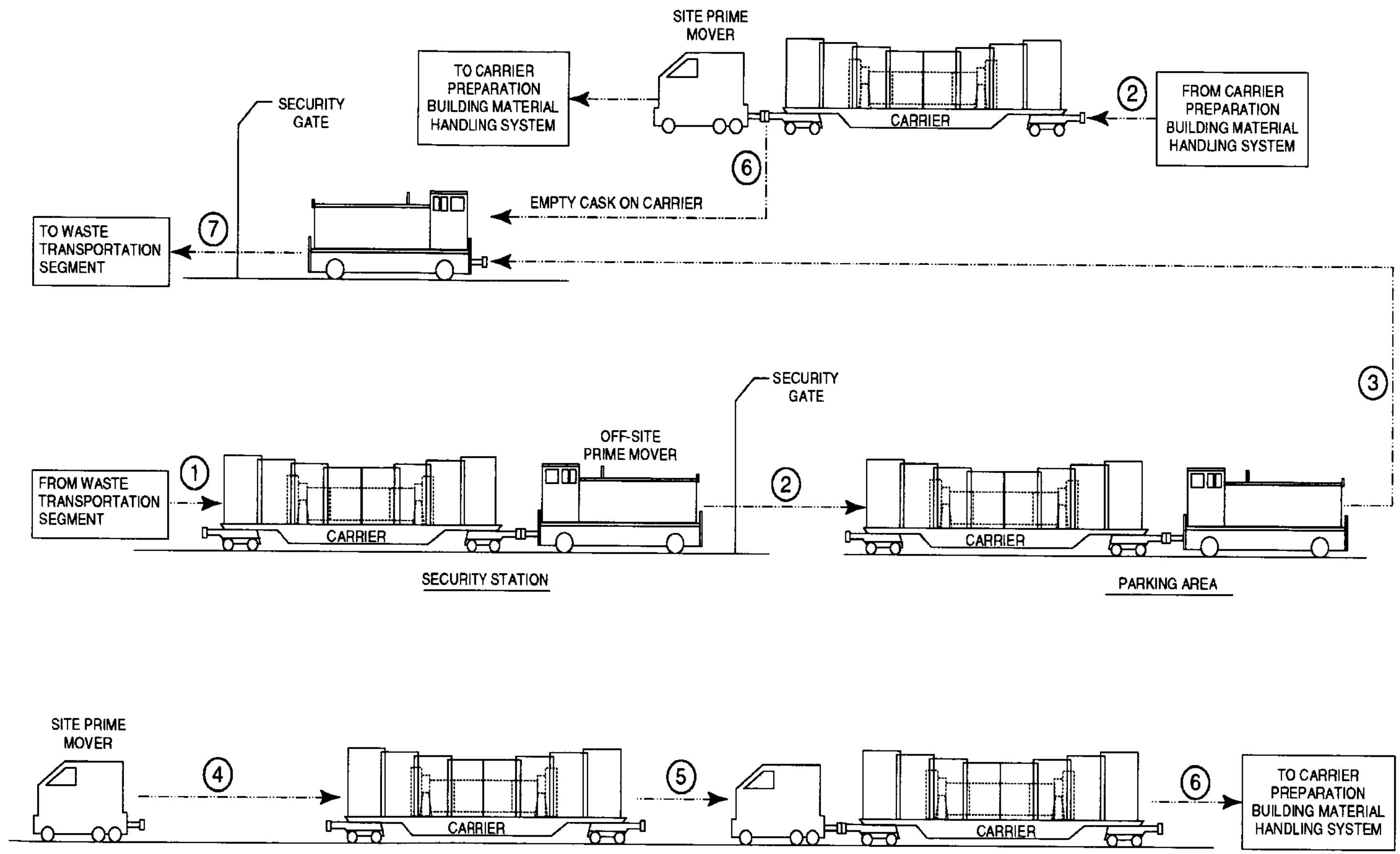


Figure 3-7. Transportation System, Site Prime Mover Engaged to Cask Carrier (CRWMS M&O, 1999a)

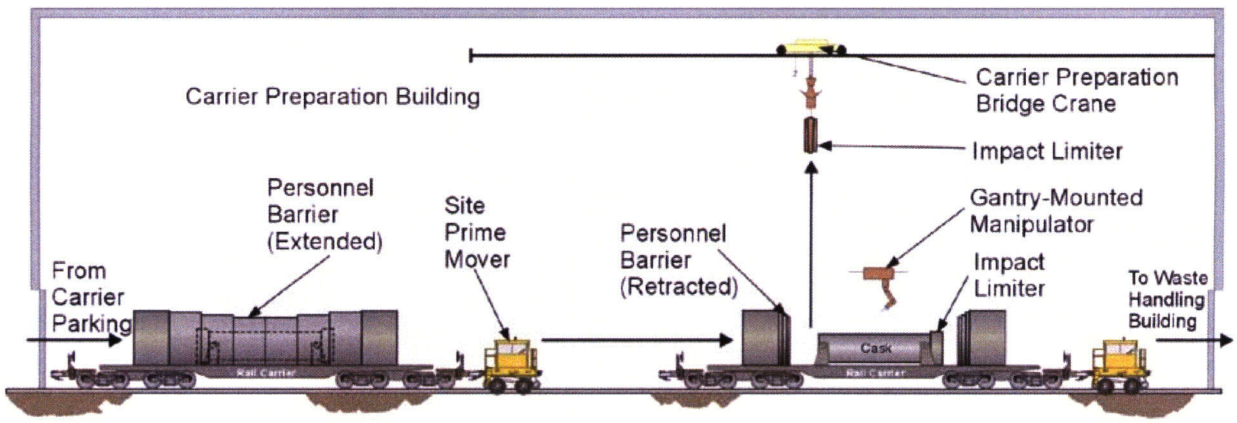


Figure 3-8. Carrier Preparation Material Handling System (DOE, 2001b)

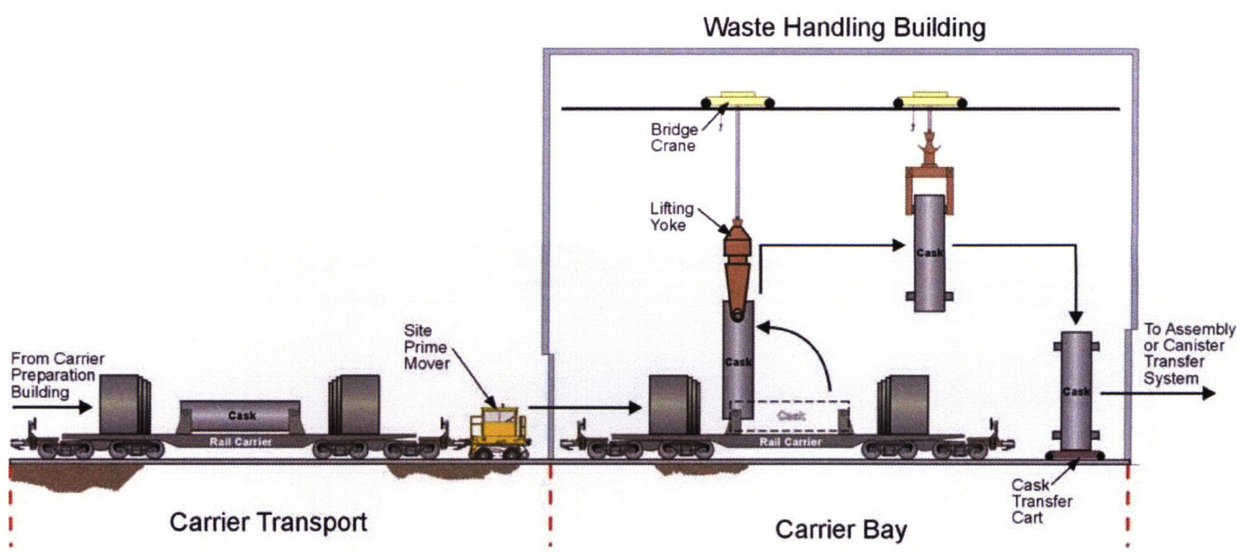


Figure 3-9. Carrier/Cask Handling System (DOE, 2001b)

Canister transfer system. The canister transfer system receives casks containing waste in disposable canisters and transfers the canisters to disposal containers. The Waste Handling Building would have one canister line to move high-level waste canisters, DOE spent fuel canisters, and Naval fuel canisters through the system. The mechanical flow diagram of the operations for the canister transfer system is shown in Figure 3-10 (DOE, 2001b). The vertically loaded cask would enter the cask preparation area on the remotely operated transfer cart through an airlock. The airlock, which maintains lower air pressure in the canister transfer work area, has two remotely operated isolation doors at both ends. In the cask preparation area; the cask would be vented; gasses sampled; lid bolts removed; and the cask opened, with outer cask lid removed, and decontaminated with remotely operated cask preparation manipulator and required tools. The transfer cart would then move the canister to the shielded canister transfer cell. At the unloading station of the canister transfer cell, the cask inner lid would be removed and the canisters would be lifted from the cask to be loaded into the disposal canister. At the disposal canister-loading station, the large canisters are loaded directly into a disposal canister, while small canisters are either loaded directly into a disposal canister or accumulated in a staging rack for temporary storage. The staging rack would hold 20 small canisters for either heat balance or schedule operations. The transfer operations of the canisters would be achieved using a remotely operated 65-ton overhead bridge crane, a manipulator, and canister-lifting fixtures. The canister transfer system would also consist of an off-normal handling cell next to a canister transfer cell connected by a transfer tunnel. The off-normal cell would handle damaged canisters that do not meet the acceptance criteria for corrective actions using a remotely operated overhead crane, manipulator, and welding stations. The loaded disposal canister is then transferred to the disposal canister handling system.

Assembly transfer system. In the assembly transfer system, shown in Figure 3-11 (DOE, 2001b), a vertically loaded shipping cask enters through an airlock into one of the three identical assembly transfer lines from the carrier/cask handling system. The cask, on a remotely operated cart, will pass into a cask preparation area.

In the preparation area, casks containing uncanistered fuel assemblies are prepared for unloading using a series of remote operations for sampling the interior gas, venting, cooling, shield plug unbolting, filling the cask with water, and loosening the lid bolts. For casks containing a dual-purpose canister, preparation includes remotely removing the cask lid and preparing the dual-purpose canister for unloading by sampling the interior gas, venting, cooling, and attaching dual-purpose canister lifting fixtures. A large bridge crane then moves the cask into a cask unloading pool.

In the pool, depending on the cask type, either the cask shield is removed (thus providing direct access to the fuel assemblies) or the dual-purpose canister is unloaded from the cask with the bridge crane. The dual-purpose canister welded lid is cut open.

The exposed assemblies are transferred by a wet fuel-handling machine to baskets in the assembly staging pool or directly to an underwater transfer cart. The cart transfers the assembly staging basket up through an inclined canal to the assembly handling cell.

The assembly basket may be transferred to the fuel blending and storage pools if needed. Fuel is stored and blended in this area to ensure that the waste package does not exceed the maximum design heat output of 11.8 kW [4.03×10^4 BTU/hr]. It is estimated that to meet the

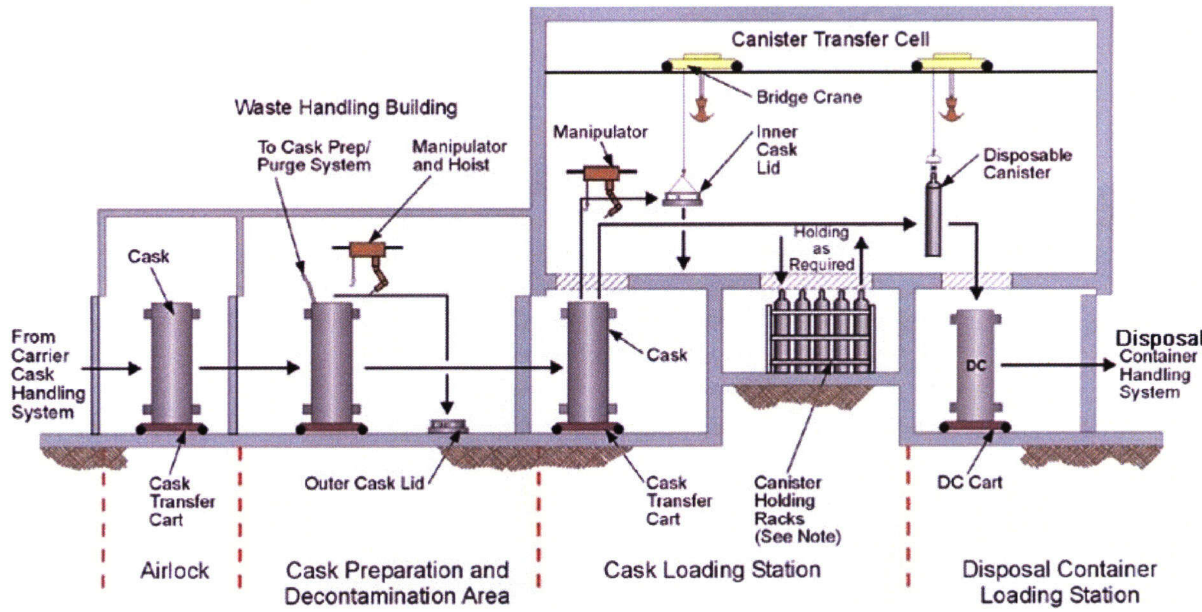


Figure 3-10. Canister Transfer System (DOE, 2001b)

waste package thermal load criteria, an inventory of 5,000 MTU (approximately 12,000 spent nuclear fuel assemblies in 2,800 assembly baskets) will be needed. The four fuel blending and storage pools will be designed for this total capacity (CRWMS M&O, 2000e).

Nonstandard spent nuclear fuel assemblies and single-element canisters are handled in the nonstandard fuel handling pool.

In the assembly handling cell, a vacuum drying system dries the assemblies before their transfer to an empty disposal canister by a dry-fuel-handling machine. During the transfer, the disposal canister will be mated to the cell through a transfer port to limit any spread of contamination.

Disposal canister load and decontamination cells are located below the transfer port. In these cells, the loaded disposal canister receives a temporary lid, disengages from the port, and will be transferred on a cart to the decontamination cell.

The disposal canister is decontaminated, temporarily filled with nitrogen, and temporarily sealed before transfer to the disposal canister handling system for permanent welding. All operations will be conducted remotely.

Disposal container handling system. The system provides empty disposal canisters to the assembly transfer system and canister transfer system to be loaded with either the assemblies or canisters. The operations for the disposal canister handling system are schematically shown in Figure 3-12 (DOE, 2001b). A remotely operated cart moves the disposal canister from the

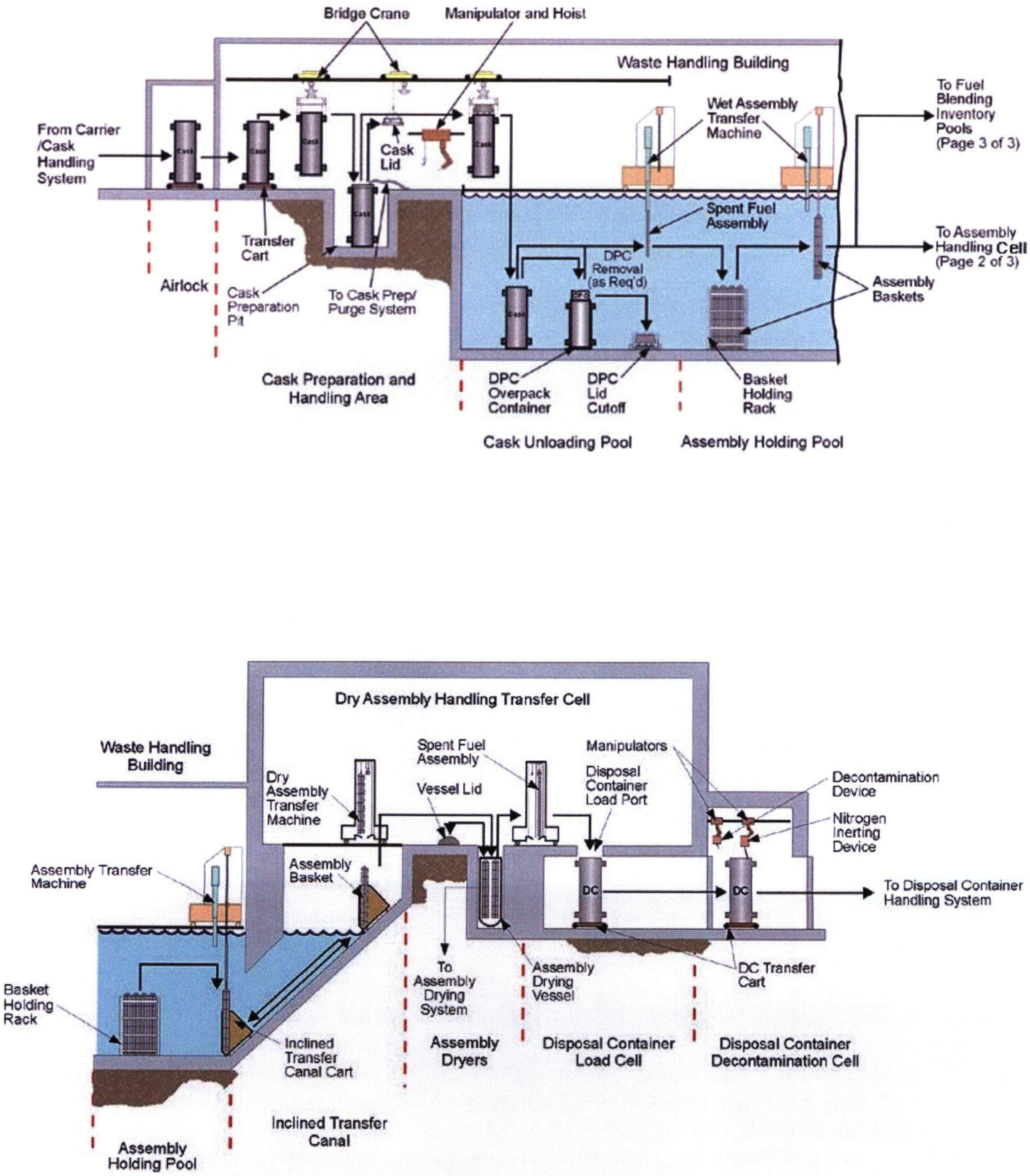


Figure 3-11. Assembly Transfer System (DOE, 2001b)

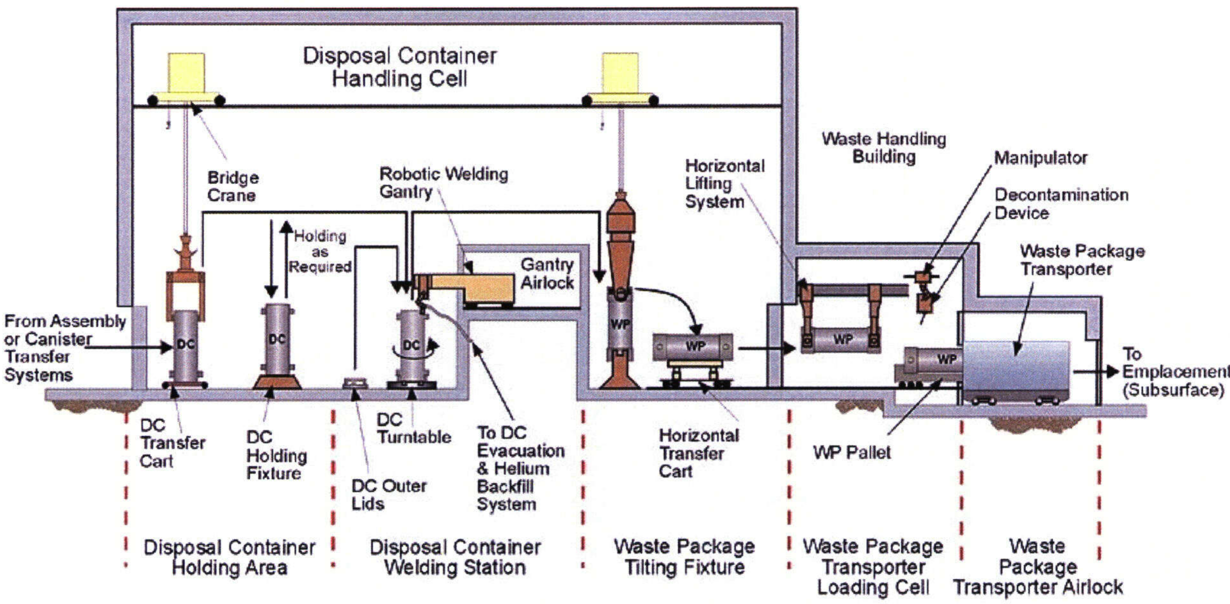


Figure 3-12. Disposal Container Handling System (DOE, 2001b)

assembly transfer system or canister transfer system in a vertical position within the reach of a large bridge crane. The crane moves the disposal canister to the disposal canister staging area or directly to a disposal canister welding station. At the welding station, the operations are (i) welding of inner lid, (ii) inspecting, (iii) filling the disposal canister with helium, (iv) welding of outer lid, and (v) inspecting. The welding is accomplished using a robotic welder mounted on a gantry. The disposal canister is placed on a rotating turntable during welding at the welding head station. The welded and loaded disposal canister is called a waste package, which is lifted from the welding station and placed in a staging fixture or directly in a waste package tilting fixture. A crane lowers the waste package onto a horizontal transfer cart. The cart transfers the waste package from a disposal handling cell to a waste package transporter loading cell, then to the waste package transporter airlock.

3.2.2.1.3 Essential Support Systems

The electrical system of the Waste Handling Building performs the functions of conditioning, distributing, monitoring, and controlling power to all waste handling facility users (CRWMS M&O, 1999d,f) . The system consists of the transformers, switch gear, controllers, uninterruptible power supplies, and distributor subsystems required to power facility lighting, ventilation, instrumentation, process, and mechanical equipment. The Waste Handling Building fire protection system performs the functions of detecting a fire, alerting facility personnel, and automatically suppressing the fire with a wet sprinkler system (CRWMS M&O, 1999d,f). The sprinkler water will be collected by floor drains and routed to a holding tank. The Waste Handling Building radiological monitoring system will monitor, display, annunciate, and report on the radioactivity levels in the facility equipment and operating areas, exhaust air, waste water, and facility effluents under normal and off-normal conditions. The Waste Handling Building ventilation system supplies fresh air and controls the environmental conditions to equipment and operating areas within the facility (CRWMS M&O, 1999d,f). The system operates in conjunction with facility physical barriers to control the airflow and pressure within the facility and filter the air to prevent radioactive contamination, exposure, and release. The Waste Handling Building will contain nine pools and several transfer canals for the Assembly Transfer System (CRWMS M&O, 1999d,f). The treatment and cooling system for pool water consists of a water cooling system; a water treatment system; a leak detection system; a water level management system; and a supplemental water system to control water temperature, control water quality and radioactive contamination, detect water leaks, and control pool water levels.

3.2.2.2 Subsurface Systems and Operations

The primary system and subsystem associated with subsurface operations are (DOE, 2001b; CRWMS M&O, 1997, 1999e) as follows:

- Waste package transport train system
- Rail system for transporter train
- Waste package emplacement gantry system

Brief descriptions of the systems follow.

3.2.2.2.1 Waste Package Transporter Train

The transporter train consists of two locomotives and the transporter. The two locomotives will be powered by an overhead electric trolley and will be identical except that the primary locomotive will be permanently coupled to the transporter, while the secondary locomotive will be frequently coupled and decoupled to the transporter. The train may be operated either remotely from the centralized control room via radio signals or by on board manual control. The maximum speed of the fully loaded transporter will be 8 km/hr [5 m/hr]. Although the transporter and both locomotives will be provided with multiple brake systems (e.g., dynamic service brake, emergency brake, and parking brake), transporter train runaway down the North Ramp is a credible event.

3.2.2.2.2 Rail System for Transporter Train

The subsurface rail (track) system extends from the exit of the Waste Handling Building to the North Portal and into the North Ramp and throughout the Main Access Drifts and turnouts. There will be many switch tracks to accommodate operations such as coupling and decoupling of locomotives to the transporter and reorientation of transporter as necessary in the drifts. Each switch track will be remotely operated and instrumented for remote position indication. The reliability of the rail system to maintain the gauge and the alignment between rail segments and the reliability of the switch track mechanism for proper realignment in each emplacement operations are potential contributors to derailment. In addition, failures in the instrumentation and control and remote communications systems, failures in control software, and human actions may contribute to the likelihood of derailment.

3.2.2.2.3 Waste Package Emplacement Gantry

A remotely controlled device for the waste package emplacement functions in the emplacement drifts. The gantry is self-powered through a direct-current, third-rail system. Various failures in mechanical, electronic, software, and human function can contribute to potential events that may result in radiological dose release.

3.2.2.2.4 Other Systems

Other systems that contribute to the subsurface operations are remote control and data communications system, central control room, rail electrification system, subsurface ventilation system, and performance confirmation system for the gantry.

3.2.2.2.5 Sequence of Operations

During the active phase of the repository, when waste forms are being accepted at the repository, the transport and emplacement of waste packages will include the following operations (DOE, 2001b; CRWMS M&O, 1997, 1999e):

- At the Waste Handling Building, the waste package is transferred to the reusable railcar and loaded into shielded transporter railcars by remote control; the transporter is pulled away by the primary locomotive under remote control.
- After coupling a secondary locomotive to the transporter, the transporter train (two locomotives and a transporter) is driven under onboard manual control from the surface at the Waste Handling Building, down the North Ramp and Main Access Drift, and then to the turnout to the destination emplacement drift [see Figure 3-13, (DOE, 2001b)].
- After decoupling the secondary locomotive, the drivers vacate the locomotive. The transporter is backed into the turnout (pushed by the primary locomotive under remote control) to the vicinity of the emplacement drift isolation doors [see Figure 3-14, (DOE, 2001b)].
- The emplacement drift isolation doors are opened by remote control, and the transporter is backed to the emplacement drift transfer dock (pushed by one locomotive under remote control).
- The waste package is moved out of the transporter on the reusable railcar and transferred to the emplacement gantry; all operations are by remote control [see Figure 3-15 (DOE, 2001b).
- The emplacement gantry raises the waste package, transports it into the emplacement drift to the desired location, lowers it to the pedestals, and returns to the emplacement drift entrance; all operations are under remote control [see Figure 3-16 (DOE, 2001b)].

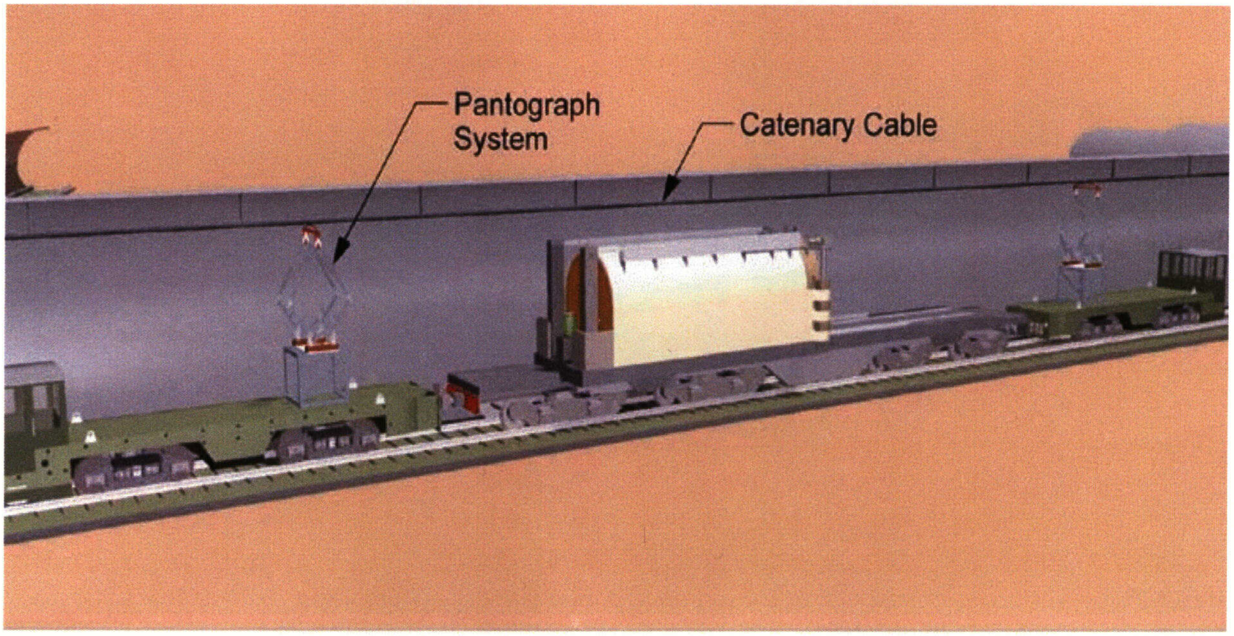


Figure 3-13. Waste Package Transported Down the North Ramp to the Repository (DOE, 2001b)

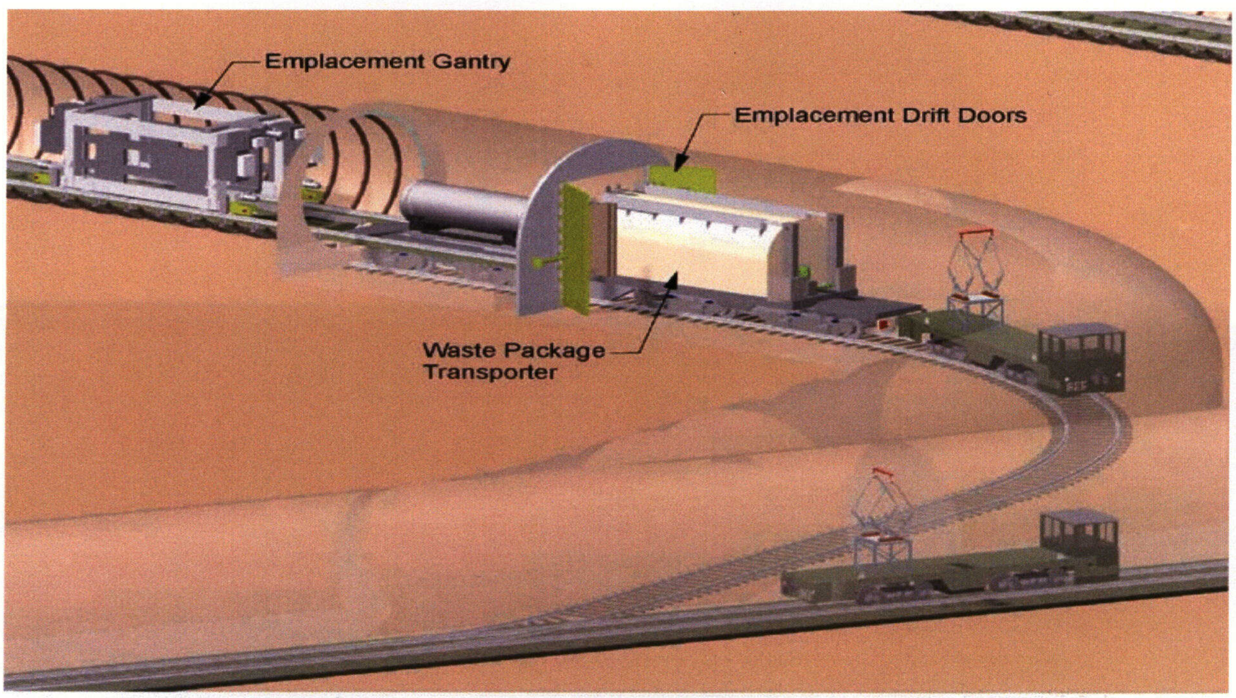


Figure 3-14. Secondary Locomotive Decoupled, Primary Transport, and Waste Package Transporter Move from Main Drift into Turnout (DOE, 2001b)

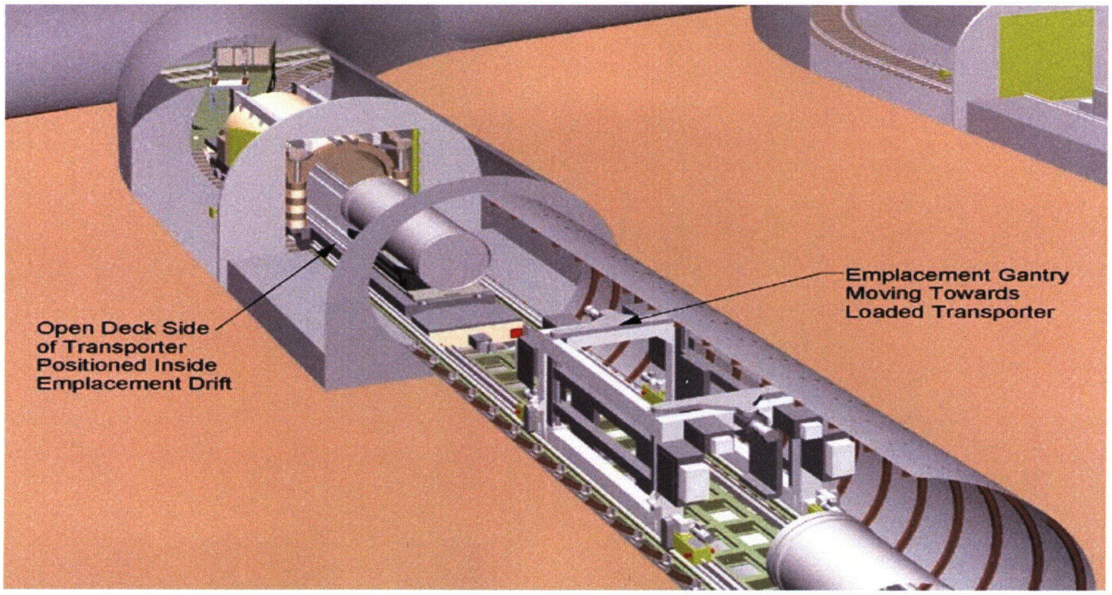


Figure 3-15. Waste Package Move Out of the Transporter Inside the Drift and Gantry Moves to Pick Up (DOE, 2001b)

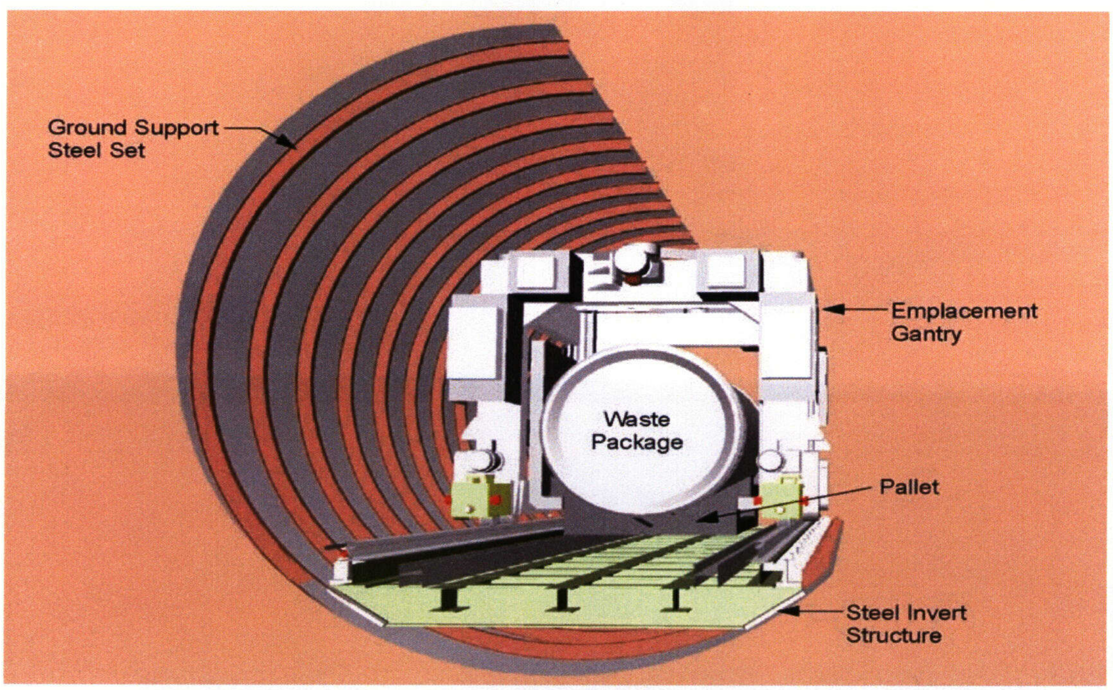


Figure 3-16. Gantry Picks Up Waste Package and Moves toward Emplacement (DOE, 2001b)

- After the train has moved from the transfer dock, the emplacement drift isolation doors are closed. After arrival of the train in the main drift, drivers return to the locomotive for recoupling of the secondary locomotive and a return trip to the surface to receive another waste package.

The operations and equipment and components for major systems involved in handling high-level waste in surface and subsuface facility are summarized in Table 3-1.

3.2.3 Waste Handling Schedule

The repository will have the capability to receive and emplace approximately 70,000 MTU of waste. The waste will arrive at the repository by rail or truck and be received at the radiologically controlled area 24 hours a day. Rail shipment will arrive at the site as a unit train consisting of one or two locomotives, three to five rail cars carrying one cask per rail car, and buffer rail cars between rail cars with casks. Truck shipments will arrive in legal-weight trucks. DOE developed a schedule of receipt based on a reference design (CRWMS M&O, 1999d). The reference design is based on a peak annual receipt rate of 3,000 MTU over an operational period of 24 years. Annual rate of receipt and handling of casks, canisters, fuel assemblies, and disposal canisters in the facility will vary. In the preclosure safety analysis, however, it is

important to note the maximum handling rate because proposed 10 CFR 63.21(c)(5) requires that the preclosure safety analysis are carried out at maximum capacity and rate of receipt of waste. The total and maximum annual receipt and handling of casks, canisters, and disposal canisters in different areas of the facility are given in Table 3-1 (CRWMS M&O, 1999d).

3.3 PCSA Tool Capabilities

The preclosure safety analysis requires information on site data and facility design and operations. The tool does not have provisions to store site-specific data required to review each naturally occurring and human-induced hazard because the tool is not used to conduct in-depth review of these hazards. The tool, however, provides capability to store essential information in the project database required to review and conduct operational hazards. The entire facility is divided into major functional areas, which can be further divided into subareas. Under each functional subarea, the PCSA Tool conducts operational hazard analysis, event sequence analysis, and radiological dose consequence analysis.

3.3.1 Functional Area

3.3.1.1 General

DOE divided the repository operations area and the related processes into functional areas to facilitate preclosure safety analysis (Bechtel SAIC Company, LLC, 2002, DOE, 2001a; CRWMS M&O, 1999b). Functional areas are established by specific functions or physical boundaries or both. Segmenting the facility repository into several functional areas for convenience of preclosure safety analysis is reasonable, and a similar concept has been adopted in the PCSA Tool. The tool has been designed to develop a project tree by dividing the facility into major functional areas, then dividing each functional area into several subareas.

Table 3-1. Operations and Components/Equipments for Surface and Subsurface Facility*		
System	**Operations**	**Component/Equipment**
1. Transportation System (Figure 3-7)	1. Cask from distant site received 2. Off-site rail/truck disengaged from cask carrier 3. Site prime mover engaged to the cask carrier 4. Cask carrier transported to Carrier Preparation Building	1. Rail cask carrier 2. Truck cask carrier 3. Site prime mover 4. Equipment to engage and disengage carriers
2. Carrier Preparation Material Handling System (Figure 3-8)	1. Carrier and cask surveyed for radiation 2. Personnel barriers removed 3. Contaminants sampled 4. Cask temperature measured 5. Cask impact limiters removed	1. Site prime mover 2. Overhead bridge cranes 3. Gravity-mounted manipulator 4. Fixtures for removing barriers and impact limiters
3. Transportation System	1. Cask transported from Carrier Preparation Building to Waste Handling Building	1. Site prime mover
4. Carrier Cask Handling System (Figure 3-9)	1. Cask tilted from horizontal to vertical 2. Cask unloaded from rail or truck carrier 3. Cask placed on transfer carts	1. Site prime mover 2. Remotely operated overhead bridge cranes 3. Gantry-mounted manipulator 4. Lifting yoke, tools, and fixtures 5. Transfer carts

Table 3-1. Operations and Components/Equipments for Surface and Subsurface Facility* (continued)		
System	**Operations**	**Component/Equipment**
5. Canister Transfer System (Figure 3-10)	1. Canister unloaded from cask 2. Canisters stored in staging rack 3. Canisters loaded into disposal container 4. Large canisters loaded directly from transportation cask to disposal container 5. Lid unbolted 6. Lid removed 7. Decontamination	1. Area-shielded hot cell 2. Remote-operated cask transfer carts 3. Cask preparation manipulators 4. Equipment for samples 5. Bridge crane 6. Shield door 7. Cameras 8. Various lifting fixtures
6. Assembly Transfer System (Figure 3-11)	1. Cask placed in unloading pool 2. Inner shield plug removed under water 3. Spent nuclear fuel assemblies individually removed from open cask into assembly basket 4. Assembly basket transported from basket staging rack to incline underwater transfer cart 5. Assembly transferred to drying vessels 6. Dry assembly placed into a disposal container 7. Disposal container inner lid installed 8. Decontamination of disposal container	1. Bridge crane 2. Underwater camera 2. Manipulator 3. Area shielded hot cell 4. Wet transfer machine 5. Disposal container transfer cart 6. Incline and cross-transfer cart 7. Dry-fuel-handling machine 8. Cameras 9. Decontamination equipment 10. Staging basket 11. Underwater camera 12. Shielded door

Table 3-1. Operations and Components/Equipments for Surface and Subsurface Facility* (continued)		
System	**Operations**	**Component/Equipment**
7. Disposal Container Handling System (Figure 3-12)	1. Disposal container transferred to and from assembly transfer and canister transfer system 2. Inner and outer lid welded 3. Disposal container temporarily loaded before and after welding 4. Disposal containers tilted to horizontal position 5. Disposal containers loaded onto waste emplacement transport 6. Decontamination	1. Area shielded hot cell 2. Remotely operated overhead bridge crane with lifting fixtures 3. Transfer carts 4. Disposal container welding/inspection 5. Welding station jib cranes 6. Weld turn table 7. Horizontal transfer cart 8. Horizontal lifting system 9. Decontamination and inspection manipulated 10 Robotic welding machine
Subsurface Systems (Figures 3-13 thru 3-16)	1. Waste package transported to underground drift 2. Waste package emplaced in the drift	1. Transport locomotive 2. Remote controlled gantry for waste package emplacement function 3. Drift isolation door
*CRWMS M&O. "Monitored Geologic Repository Internal Hazards Analysis." ANL–MGR–SE–000003. Revision 00. Las Vegas, Nevada: CRWMS M&O. 1999.		

The concept of functional areas embedded in the tool is demonstrated through an example. As an example shown in Figure 3-17, the facility is divided into six main functional areas: (a) Facility Gate, (b) Cask Carrier Parking Area, (c) Carrier Preparation Building (d) Area between Carrier Preparation Building and Waste Handling Building, (e) Waste Handling Building, and (f) Subsurface. Further sublevels under the six functional areas are shown in Figures 3-18 and 3-19. These figures show that main functional areas have been divided based on the systems used in that section of the facility. For example, the operations in the Waste Handling Building have more systems than any other functional areas, and some of the systems within the Waste Handling Building, such as the assembly transfer system, may require further sublevels. On the whole, the tool allows four levels of divisions and has the potential to create space in the database for 18,954 functional areas. The project tree assigns a functional identification to a functional area that helps in systematizing the data entry and data retrieval in the project database (see Figure 3-3) in the tool. For example, as shown in Figure 3-19, the functional identification for the functional area canister transfer cell is E.3.3. The canister transfer cell is a part of the canister transfer system, which is located within the Waste Handling Building.

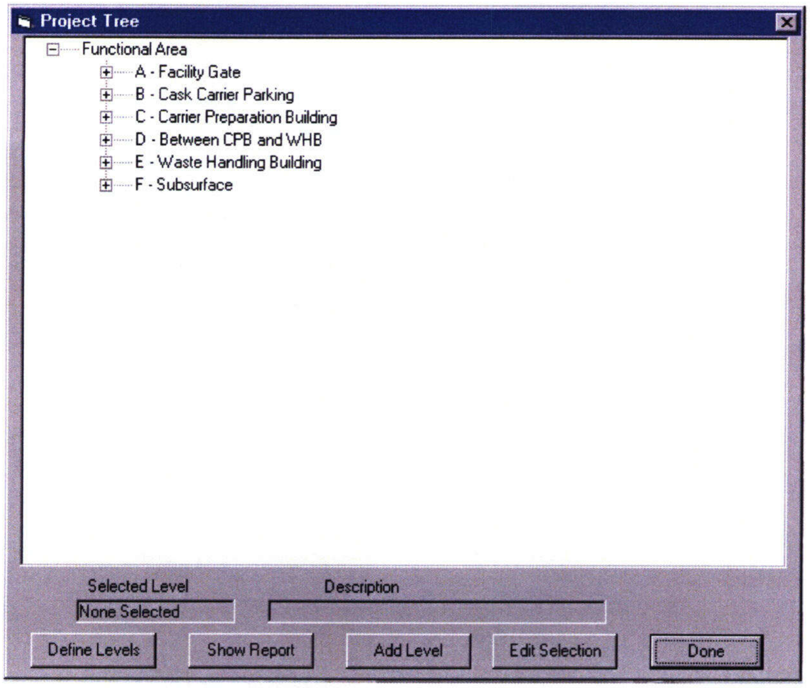


Figure 3-17. Project Tree Showing Main Functional Areas

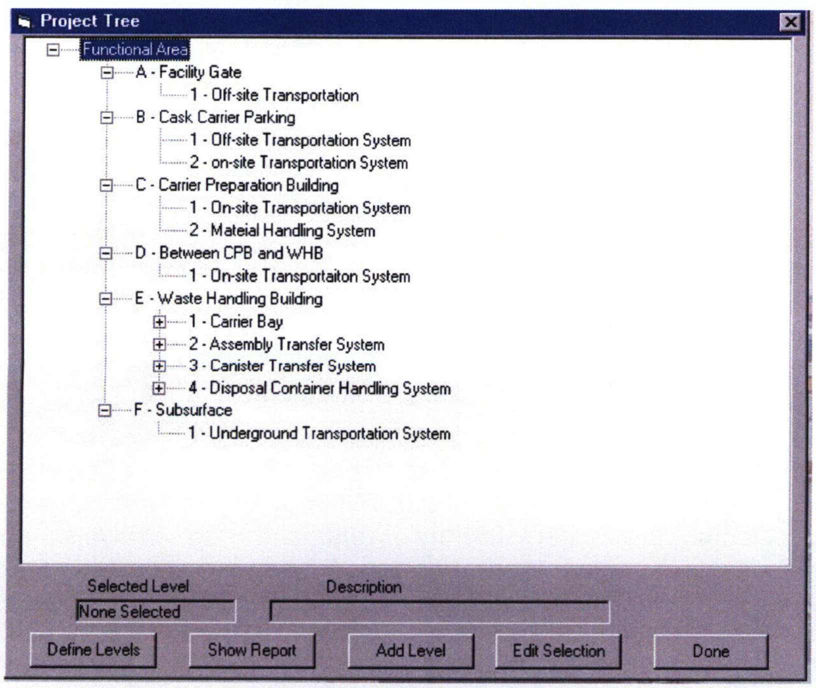


Figure 3-18. Project Functional Areas Expanded to Second Level

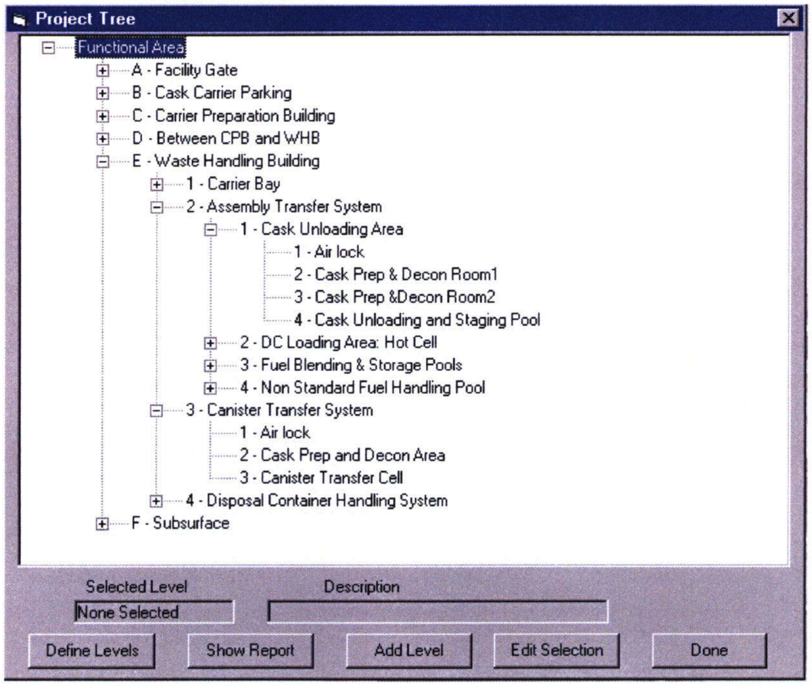


Figure 3-19. Project Tree Functional Areas Expanded to Third Level

3.3.1.2 PCSA Tool Function to Construct a Project Tree

In the PCSA Tool, the project tree is developed when a new project is first initiated using Create Project. The project tree is an expandable or collapsible tree view created by a process using mouse clicks and the button controls. The dialog box to create levels is shown in Figure 3-20. The levels are constructed by clicking on the alphabets and the sublevel numbers and then by pressing on the Apply button. The tree structure can be viewed using the View Tree button. To create the tree structure effectively, Reset and Delete buttons may be helpful. The session can be closed either by Done or Cancel buttons. The tree structure should be planned in advance before creating a project tree. After creating the tree structure, the Project Tree menu can be selected for additional operations, such as assigning level names using the Define Level button, editing level names using the Edit Selection button, generating and printing reports using Show Report button, and adding levels using the Add Level button. Information can be stored in the project database by selecting the end of a branch. The project tree assigns functional identification to that end branch. When a functional area (e.g., E.3.3, see Figure 3-19) is selected, the System, Internal Events and Freq. Analysis menus and Current Level Results submenu under the Performance menu are activated. By this process, the tool ensures that the information under those menus is stored and retrieved from the appropriate location linked by the functional identification. The remaining menus, SAPHIRE, Consequences, Performance, External Events, Probability, Checklists, Regs, and Help can be used with or without selecting a functional area. Online help for the first-time user of the tool will be available in future versions.

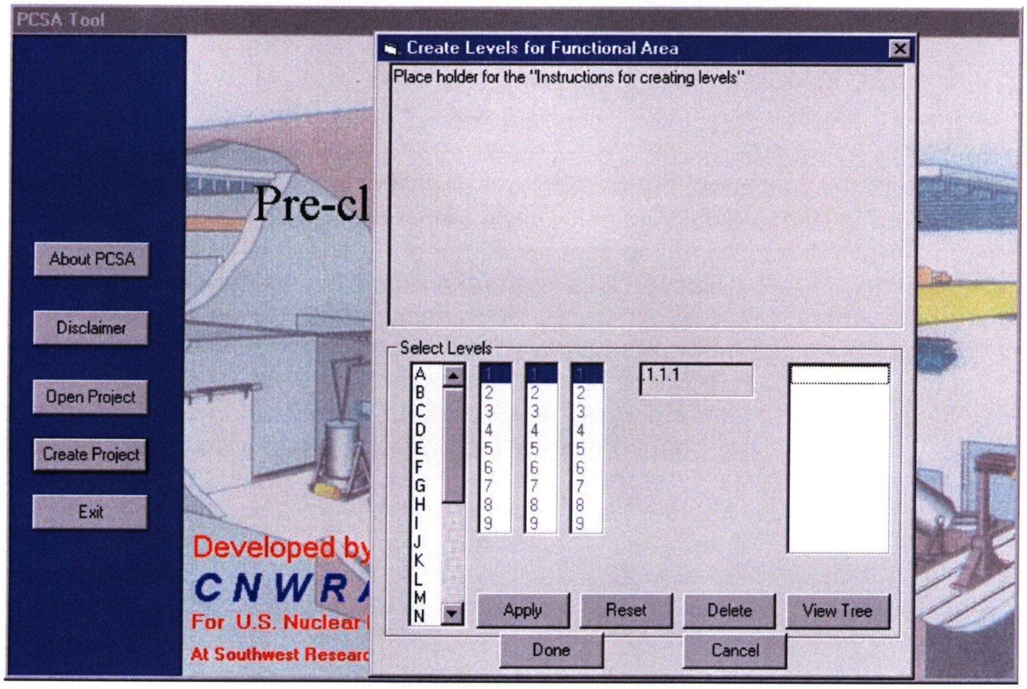


Figure 3-20. PCSA Tool Form to Create Levels

3.3.2 System Description

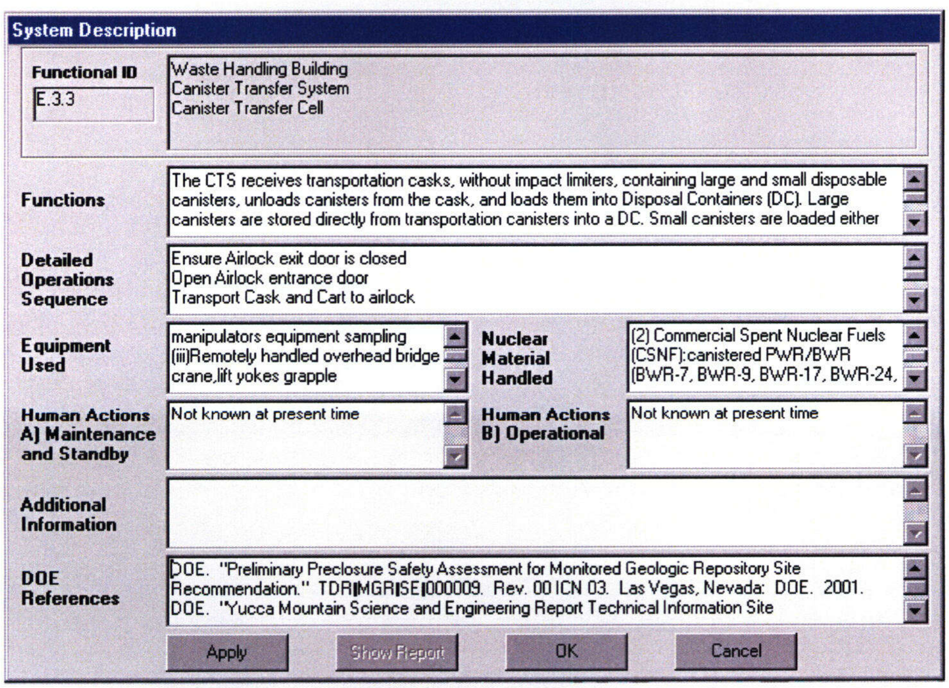
3.3.2.1 General

Information on the description of structures, systems, and components in the functional area including process, operations (remote and manual), systems and procedures for each functional area is stored in the project database. This information provides input to the operational hazard analysis, event sequence analysis, and consequence analysis. Requisite information is abstracted from review of the description of facility and facility functions and introduced into PCSA Tool under each functional subarea. The information is entered into the project database from the "System Description" form using the fields: Functions, Detailed Operations Sequence, Equipment Used, Human Actions (Maintenance and Standby Human Actions and Operational Human Actions), Source Terms, Additional Information, and DOE References.

The level of detail provided by DOE on the human actions anticipated as part of operations and the software systems used for computer control of equipment do not appear to be sufficient for preliminary evaluation of safety, including the identification of structures, systems, and components important to safety. Fundamental characteristics of the system needed to evaluate reliability and safety at a preliminary level that have not yet been specified include (i) designation of operations to be human or computer controlled, (ii) requirements for computer software and personnel, and (iii) central versus distributed control of human actions, computer systems, or both. In the present PCSA Tool, two types of human actions that would correspond to the types of human errors defined as Category A and Category B have been included. The details on the human reliability analysis is discussed in Chapter 4.

3.3.2.2 PCSA Tool Function to Describe System

The system description form is opened in the PCSA Tool by clicking on the SysDesc menu under System menu. The SysDesc menu can be used only when a functional area is selected from the Project Tree menu. The system description form provides fields to document a detailed description of the functions of the system, a detailed operation sequence, a list of equipment used, source terms in the functional area being analyzed, and human actions. The form also has provisions to store additional information and DOE references. The data entered can be reviewed using the Show Report button, and the report can then be printed. There is no restriction on the amount of data that can be stored in each field. The system description can be modified with improving design details. Data entered in the form can be transferred to the database using the Apply button; however, data can be permanently saved in the project database only by using the Save menu under the File menu. The text in each field can be edited using features such as cut, copy, paste, delete, select all, and undo, or accessed by right clicking on the mouse. The system description for the functional area E.3.3 (i.e., canister transfer cell) is shown in Figure 3-21 and serves as an example of a completed system description in the PCSA Tool. A sample of the system description report is shown in Figure 3-22.


System Description

Functional ID: E.3.3

Waste Handling Building
Canister Transfer System
Canister Transfer Cell

Functions: The CTS receives transportation casks, without impact limiters, containing large and small disposable canisters, unloads canisters from the cask, and loads them into Disposal Containers (DC). Large canisters are stored directly from transportation canisters into a DC. Small canisters are loaded either

Detailed Operations Sequence:
Ensure Airlock exit door is closed
Open Airlock entrance door
Transport Cask and Cart to airlock

Equipment Used: manipulators equipment sampling (iii)Remotely handled overhead bridge crane,lift yokes grapple

Nuclear Material Handled: (2) Commercial Spent Nuclear Fuels (CSNF):canistered PWR/BWR (BWR-7, BWR-9, BWR-17, BWR-24,

Human Actions A) Maintenance and Standby: Not known at present time

Human Actions B) Operational: Not known at present time

Additional Information:

DOE References: DOE. "Preliminary Preclosure Safety Assessment for Monitored Geologic Repository Site Recommendation." TDR–MGR–SE–000009. Rev. 00 ICN 03. Las Vegas, Nevada: DOE. 2001. DOE. "Yucca Mountain Science and Engineering Report Technical Information Site

Apply | Show Report | OK | Cancel

Figure 3-21. Example of System Description Form

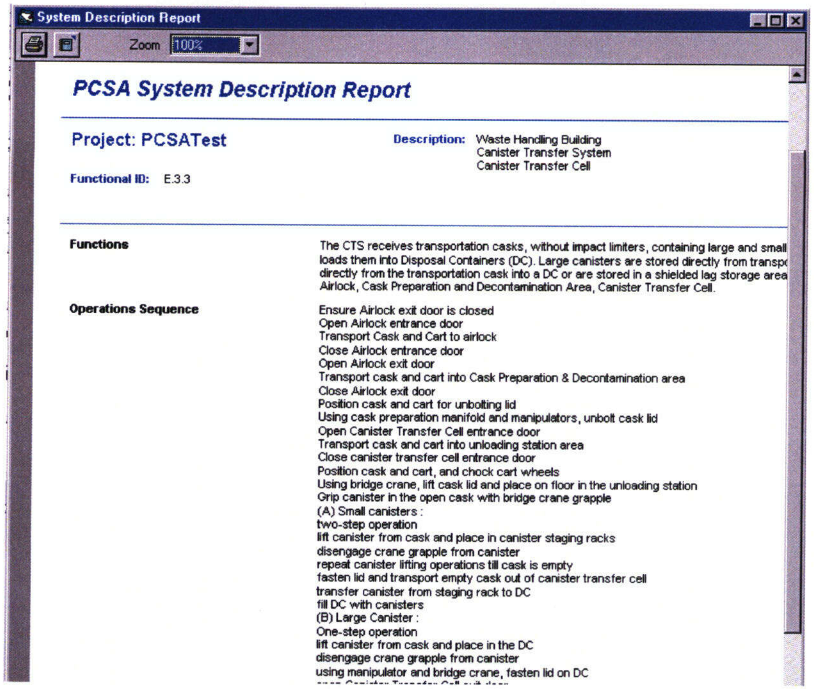


Figure 3-22. Example of System Description Report

4 IDENTIFICATION OF HAZARDS AND INITIATING EVENTS

The initial step in the preclosure safety analysis is a hazard analysis that systematically identifies facility hazards through hazard identification and hazard evaluation. Hazard analysis examines the complete spectrum of potential events that could expose the public or workers to radiological dose. The hazard analysis forms the basis for selection of initiating events and subsequent development of event scenarios and comprehensive identification of potential event sequences. Because the hazard analysis is the starting point for the preclosure safety analysis, which forms the basis for the U.S. Department of Energy (DOE) demonstration or the U.S. Nuclear Regulatory Commission (NRC) determination of compliance with the regulatory requirements, a critical element of the licensing review and the PCSA Tool is evaluation of hazards and initiating events.

Naturally occurring and human-induced events, in addition to operations hazards, may lead to an event sequence with potential for radiological release. Inadequate identification of hazards can lead to an incomplete and erroneous safety analysis, if the determination of the frequency of initiating event is not correct. Furthermore, the categorization of event sequences, a central element in the compliance demonstration, may be incorrect. Largely qualitative techniques are used in the hazard analysis to identify weaknesses in the design and operation of a facility that could lead to an event. The guidance for review of the identification of hazards and initiating events is provided in Section 4.1.1.3 of the Yucca Mountain Review Plan (NRC, 2002a). Review of the identification of hazards and initiating events would be based on review of technical basis and assumptions for methods used, use of relevant data, determination of frequency or probability of occurrence, the technical basis for inclusion or exclusion of specific hazards and initiating events, and completeness of the list of hazards and initiating events to be considered in preclosure safety analysis. The hazards and initiating events are then screened based on low probability or low consequence and mitigative controls. The purpose of the hazard analysis is to identify a limited subset of events that is carried forward for further safety analysis.

This chapter discusses the hazard analysis capabilities in the PCSA Tool for reviewing the DOE identification of hazards and initiating events that may potentially cause radiological consequence to the public or facility workers. It addresses the PCSA Tool module naturally occurring and human-induced hazards and initiating events shown in Figure 2-2(a).

4.1 Naturally Occurring and Human-Induced External Hazards

Site-specific hazards, naturally occurring and human-induced, external to the facility could act as initiating events to generate event sequences at the geologic repository operations area that could be significant contributors to the release of radioactive materials. The naturally occurring events include seismic, tornado, wind, flood, and other such events; while human-induced events include aircraft crash, fire, and other such events. Identification of natural and human-induced external hazards requires, as discussed in Chapter 3, site-specific information, such as description of the site, location of the facilities within the site, proximity to the public and other facilities, meteorology, seismology, hydrology, geology, etc. The DOE external hazard analysis methodology (CRWMS M&O, 1999a) consists of a screening process to identify hazards from a generic events list of natural and human-induced external hazards. In compliance with the guidance in the Yucca Mountain Review Plan, the review would verify the appropriateness of use of site-specific data to identify naturally occurring and human-induced external hazards and verify the technical basis for inclusion or exclusion of hazards from the generic list. When probability or frequency of occurrence is used as the basis for excluding a hazard by the DOE, in-depth review will be conducted to assess methodology, data, and evaluation process; an independent analysis may be performed by the NRC to evaluate the DOE basis and results. The PCSA Tool provides a capability to store in the project database the review results of each hazard to make a determination of DOE justification for inclusion or exclusion of potential initiating events.

4.1.1 Naturally Occurring and Human-Induced External Hazard Analysis

The DOE has developed a generic list of naturally occurring and human-induced external hazards that need to be considered for potential radiological release from the proposed repository during the preclosure period (CRWMS M&O, 1999a). Events in this list are based on the hazard evaluation techniques described in American Institute of Chemical Engineers (1992) and System Safety Society (1997). This identification of hazards uses the DOE Enhanced Design Alternative II (CRWMS M&O, 1999a). CRWMS M&O (1999a) provides the background information on each identified hazard necessary to assess if it has sufficient potential to become an initiating event during the assumed 100-year preclosure period.

The DOE has included in the generic hazard list 53 naturally occurring and human-induced events that may have a potential for initiating a radiological release during the preclosure period (CRWMS M&O, 1999b; DOE, 2000a). For each identified hazard, five evaluation criteria were applied by DOE in a consistent sequence to determine whether or not each hazard could be screened from further consideration. The natural events from the generic list were screened by the DOE for potential, for initiating events over a 100-year preclosure period, taking into consideration the following five factors:

(1) Potential exists for the initiating event to be applicable to the proposed repository site at Yucca Mountain. Additional and separate analyses may be needed to establish the potential.

(2) Rate of the physical process of the hazard is sufficiently high to affect the potential repository during the 100-year operational period.

(3) Consequence of the initiating event is sufficiently high to affect the potential repository during the 100-year operational period.

(4) Initiating event annual frequency is greater than or equal to 10^{-6} per year.

(5) Initiating event is not bounded by analysis of another event.

If all these screening criteria are determined to be true for any naturally occurring and human-induced external event, the event is considered to be credible for the proposed repository. If any statement or screening criterion cannot be evaluated appropriately at this time because of lack of specific information, the outcome of the screening criterion is assumed to be true. Recently, the DOE has excluded the last screening criterion (Bechtel SAIC Company, LLC, 2002).

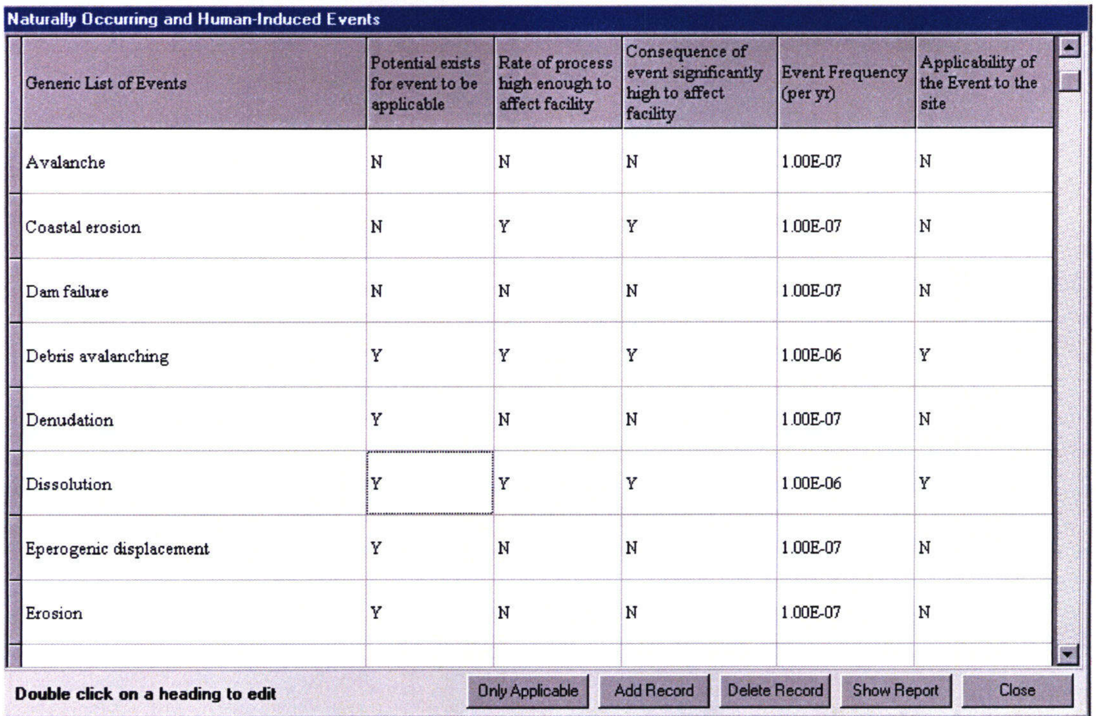
The complete list of natural and human-induced hazards considered by DOE, including its assessment of each hazard, is shown in Table 2-1 (Dasgupta, et al., 2002). As a result of the above screening process and bounding analyses, DOE reduced the potential list of natural hazards to the proposed repository during the preclosure period to only 12 events: (i) debris avalanche; (ii) extreme wind including sandstorms; (iii) flooding including rainstorm and river diversion; (iv) landslide; (v) lightning; (vi) seismic activity, earthquake; (vii) seismic activity, surface fault displacement; (viii) seismic activity, subsurface fault displacement including subsidence; (ix) tornado winds and tornado missiles,(x) industrial activity, (xi) loss of offsite power, and (xii) military activity. DOE further grouped these hazards and generated a list of six hazards that are credible initiating events and have the potential for dose consequences (DOE, 2001a). The six hazards identified are (i) loss of offsite power; (ii) seismic activity, earthquake; (iii) seismic activity, subsurface fault displacement, (iv) flood; (v) tornado missiles; and (vi) tornado wind. DOE plans to take a deterministic approach following NRC licensing precedence for nuclear power plants to design the structures, systems, and components important to safety to withstand these potential hazards (DOE, 2001a). The DOE strategy is to prevent release scenarios and loss of containment or confinement of radiological material resulting from credible initiating events. Bechtel SAIC Company, LLC (2002) described approaches to identify structures, systems, and components required to withstand the naturally occurring and human-induced hazards that have been determined to be credible and also describes methods to develop controls to prevent radiological releases if the initiating event occurs. Methodologies and analyses for these approaches would vary with characteristics of the hazards. In future versions, the PCSA tool will have the capability to review the analyses particularly for the seismic event.

4.1.2 PCSA Tool Function For Naturally Occurring and Human Induced External Hazards Analysis

The DOE would produce justification and analyses for including or excluding naturally occurring and human-induced hazards, including their occurrence frequencies, that may potentially initiate events and cause release of radiological dose to the public and workers. DOE analyses will be reviewed, and, if required, independent detailed analyses will be made outside the PCSA tool. The module in the tool will record the results of the staff review and identify the site-specific events that may initiate event sequences in the facility.

The PCSA Tool provides a list of naturally occurring and human-induced external hazards and a summary of in-depth review of each hazard. The tool database includes a list of 53 initiating events based on the DOE generic list of hazards. The staff will review the list with respect to NRC and other guidelines for other nuclear-related facilities (NRC, 2002b, Dasgupta et al., 2002) and new hazards can be added to the tool database. The tool also provides means to store detailed information on each hazard in the database. Information includes the detailed input used in the screening process by the DOE and the option to include detailed information on the review process along with the conclusion(s). Frequency of all credible events estimated by the DOE and the NRC reviewer will be stored in the database.

The External Events on the PCSA Tool main menu bar contain a submenu, Generic List, that leads to a form with tables containing a generic list of naturally occurring and human-induced external events, as shown in Figure 4-1. The table shows the four categories of screening processes: potential exists for event to be applicable; rate of process high enough to affect



Naturally Occurring and Human-Induced Events

Generic List of Events	Potential exists for event to be applicable	Rate of process high enough to affect facility	Consequence of event significantly high to affect facility	Event Frequency (per yr)	Applicability of the Event to the site
Avalanche	N	N	N	1.00E-07	N
Coastal erosion	N	Y	Y	1.00E-07	N
Dam failure	N	N	N	1.00E-07	N
Debris avalanching	Y	Y	Y	1.00E-06	Y
Denudation	Y	N	N	1.00E-07	N
Dissolution	Y	Y	Y	1.00E-06	Y
Eperogenic displacement	Y	N	N	1.00E-07	N
Erosion	Y	N	N	1.00E-07	N

Figure 4-1. Site-Specific Hazard Analysis Database

facility; consequence of an event significantly high to affect facility; and event frequency. Applicability of an event to the repository is indicated by "Yes" while "No" indicates a negative outcome. An event is considered applicable when all the screening criteria are determined to be true (Y) and the frequency of occurrence is more that 10^{-6}. The frequency limit is based on the definition of Category 2 event sequence in 10 CFR 63.2 assuming preclosure period to be 100 years for high-temperature repository operating mode (DOE, 2001a). For seismic activity, mean annual probabilities are used as the reference values in determining cutoff frequencies. For seismic activity related to earthquakes, the reference value of frequency is 10^{-4}, and for seismic activity related to surface and subsurface faulting, the reference value of frequency is 10^{-5} (CRWMS M&O,1999a). These values are considered appropriate based on the seismic topical report (DOE, 1997), which has been tentatively approved by NRC.

Data in each screening criterion and frequency grid come from review of each hazard conducted individually in their respective forms, while data in the applicability grid are automatically updated based on the screening criteria. The Hazards List form has Only Applicable, Add Record, Delete Record, Show Report and Close buttons as shown in Figure 4-1. The Only Applicable button shows the list of credible hazards based on the screening process, the Add Record button will allow to add an event to the generic list, the Delete Record will delete the selected event from the table, Show Report will display a report showing the information in the hazards' list, and the Close button will exit the form.

The event screening process is based on an in-depth review of DOE reports. The outcome of the review for each category can be stored in the database by double-clicking on the event. The double-click will launch a form, as shown in Figure 4-2. The form provided in the dialog

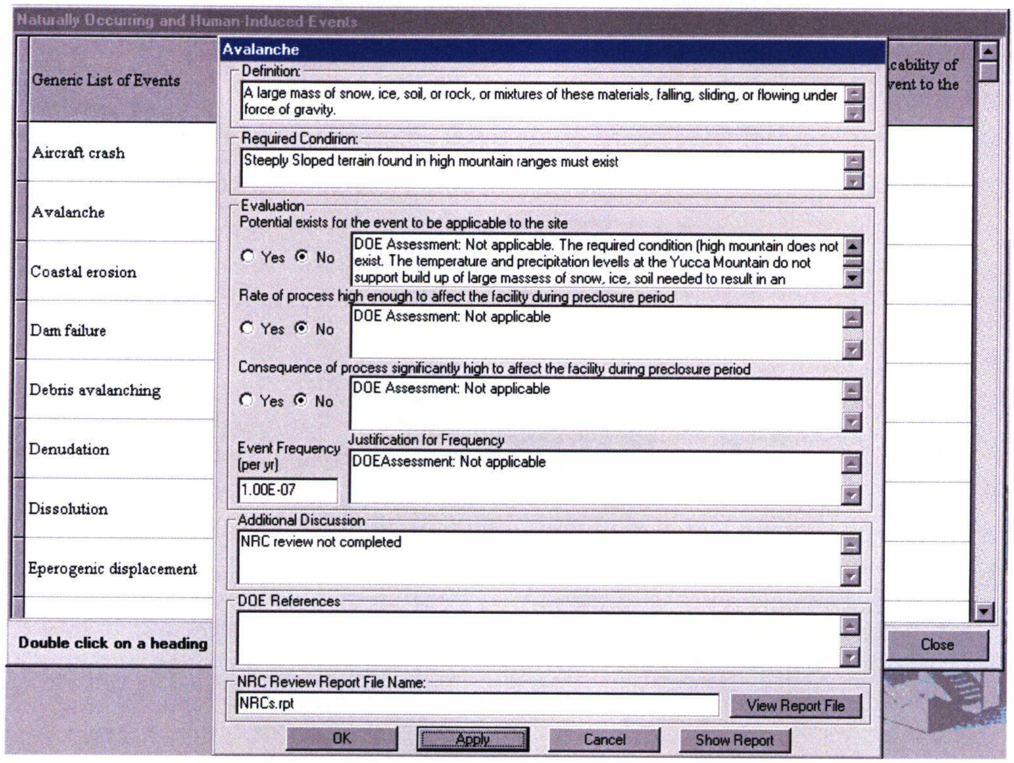


Figure 4-2. Form to Store Staff Review Results for a Particular Site-Specific Hazard

box will allow the reviewer to provide comments on the DOE definition of events, required condition for the events, and on each screening category including reviewers' evaluation of frequency of occurrence. The acceptance of the DOE demonstration is indicated by clicking the Yes or the No button provided next to it which updates corresponding criteria in the generic hazard's list. Furthermore, the events form has Additional Discussion and DOE References text fields for storing more information. If there is an independent report generated from the review, the report file can also be linked to the database by providing the name and path of the directory structure. Show Report buttons in the forms will generate reports on the contents in the form. The Apply button will store the data in the database and the Cancel button will not update the information in the form to the database.

The DOE is considering several options for a lower repository temperatures, which may extend the preclosure period to 325 years (DOE, 2001a). As a result of a longer preclosure period, the frequency limit in the fourth screening criterion, which is based on a 100-year preclosure period, would not be justified for some natural and human-induced initiating events (e.g., seismicity and rockfall) that have the potential to release radioactivity from the subsurface facility during the emplacement period. The preclosure period of 100 years has been hard-coded into the PCSA Tool. In future versions, the tool will provide flexibility to consider a different preclosure periods for each hazard.

4.2 Hazards from Facility Operations

The hazards and initiating events associated with the facility operations that may lead to radiological consequences to the public, or the workers, are identified through operational hazard analysis. Operational hazards result from equipment failure, human error, or a combination of both during the surface and subsurface operations. In addition, operational events may result from the failure of software and electronic hardware that may be used in the repository facility for waste handling and emplacement. The facility would be designed to handle approximately 70,000 MTU of nuclear waste during the preclosure period. During this period, the facility would receive commercial spent nuclear fuel, commercial high-level waste, defense high-level waste, and DOE spent nuclear fuel with the peak annual rate of receipt of approximately 3,000 MTU of nuclear waste (CRWMS M&O, 1999d). The waste would undergo several handling operations before it is placed underground. The peak annual handling schedule of casks, canisters, fuel assemblies, and disposal containers/waste packages indicates that a substantial number of handling operations would take place (Table 4-1). Although the annual operations would vary, the peak annual handling rate would be used in the safety analysis as required by 10 CFR 63.21(c)(5).

The PCSA Tool implements guidance and corresponding acceptance criteria in NRC (2002a) to review the operational hazards. Consistent with relevant sections of the acceptance criteria, the review would verify:

- The DOE hazard analysis is supported by adequate information on facility operations and structures, systems and components, and equipment

- Identification of hazards encompasses all modes of operations

- Use of appropriate bases and justifications for determining frequency or probability estimates considering associated uncertainties

- Adequate identification of human errors through human reliability analysis, and

- Adequate basis for inclusion and exclusion of hazards

For the comprehensive identification of hazards and an independent confirmation of the DOE list of operational hazards, the PCSA Tool currently uses four hazard analysis techniques (i) Failure Modes and Effects Analysis, (ii) What-If Analysis, (iii) Energy Method, and (iv) Human Reliability Analysis. Failure modes and effects analysis would evaluate ways facility hardware (e.g., equipment and components) in each system can fail, and the effect of those failures on potential release of radioactive material is assessed. What-If analysis examines the process or operational activities to identify radiological safety issues. Based on the DOE hazard analysis methodology, the energy method identifies energy (e.g., kinetic, pressure, thermal, electrical, etc.) in the system that can interact with the waste and potentially cause radiological consequence. A human reliability analysis will systematically evaluate performance of operators, maintenance staff, technicians, and other facility personnel to identify possible errors that can lead to events and result in radiological consequences. The hazard analysis techniques may not initially distinguish between different kinds of hazards and analyze all kinds of hazards (e.g., chemical safety, radiological safety, and personnel safety); however, hazards

Table 4-1. Total and Peak Annual Receipt Handling Schedule*			
	Handling Area	**Total for 24-year Operational Period**	**Peak Annual**
Cask	Canister Transfer	2,866	187
	Assembly Transfer	9,604	551
Canister	Canister Transfer	12,022	801
	Assembly Transfer	3,493	411
Fuel Assembly	Assembly Transfer	219,144	12,250
Disposal Container/Waste Package	Disposal Handling and Underground Emplacement	10,213	524
*CRWMS M&O. "Repository Surface Design Engineering Files Report." BCB–000000–01717–5705–0009. Revision 03. Las Vegas, Nevada: CRWMS M&O. 1999.			

related to radiological safety would be considered for further analysis through the severe events list. The DOE performed a hazard analysis to identify internal hazards and generated a preliminary list of events associated with the preclosure operations. Staff review of the DOE operational hazard analysis is discussed by Dasgupta, et al. (2002). This section discusses the application of the PCSA Tool and describes the approach and the methodologies used to review and identify facility hazards.

4.2.1 Hazard Evaluation Techniques

Operational hazard analysis is invoked in the tool from the main menu bar under the Internal Events menu. A functional area must be selected from the Project Tree menu to activate the analysis. A systematic analysis of the operational hazards internal to the facilities requires (i) description of the surface and subsurface facility; (ii) facility design information; (iii) description of the systems and repository operations; (iv) description of structures, systems, and components; and (v) human actions. The basic input to the hazard analysis is obtained from the System menu in the main menu bar of the tool as described in Section 3.3.2.

4.2.1.1 Failure Mode and Effects Analysis

The failure modes and effects analysis technique is a systematic approach intended to recognize and evaluate the potential failure of a process and its effects (American Institute of Chemical Engineering, 1992). Further, the failure modes and effects analysis can identify actions that could eliminate or reduce the chance of the potential failure. In a design application, such as in the case of the Yucca Mountain repository project, the failure modes and effects analysis technique is used primarily to assure that potential failure modes and their associated causes/mechanisms have been considered and addressed to the extent necessary.

The purpose of the failure modes and effects analysis is to identify the failure modes of the structures, systems, and components and the potential effect of each failure mode in the facility. This technique is universally applicable to the systems, subsystems, components, procedures, and interfaces. The method uses deductive logic to evaluate a system or process for safety hazards and ultimately to assess risk (System Safety Society, 1997). This method is an extremely detailed approach in which a design is reviewed, component by component, to determine failure modes of the components and their effect on a system or process. For a specific functional area of the facility or process, the method is used to identify specific failure modes, possible causes, and immediate effects. The failure mode describes how the equipment or hardware fails. The effect of the failure mode is determined by the system response to the equipment failure. The method then identifies each potential failure according to its severity. The failure modes and effects analysis procedure contains three steps: (i) defining the problem, (ii) performing the review, and (iii) documenting the results.

A standard failure modes and effects analysis format allows analysis in a systematic manner, reduces the possibility of omission, and enhances the completeness of the failure modes and effects analysis. The standard failure modes and effects analysis format was used in the tool, with minor modification, to help ensure a thorough and efficient review. The failure modes and effects analysis has been designed to be a living document to carry forward the analysis from construction authorization to the receive and possess waste stage. The failure modes and effects analysis will accommodate changes in the design, which will be more detailed at the receive and possess waste stage compared to the preliminary design at the construction authorization stage.

PCSA Tool Function for Failure Modes and Effects Analysis: The Failure Modes and Effects Analysis feature can be used only when a functional area is selected from the Project Tree menu. Under the Internal Events Analysis menu, the Failure Modes and Effects Analysis is a submenu that leads to Form, Table, and Severe Events submenus. Upon selecting the Form or Table submenu, the tool brings up a Failure Modes and Effects Analysis Form or Failure Modes and Effects Analysis Table dialog box showing form view or table view respectively. The Failure Modes and Effects Analysis Form has been designed for easy data entry during hazard analysis, component by component, and stores data into a database. Equipment and components used in the functional area are documented in System Description. The data can also be entered using the Failure Modes and Effects Analysis Table and the user can use both forms interchangeably. As shown in Figure 4-3, fields available in a Failure Modes and Effects Analysis Form are Item No., Component Description, Failure Mode, Causes of Failure, Effect of Failure, Recommended Safeguards and Controls, DOE Failure Detection, Additional Information, and Severe Events. At the top, the form also displays information related to the functional area being analyzed. The Failure Modes and Effects Analysis Form fills only one row of a record in a Failure Modes and Effects Analysis Table. The button controls at the bottom of the form are Add Record, Delete Record, Show Report, Failure Modes and Effects Analysis Table, and Close. The tool allows data to be entered using the Add Record button. There is no restriction on the amount of information that can be stored in each text file. At the end of the data entry, the Update Record button would save data into the database while the Cancel button would quit the form without saving. The Edit Record button would enable editing all the fields in the form and the edit changes can be saved with Update Record; clicking the Cancel button will not save any edit changes. The Failure Modes and Effects Analysis Table button will directly access the Failure Modes and Effects Analysis Table form and the Close button will end the session in failure modes and effects analysis.

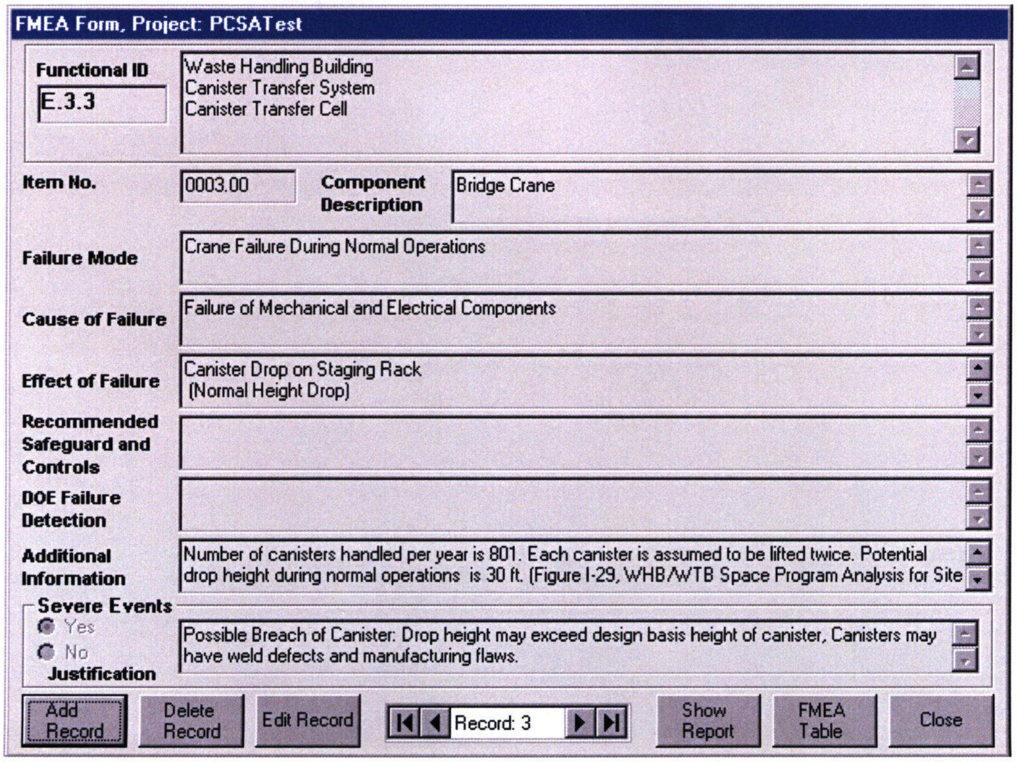


Figure 4-3. Example of Failure Modes and Effects Method Form

The Failure Modes and Effects Analysis Table dialog box, which displays data in a tabular format, functions through Add Record, Edit Record, Copy Record, Delete Record, Show Report, and Close buttons. The Failure Modes and Effects Analysis Form button takes the user to the Failure Modes and Effects Analysis Form dialog box. The Add Record button will add a row at the end of the current record or insert a row where needed. The Add Record button displays a dialog box showing an item number for adding a record at the end of the current item number. Rows can be inserted between records by incrementing item numbers in decimals. For

example, to insert a row between row 3 and 4, the item number may be specified as 3.5. Data can be entered or edited by double-clicking on the cell or using, the Edit Record button. The Copy Record button copies the entire row to a desired location specified through the item number. Additional edit features can be accessed by right-clicking with the mouse. The edit record and add record features allow modifications of the Failure Modes and Effects Analysis Table to document changes in the design of the facility. Furthermore, these features will help to maintain the continuity of the DOE safety analysis for license application for the construction authorization stage, the receive and possess waste stage, and future safety analyses during operations until permanent closure, as necessary. The Show Report button can be used to generate a report on failure modes and effects analysis for display and print. The Failure Modes and Effects Analysis Table form view for functional area E.3.3 is shown in Figure 4-4.

Each potential failure that may result in a radioactive dose to the public or workers is judged according to severity, on a qualitative basis, and entered as Yes or No in the Severe Event field. The User will have to enter the rationale in the Justification box for selecting the Yes or

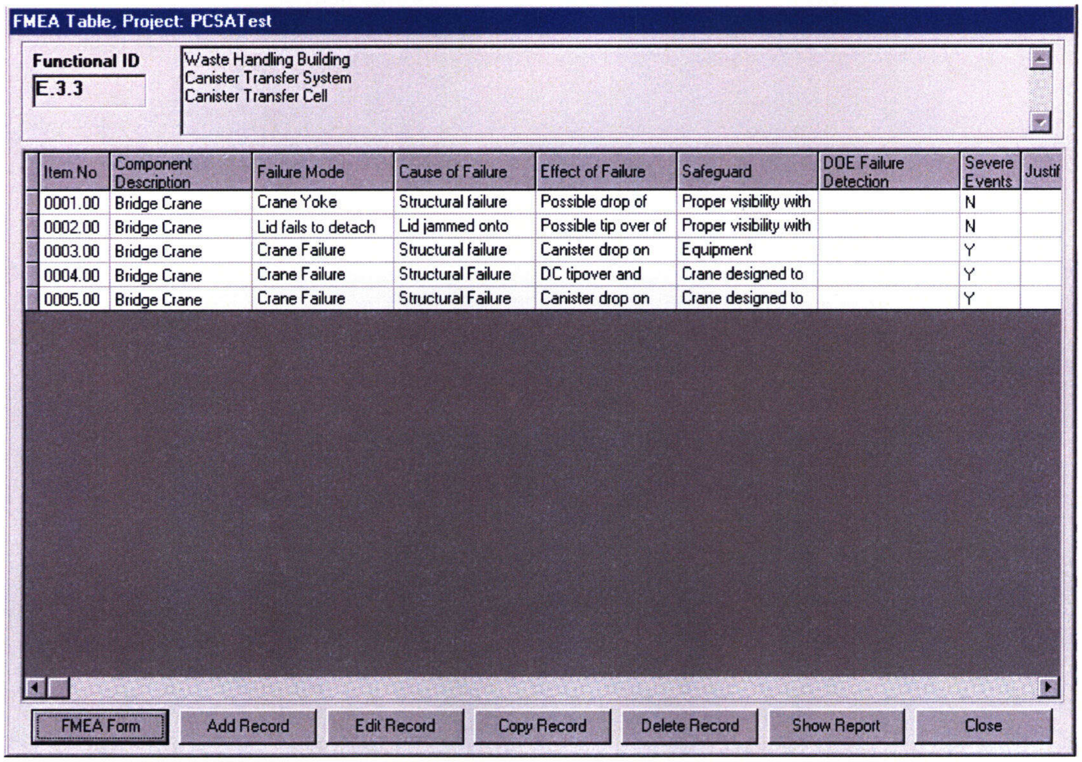


Figure 4-4. Example of Failure Modes and Effects Method Table

the No button. If the decision is based on certain calculations, the user can record this in the Justification box. The severity will be influenced by the safety features and controls incorporated by the DOE in their design. The failure modes and effects analysis also allows recording the safeguards and controls claimed by the DOE for eliminating a severe event. This feature will be useful in ensuring that the DOE implements the controls in their design if they are authorized to receive and possess waste. The Failure Modes and Effects Analysis Form also includes a recommended safeguards and controls text field, which serves as a checklist for comparison with the safeguards and controls proposed by the DOE. This column will be useful if the staff choose to perform an independent failure modes and effects analysis on selected critical areas of the process.

A database on component failures has been developed to assist in a failure modes and effects analysis. The Component Failure Mode Checklist menu under Checklist in the main menu bar provides a list of possible failures for components and equipment.

The next step in the preclosure safety analysis is to identify the initiating events. The events judged severe in the failure modes and effects analysis are candidates for initiating an event sequence. Thus, initiating events can be identified by screening the severe events postulated in the failure modes and effects analysis. When the Severe Events List menu is selected from the Failure Modes and Effects Analysis menu, a table form view is displayed containing the events filtered by Yes in the Severe Events field in the Failure Modes and Effects Analysis Table. The table displays Failure Mode, Cause of Failure, Effects of Failure and Justification from the Failure Modes and Effects Analysis Table, and Remarks. There is an Edit Record button control that allows editing only the Remark column to help record additional information. The tool also generates a report on the severe events list.

4.2.1.2 What-If Analysis

The purpose of what-if analysis methodology is to identify hazards, hazardous situations, or specific events that could produce an undesirable consequence (American Institute of Chemical Engineers, 1992). In the what-if analysis technique, a diverse team of experts is used to brainstorm and examine in detail each step in the process to identify potential hazards and ensure that appropriate safeguards against performance problems are in place. Questions (What if a specific component failure, or process upset, or human error, or external event occurs?) are posed with regard to each of the operations sequence steps described in the preceding discussion. Through this questioning process, the possible accident situations, consequences, and existing safeguards are identified.

The what-if analysis technique will generate a list of questions and answers about the process and the procedures. The result will be a tabular listing of hazardous situations, their consequences and safeguards, and possible action items to reduce hazards. Hazards postulated to be severe will be further analyzed for scenario development and event grouping for event sequence analysis. The what-if analysis will be applied in the cask-handling area, where human interactions in the operations are more involved.

PCSA Tool Function for What-If Analysis: The tool functions for a what-if analysis are similar to the failure modes and effects analysis. The analysis is performed by entering data into the database through a form or table. Fields available in the form are Item No., What-If, Causes, Consequences, DOE Safeguards, and Action Items. What-If analysis would identify potential initiating events from human interactions. In present version of the tool does not offer any process to filter the potential severe events that are candidates for initiating events. A process similar to what is used in failure modes and effects analysis is used to filter the severe events. An example of what-if analysis applied to the off-site transportation system in functional area B.1 is presented in Figure 4-5.

4.2.1.3 Energy Method

The energy method used in the tool is adopted from the DOE internal events analysis technique (CRWMS M&O, 1999b; DOE, 2001a). The DOE hazard analysis methodology is based on a composite of three hazard evaluation techniques, energy method, energy trace and barrier analysis, and energy trace checklist as described in System Safety Society (1997). These techniques are applied to all systems that contain, make use of, or store any forms of energy (e.g., potential or kinetic mechanical, electrical, chemical, thermal, and such). All three methods evaluate hazards based on identifying the source of energy and nature of energy flow in a system by using a checklist type of evaluation process. The DOE checklist has been customized for application to the repository from generic checklists provided in the three approaches. While the methods selected by the DOE for identification of hazards and initiating events based on energy method, are consistent with acceptable industry practice, the failure modes and effects analysis and what-if analysis are widely used techniques in the industry and allow more systematic and comprehensive hazards analysis. The energy method technique has been introduced in the tool for convenience to review the DOE identification of hazards.

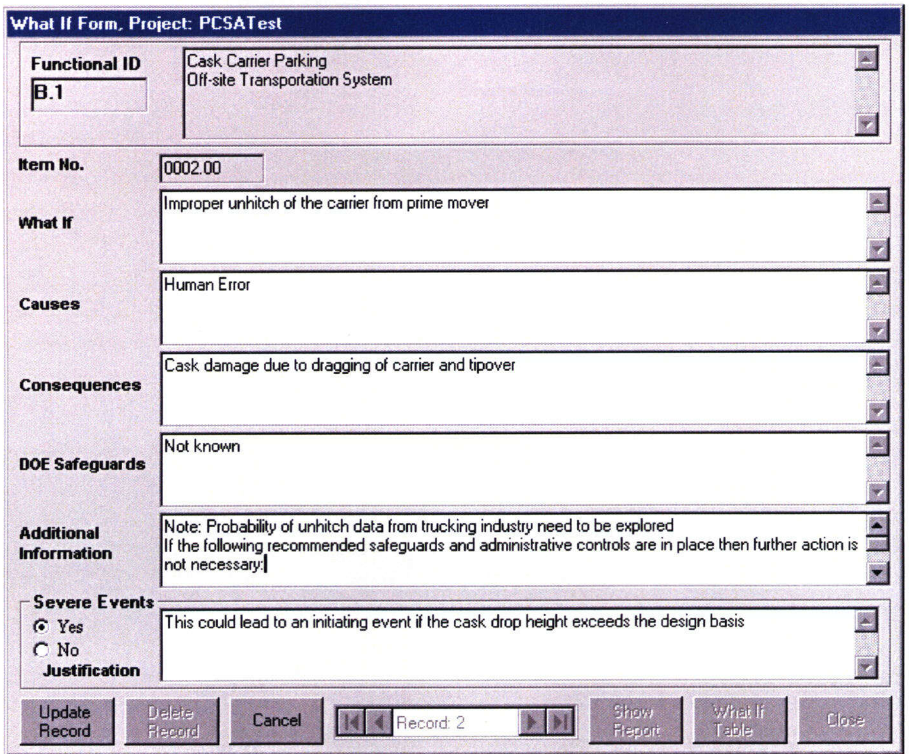


Figure 4-5. Example of an What-If Analysis Form

PCSA Tool Function for Energy Method: A functional area must be selected for the energy method. Located under the Internal Hazard Analysis menu from the main menu bar, the energy method is initiated by selecting either the Energy Method Form or Energy Method Table submenus. The data can be introduced in the database using the Energy Method Form. The Energy Method Form allows using the checklists to identify the hazards in the system. Adopting the DOE approach, the events have been categorized as collision/crushing, chemical contamination/flooding, explosion/implosion, fire, radiation/magnetic/electrical/fissile, and thermal. Upon selecting a category from the drop-down menu in the form, the checklist and the applicability guidelines appear. The checklist helps to identify the energy in the system that can potentially interact with the waste form. The checklists developed by the DOE contain a series of questions for each generic hazard. The applicability of the hazard to the functional area is determined by a positive response to all questions. The data can be stored by Add Record/Update Record button controls. Other button controls are Delete Record, Show Report, Energy Method Table/Energy Method Form, Copy, and Close. The Energy Method Table allows the user to view the entries in a tabular form and edit the entry in cell. An example of the Energy Method Form is shown in Figure 4-6.

4.2.1.4 Human Reliability Analysis

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

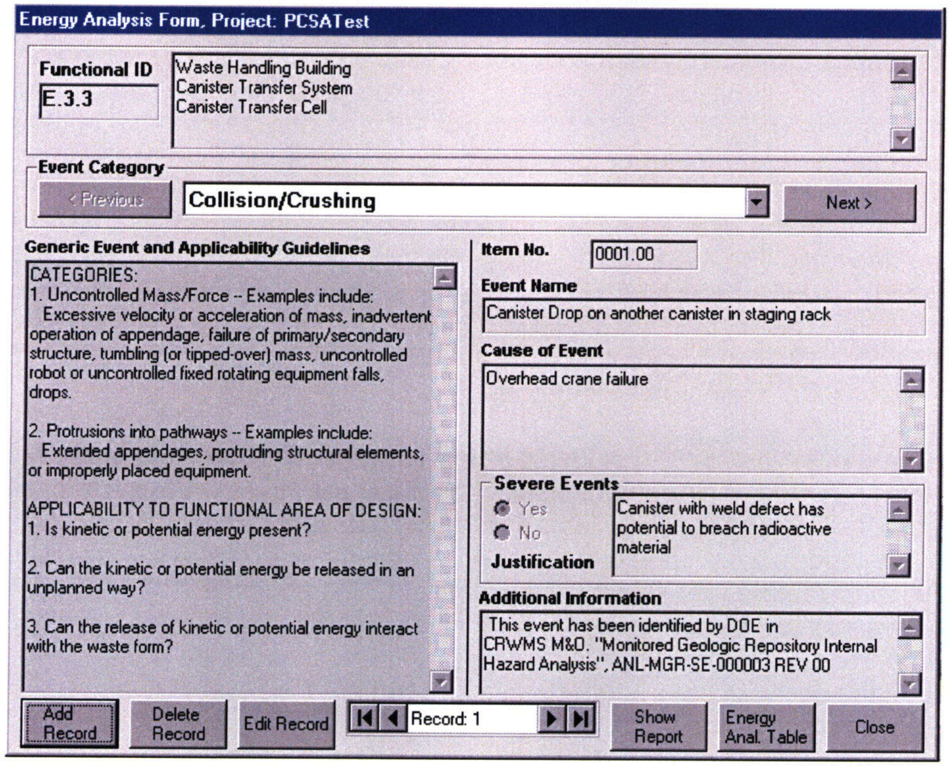


Figure 4-6. Example of an Energy Method Form

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. Eisenberg (2001a) provides a discussion of human reliability analysis in the context of repository preclosure safety analysis.

4.2.1.4.1 Human Reliability Analysis Methods

Human reliability analysis methodologies are complex assemblages of models, databases, techniques, and approaches. Listings and characterization of various methodologies may be found in several sources (Eisenberg, 2001a; Hollnagel, 1993; Smith, 1997; Swain and Guttman, 1983). 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 (NRC, 1994):

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

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

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. The PCSA Tool provides a capability to analyze Type 1 human errors.

4.2.1.4.2 Human Reliability Analysis Process

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).

A general approach for human reliability analysis originally developed for nuclear power plants operations (Swain and Guttman, 1983) would be applicable to any nuclear facility, including the preclosure operations of the repository (Eisenberg, 2001a). 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 (including, e.g., Technique for Human Error Rate Prediction) estimate these human error rates using a two-step process:

(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

4.2.1.4.3 Technique for Human Error Rate Prediction

The Technique for Human Error Rate Prediction was developed by Swain and Guttman (1983) for Sandia National Laboratories. This methodology has been broadly used for nuclear facilities. The 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:

(1) Define system (or subsystem) failure

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

(3) Predict error rates for each relevant human operation

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

(5) 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, using a human reliability event tree, is required. Although the **T**echnique for **H**uman **E**rror **R**ate **P**rediction methodology will form the basis for implementing a quantitative treatment of human reliability in the PCSA Tool, this has not been implemented at this time.

4.2.1.4.4 Human Reliability Analysis in the PCSA Tool

4.2.1.4.4.1 Objective

The goals of the qualitative Human Reliability Analysis are:

(1) To describe the human activities and sequence of actions in preclosure repository operations

(2) To identify the human errors that might occur in these activities

(3) To estimate the consequences of the various human errors, so those associated with a severe event may be flagged

(4) To provide other information associated with each activity that may be useful or provide input to the quantitative analysis

Like the other qualitative approaches in the PCSA Tool, the Human Reliability Analysis will consist of a data base, with well-defined data categories for each record and an approach for systematically performing the analysis by entering the data for each record.

4.2.1.4.4.2 Description of Human Activities and Sequence of Actions

The description of human activities and sequence of actions in preclosure repository operations forms the basis for the human reliability component of the PCSA Tool. The natural place to describe and document these activities and actions is within the System Description form accessed from the System menu, from the main menu of the PCSA Tool. The System Description is keyed to the Project Tree, which breaks the repository up into functional areas. The System Description describes a sequence of operations and human actions for the lowest level of functional area.

Since the Functions and Detailed Operations Sequence fields in the System Description Form (Figure 3-21) provide a good analytical basis from which the human operations may be designated, this is a logical location for the placement of the description of human activities and actions. The Detailed Operations Sequence will list the various operations performed by the particular functional area being analyzed; the Human Actions field will provide the specific human actions required to achieve the overall operations. In a sense, the Human Actions field parallels the Equipment Used field, except the former is associated with the human components in the system, while the latter is associated with the mechanical components. Both fields are generated by the analyst, who reviews the Detailed Operations Sequence and, based on those descriptions, identifies the hardware components and human actions required to accomplish the operational goal of the functional area. By placing this field in this location, integration of human actions and hardware functions will be facilitated; as the analyst thinks through the sequence of operations, the flow of work and reliance, alternatively, on human or machine, should become apparent.

As always, the analyst would need to decide on a level of detail and try to maintain the same level of detail throughout. For example, one human action might be "operate the crane to lift an assembly from a cask to the storage pool." This action could be further subdivided to include (i) check to assure the grapple is attached; (ii) initiate lift; (iii) terminate lift; (iv) advance horizontally; (v) check on position above storage pool; (vi) initiate descent; (vii) terminate descent; and (viii) release assembly. The analyst would need to choose a different level of analysis, depending on the a number of factors (i) the amount of detail about operations available or assumable, (ii) the corresponding level of detail in the hardware analysis, (iii) the purpose of the analysis, and (iv) the importance of the human operations analyzed.

4.2.1.4.4.3 Classification of Human Error

Classification of human error is a desirable part of the qualitative analysis, because it provides an indicator of (i) the role the particular type of human error will play in overall system performance, (ii) the analytical approach for treating the human error, and (iii) the appropriate type of data to use if the human error is quantified. The PCSA Tool adopts the following classification scheme for human activities, adapted from Nuclear Energy Agency (1998). This classification scheme is based on the timing of various human actions relative to the timing of upset events:

(1) Normal operation, which includes maintenance and testing

(2) Initiation of abnormal scenarios

(3) Response of the plant and human operators in the abnormal scenarios.

The classification categories are:

- **Category A:** Human actions occurring prior to an initiating event.

- **Category B:** Human interactions that initiate a scenario, sometimes called human-induced initiators. These include the following subcategories:
  - Category B1. Human-induced initiators that lead to top events already defined by mechanical-failure initiators.
  - Category B2. Human-induced initiators that lead to top events not previously defined by mechanical-failure initiators.

- **Category C:** Human actions taken after the initiating event. Subcategories include:
  - Category C1. Human actions taken in response to an initiating event for which rules and procedures have been put in place.
  - Category C2. Human errors of commission that increase rather than mitigate the adverse effects of the initiating event.
  - Category C3. Improvised human actions intended to recover from an initiating event and repair any damage.

Category A errors are enabling errors that result in equipment in standby systems being unavailable to perform their function as required when a demand is made. Category B1 errors typically may be caused by either mechanical failure or human error; for example, an assembly drop from an excessive height could be produced by the failure of a limit switch on the lifting crane or it could be produced by the operator deactivating the limit circuit. Category B2 errors will typically be caused infrequently, if ever, by mechanical failure; for example, the operator could guide the lifted assembly into the side of the hot cell, a failure mode not previously defined by mechanical failure. Category C actions are made in response to the scenario, attempting to reach a safe state. These actions, sometimes called "dynamic operator actions," may be "rule-based" (Subcategory C1) or not (Subcategories C2 and C3).

It should be noted that, in the context of the previous discussion, the routine (pre-initiator) human errors are Categories A and B. Category C1 might also be regarded as a routine human error, however cognition is involved in recognizing that an off-normal event has occurred and determining that a particular rule-based procedure must be followed. However, Categories C2 and C3 are clearly cognitive-based human error (post-initiator or dynamic human errors). Given the current scope for improvements to the PCSA Tool, none of the Category C human errors are planned for implementation at this time. At the time that a quantitative capability for human reliability analysis is incorporated into the PCSA Tool, a judgement will be made regarding whether or not to incorporate the limited treatment of Category C1 events contained in the Technique for Human Error Rate Prediction methodology.

The Human Actions category is subdivided in System Description to reflect the essential difference between activities that lead to Category A and Category B human errors. That is, Category B human errors result from operational activities conducted to fulfill directly the mission of the facility; Category A human errors result from maintenance and other support activities, that could impair mission-direct activities, if errors are committed. Specification of

Category A activities for each functional area identified in the Project Tree may lead to a lot of duplication. However, specification of these activities for each functional area appears the best approach because: (1) the Human Reliability Analysis may not be performed for the entire repository, therefore this detail may only be required for selected functional areas and (2) the combination of maintenance activities in each functional area may be unique, so even if all such activities were described in a single list, selections for each functional area would need to be made.

4.2.1.4.4.4 PCSA Tool Functions for Human Reliability Analysis

The Human Reliability Analysis feature can only be used when a functional area is selected from the Project Tree menu. The Human Reliability Analysis menu, when selected from the Internal Events menu in the main menu bar of the PCSA Tool, leads to Form, Table, and Severe Events submenus. The Form submenu brings up the Human Reliability Analysis dialog box showing a form view (Figure 4-7) which is similar in appearance to the Failure Modes and Effects Analysis form (because, like the Failure Modes and Effects Analysis form, this form could be a precursor to an Human Reliability Analysis tree or a fault-tree or event-tree analysis). Fields in the Human Reliability Analysis form include the following:

(1) Functional ID and Functional Area Description

(2) Item Number

(3) Human Action. This would be one of the Human Actions now listed in the System Description template. It is a description of the human action that may lead to error.

(4) Human Failure Event. There may be several types of error possible for a single human action. For example, a task might be omitted, a valve might be turned in the wrong direction, or a valve might be turned too far in the right direction.

(5) Performance Shaping Factors. This field would be unique to the Human Reliability Analysis. In this field, the analyst would indicate any performance shaping factors that would influence the human error probability (e.g., training, stress level, use/no use of checklist, repetitiveness of action).

(6) Recovery Action. This field would be unique to the Human Reliability Analysis. In this field, the analyst would indicate what actions could be taken to recover from the error. For example, a supervisor checking after maintenance might discover and correct an inappropriately closed valve.

(7) Effect of Failure. For Type A Human Actions, the effect of failures is always enabling of some other initiating event; for Type B Human Actions, the effect of failures could be enabling, but is more likely to produce an initiating event itself. For example, actions during maintenance could close a valve that permits make-up water to be pumped into the assembly storage pool; in the event that a leak from the pool develops because of a mechanical failure, make-up water would not be available and the assemblies could become uncovered in time. As stated in the fiscal year 2001 Human Reliability Analysis report, another example would be failure of the operator to attach the cask gas purge

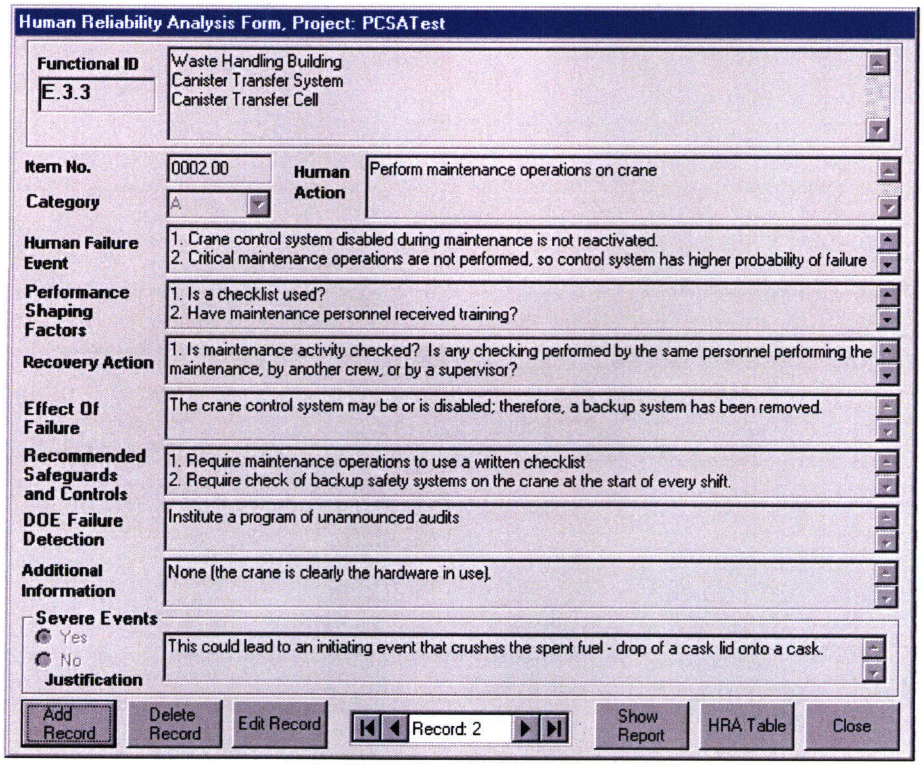


Figure 4-7. Example of a Human Reliability Analysis Form

line to the cask, thereby allowing radioactive cask gases to be released in the handling area.

(8) Recommended Safeguards and Controls. Safeguards and controls could be either human action oriented (e.g., use a checklist, provide written instructions) or hardware oriented (e.g., use interlocks or stops to prevent incorrect assembly or excessive travel, respectively).

(9) DOE Failure Detection. Failure detection for human failure events is likely to be human oriented (e.g., audits, inspections, TV monitors).

(10) Human Action Category. The appropriate human action category, see Section 4.2.1.4.4.3 is indicated. The main categories are: Type A- Maintenance and Standby Human Events; Type B—Operational Human Events (two subcategories); Type C—Responsive Human Events (three subcategories).

(11) Severe Events: Yes or No. In addition, the analysis must provide a justification for either choice.

(12) Additional Information.

4.2.1.4.5 DOE Approach to Human Reliability Analysis

DOE has articulated an approach to incorporating Human Reliability Analysis into the preclosure safety analysis, required for the license application. This approach is delineated in guidance for technical staff designing the repository and preparing the preclosure safety analysis (Bechtel SAIC Company, LLC, 2002). In particular, Section 7.3 of that document is devoted to Human Reliability Analysis.

The Human Reliability Process described by the DOE begins by using human reliability considerations in the development of event trees and fault trees that describe the safety of preclosure repository operations. The questions associated with the risk triplet (Kaplan and Garrick, 1981) are applied at any point in the development of an event tree or fault tree, where human interactions are known or are suspected to occur. As a structured approach to address these questions, the DOE has chosen the Systematic Human Action Reliability Procedure methodology.

As an aid to quantifying probabilities of human actions (i.e., human error) the DOE chooses to place human actions into three categories (Bechtel SAIC Company, LLC, 2002):

- Type A—human events that occur before an initiating event of an event sequence, typically during testing and maintenance.

- Type B—human events that are caused by, [sic] or contribute to an initiating event, typically errors of commission.

- Type C—human interactions that occur after an initiating event as part of the mitigation process; both errors of commission and errors of omission may occur.
  - Type CP—a subtype of human interactions that are governed by procedures, either formal or informal.
  - Type CR—a subtype of human interactions that relate to recoveries from unavailable equipment or prior human errors.

Note that these categories correspond roughly to those articulated by the Nuclear Energy Agency (1998) and adapted for use in the PCSA Tool (Section 4.2.1.4.4.3).

A six-step version of the Systematic Human Action Reliability Procedure methodology is designated as the framework for conducting human reliability analysis for the preclosure safety analysis (Bechtel SAIC Company, LLC, 2002):

- Identification and Logic Modeling
- Screening
- Task Analyses
- Representation and Models
- Quantification of Human Action Probabilities
- Quantification of the Event Tree or Fault Tree

Bechtel SAIC Company, LLC (2002) describes each of these steps in turn, with advice on how to execute each correctly. However, documentation for some portions of the guide is currently incomplete (e.g., Step 5). Although the DOE is advocating use of the Systematic Human Action

Reliability Procedure methodology, the guide repeatedly makes reference to the procedures, approaches, and especially data on human error probabilities that comprise the Technique for Human Error Rate Prediction methodology, adopted for use in the PCSA Tool.

4.3 Initiating Events

An initiating event is defined in 10 CFR 63.2 as a natural or human-induced event that causes an event sequence. In defining the overall scope of the preclosure safety analysis, 10 CFR 63.102 (f) requires initiating events to be considered for inclusion in the preclosure safety analysis through a systematic hazard evaluation. DOE demonstration of compliance with performance objectives of Category 1 and 2 events sequences would depend on identification of relevant initiating events and estimation of there frequencies. In addition, the DOE would need to take into account uncertainties in its approach to evaluate probabilities or frequencies for initiating events. The regulation does not specify cut-off probabilities for initiating events for exclusion, but recognizes certain initiating events may not be appropriate for inclusion in preclosure safety analysis for determining event sequences. The regulation further states in 10 CFR 63.102 (f) that the inclusion of initiating events should be based on the characteristics of geologic setting and human environment, and be consistent with precedents adopted for nuclear facilities with comparable or higher risks to workers and public.

The PCSA Tool provides the capability to review the DOE identification of initiating events by independently selecting the initiating events from (i) naturally occurring or human-induced external events identified through site-specific hazard analysis, or (ii) a failure of a component or equipment in a system or human actions during facility operations identified through facility hazard analysis. The tool further allows independent estimation of the frequencies of the initiating events considering uncertainties. The database on failure rate from actuarial data can be used to evaluate frequencies of component failure. In addition, fault tree analysis or human reliability tree analyses can also be used to evaluate initiating event frequency for a failure in a system or human action. The fault tree and human reliability tree are discussed in Chapter 6 of this report.

4.4 PCSA Tool Application for Initiating Events

This section discusses the process of including or excluding an initiating event. The initiating event can be accessed from the Initiating Event submenu located under Freq. Analysis in the main menu bar. The Initiating Event menu has two submenus, Form and Table, to enter data into the database. The Initiating Event menu can be used only when a functional area is selected from the Project Tree menu. The starting point of the selection of an initiating event is from the Severe Events list from the hazards analyses in the Internal Events menu. The severe event list contains identified hazards from qualitative hazard analyses using failure modes and effect analysis, what-if analysis, the energy method, and human reliability analysis that may result in radiological dose consequence to the public and workers. Each of the hazards in the severe event list is examined for a potential initiating event with the help of the Initiating Event Form. To identify initiating events, the user should include all the hazards in the severe event list. If review of DOE or other documents reveals other events, these also should be included in the process. Additionally, initiating events can be generated from naturally occurring and human-induced external events. Credible external events that have the potential to cause radiological consequences are obtained from the External Events menu using only the Applicable button.

The fields in the Initiating Event form are shown in Figure 4-8 and its functions are discussed below.

Functional ID: Provides identification number of the functional area along with the description of the functional area in which the analysis is being performed.

Item No.: Shows the serial number of the record in the database pertaining to the current form.

Initiating event ID: All initiating events considered in the process must have an identification number. The tool will not allow entry of additional data without an identification number. The identification number provides a link to event scenarios and event sequences and all other subsequent analyses conducted in the tool.

Description: Short description and nature of initiating event, whether operational, or natural, or human-induced.

Preclosure Period: Preclosure period associated with each initiating event. The default value is 100 years. User can use the drop down list to select the preclosure period or type it in.

Frequency: The frequency of the initiating event.

Category: The tool will evaluate frequency category of the initiating event based on the frequency category limits defined in 10 CFR Part 63.

Uncertainty: Consideration of uncertainty in estimation of the frequency and associated details are entered here.

Frequency Calculation Details: Detailed information on the frequency estimation, including all calculations, is recorded in this field. When the frequency calculator is used, the numbers used in calculating frequency are automatically transferred into this field.

Event Included for Sequence Analysis: The decision to exclude or include initiating events from the hazards list in preclosure safety analysis for determining event sequences is entered using the Yes or No button. The reason for inclusion or exclusion of initiating events for further preclosure safety analysis must be recorded in the Justification field.

Additional Information: Comments, remarks, references to reports, and literature citations should be recorded here.

The Initiating Event Form has Add Record, Delete Record, Edit Record, Show Report, Init Event Table, and Close buttons. The button functions are similar to the Failure Mode and Effects Analysis Form. In addition there is a Freq. Calculator button that launches a Frequency

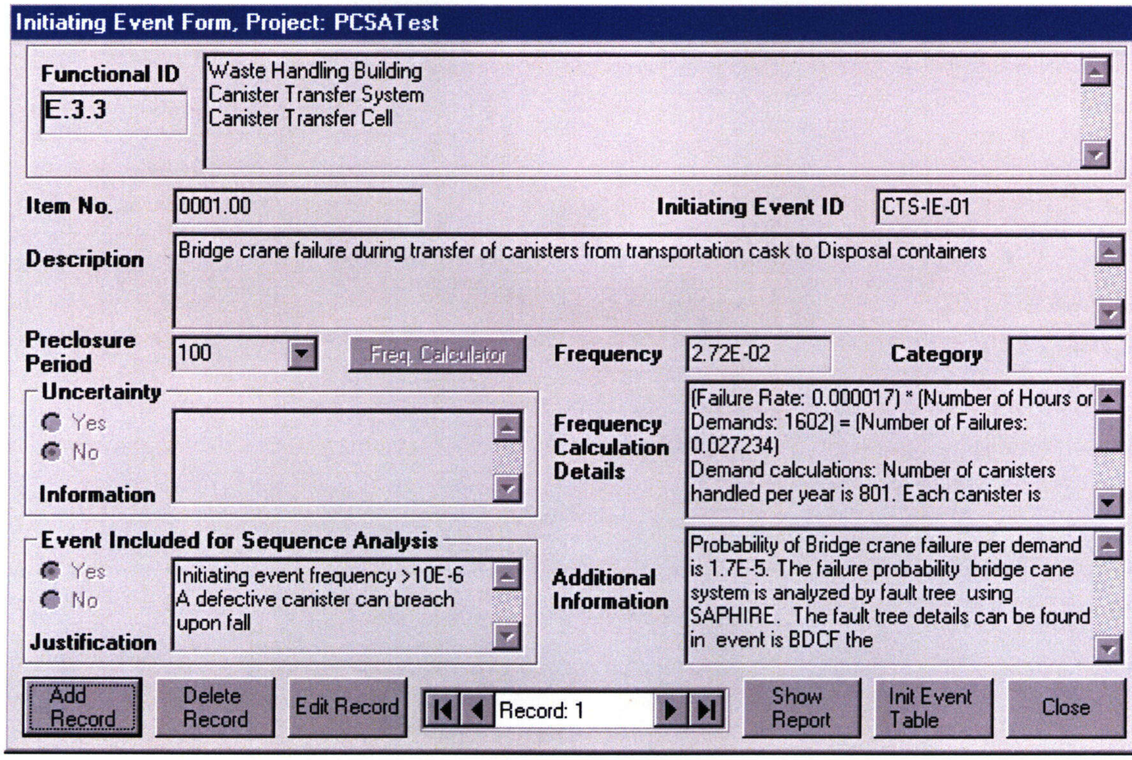


Figure 4-8. Initiating Event Form

Calculator form. The calculator has two data entry fields, one for failure rate and the other for number of hours or demands. The Calculate button will display the product of the two numbers. Upon closing the form, the frequency number automatically fills the Frequency field and, at the same time, details of the calculation are filled in automatically in the Frequency Calculation Details field, including the Frequency Calculations, shown in Figure 4-9.

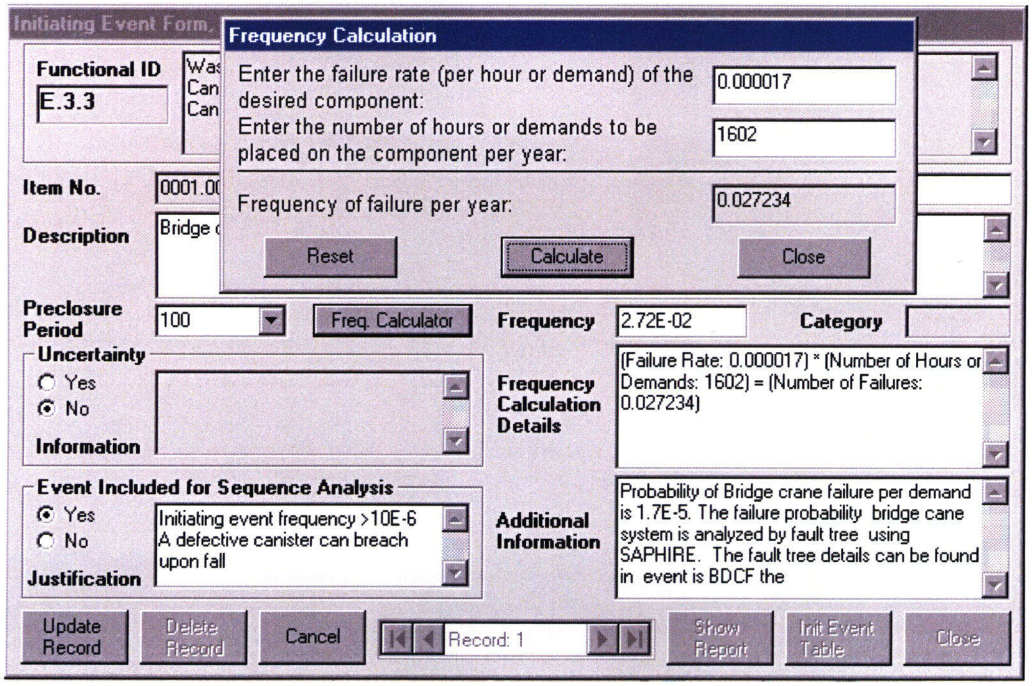


Figure 4-9. Initiating Event Form with Frequency Calculator

5 EQUIPMENT/SYSTEMS FAILURE-RATE DATABASE

The development of a database for failure rates of equipment and systems is discussed in this chapter. Frequency and probability data are required for the event tree and fault tree analyses for estimation of the frequencies of occurrence of event sequences. The probability of equipment/system failure for human-induced internal events is established from the failure rates of components and controls. The PCSA Tool provides a comprehensive failure rate database from actuarial data extracted from several sources. The database is controlled and it cannot be changed by the user. The database will be maintained and updated by Center for Nuclear Waste Regulatory Analyses (CNWRA).

The database contains failure-rate data on several categories of equipment and systems, including the systems and components to be used in the Yucca Mountain processes, such as process equipment (e.g., cranes, blowers, dryers and such), utility systems (e.g., power, heating ventilation and air conditioning system, and such), electrical equipment, instrumentation and control systems (e.g., controllers, computational modules, alarms, temperature, and pressure level measurement, and such), and miscellaneous equipment such as high-efficiency particulate air filters, casks, and such. The data have been obtained from published reports and include data from nuclear, chemical, and offshore industry sources. The database presently holds 181 different component categories and 3,251 records. Table 5-1 gives the overall size of the database in its current form. The database will be expanded to include failure-rate data on equipment, controls, and instruments that are identified as more design details become available.

Table 5-1. Present Database Statistics

Item No.	Description
1	3,251 Records
2	181 Component and Equipment Categories
3	37 Primary References
4	109 Secondary References

Because the database is intended as a quick resource for failure-rate information used primarily to check or compare against numbers used in the U.S. Department of Energy (DOE) analyses, it does not contain raw data. This report, therefore, does not include data analyses, such as uncertainty and sensitivity analyses. If raw data are needed for conducting independent statistical analyses, they can be found in the reports referenced in the database.

5.1 Organization of Data in the Database (Taxonomy)

A taxonomy, or system of classification (ordering) is employed to facilitate the location of data within the database. The taxonomy has been modeled after the taxonomy scheme used by the Center for Chemical Process Safety of the American Institute of Chemical Engineers (1989) for their Process Equipment Reliability Data. There are hierarchical levels within this taxonomy structure. The upper level includes 10 sections and broadly categorizes the equipment and systems by generic type. The lower levels further define the components of the equipment and, if chosen properly, can reduce the scatter of the failure-rate data. The number and nature of the levels vary with each data cell. The taxonomy levels for the Equipment/Systems Failure-Rate Database are graphically presented in their current form in Appendix A.

The taxonomy can be accessed via a tree display form. The tree consists of multiple nodes with subcategories consisting of the various levels of the taxonomy. Multiple categories can be viewed at once, and the user can switch groups with relative ease. After clicking on a category of data, all of the components within that category are displayed on the screen. A screen shot of the taxonomy tree is shown in Figure 5-1 on the left hand side. The taxonomy allows the user to traverse the many levels of the database with relative ease to locate a general category of components. Clicking on a category such as Crane and then on the Display Data button in the taxonomy tree box, will result in a display box where the failure-rate data for cranes are displayed.

Overall, the taxonomy provides a good starting point for organizing the database and is particularly helpful to an inexperienced user unfamiliar with the type of data they are looking for, or, simply, someone who wants to be able to choose between many different types of components or failure modes.

The failure rate database can also be accessed by first clicking on the Probability button in the main menu and then clicking on the Search Database option in the submenu. A screen shot of the Failure Rate Data Search form is shown in Figure 5-1 on the right-hand side. Data can be accessed by typing the component name and description in the Failure Rate Data Search form (e.g., Bridge and Crane). This will again result in the display box where the failure-rate data for cranes are displayed. In many cases, the search feature is found to be faster and more versatile.

5.2 Source of Database

The underlying reason for constructing the database is to provide the capability to draw data from a wide range of sources. To build the database, information was acquired from 37 reports, as shown in Table 5-1. These ranged from Nuclear Power Licensee Event Summaries to various reliability databases and reports. NUREG/CR–2300 (Hickman, et al., 1993), which outlines the procedure for developing a probabilistic risk assessment database for nuclear powerplants, was used as a model in constructing the PCSA Tool database. Many of the data sources referenced in this NUREG are used in the PCSA Tool as well.

Five example sources in compiling the data for the database in the PCSA Tool are discussed next. These represent a diverse cross section of sources used.

(1) <u>Reliability techniques used in the assessment of cranes (Duke, 1985)</u>

This report demonstrates the methods used in performing a reliability assessment on a crane and highlights some of the important factors that must be considered. It shows how the results of the assessment may be used to strengthen the design of a crane system. Tables in the report give component descriptions, failure modes, failure rates per year, and probability of failure per demand for each of 15 crane components.

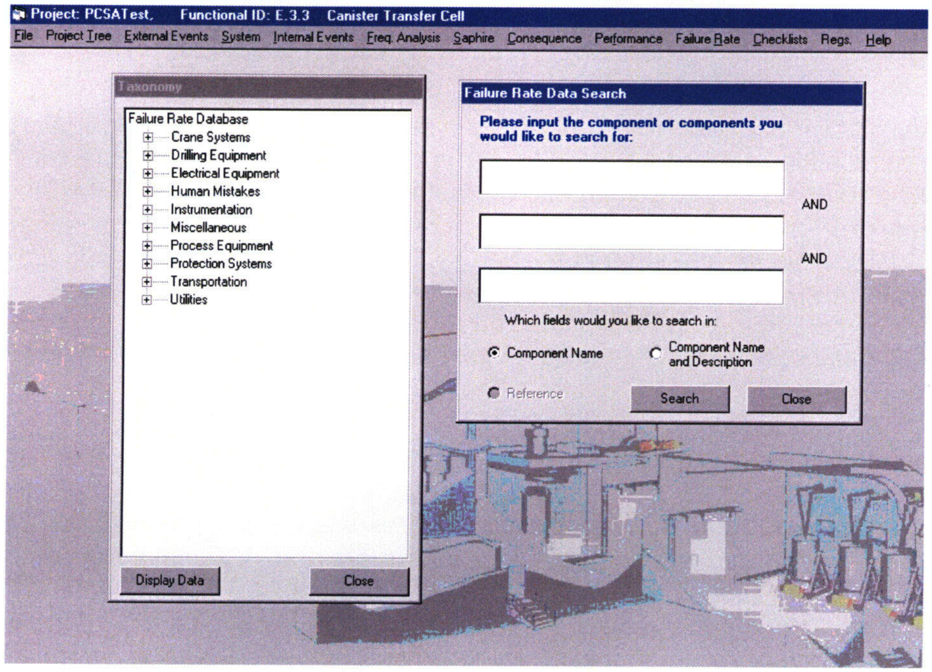


Figure 5-1. Taxonomy and Data Search Forms

(2) Component failure-rate data with potential applicability to a nuclear fuel reprocessing plant (Dexter and Perkins, 1982)

This compilation contains 1,223 pieces of component failure-rate data, under 136 subject categories, that have been compiled from published literature and computer searches of a number of databases. Component selections were based on potential applicability to facilities for reprocessing spent nuclear fuels. The report does not directly apply any statistical analysis; it simply lists the published values. Thus, the actual data and component descriptions are not as detailed as those in other references, such as the licensee event reports.

(3) Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants. NUREG/CR–1363 (Miller, et al., 1982):

This report describes the creation of a computer-based data file from Licensee Event Reports of valves in commercial nuclear power plants for the period January 1, 1976, through December 31, 1980. In addition to creation of the file, summaries of the data contained in the file are made to obtain data for risk assessment and statistical purposes. Gross constant failure rates are estimated for selected valve types in certain safety systems. The statistical analysis includes estimated information together with actual plant data. However, the plant data were not used in the PCSA Tool database, and only the statistical summaries found in the appendices were actually entered. This report updates and supersedes the original three-volume June 1980 printing of NUREG/CR–1363.

(4) Nuclear Plant Reliability Data System 1979 Annual Reports of Cumulative System and Component Reliability. NUREG/CR–1635. (Southwest Research Institute, 1980):

These Nuclear Plant Reliability Data System annual reports were designed to serve as a source of reliability and failure statistics for operators, designers, manufacturers, architect-engineers, constructors, and regulators of safety related systems and components. To achieve this end, statistics have been grouped and combined across various categories and presented as such separately for each system and component category in this report. The annual reports are an outgrowth of some 5 years of data collection experience on commercially operated United States nuclear powerplants and were initiated to serve the needs of the users in their application of operating data experience.

(5) Nonelectronic parts reliability data (Rossi, 1985)

This report, organized in four major sections, presents reliability information based on field operation, dormant state, and test data for more than 380 major nonelectronic part types. The four sections are Generic Data, Background Information, Detailed Data, and Failure Modes and Mechanisms. Each device type contains reliability information in relation to the specific operational environments. The five environments represented in the data are (i) ground fixed, (ii) ground mobile, (iii) airborne, (iv) shipboard, and (v) dormant. The report also specifies the user of each component, whether it be a military, commercial, or industrial application. Upper and lower interval limits were computed using a Chi-square distribution, and a point estimate of the mean failure rate was also included. For the purpose of the database, only the failure rates, interval limits, environment, and user codes in the Generic Data section were recorded.

A list of all the references used in assembling the failure-rate database is furnished in Appendix B. The sources are divided into primary and secondary references. References from which data have been extracted for inclusion into the database are termed primary references. In most cases, each primary reference document obtained its data inputs from several other references (secondary references). Letters denote primary references, while numbers have been used to represent secondary references. Thus, many data entries have both a letter and a number in the reference code. A description of each primary source was also added to allow the user to gain a better understanding of the available data. Each report used as a source of data is carefully perused to find the most accurate data available, which is then carefully entered into an Microsoft Access database. Each entry includes the name of the component, a short description if available, the estimated failure rate and its units, its reference code, and any additional remarks or extra data. The list of references used in the database currently contains 37 primary references (denoted by alphabetical letters) and 109 secondary references (listed by numbers), for a total of 146 documents. Some documents may be listed as both primary and secondary references if they were used as a primary reference and were also listed as a secondary reference in another primary document.

To avoid errors and maximize the quality of the database, a rigorous data entry process was used that involved reviews and checks of both the references and the failure rates. All values entered were checked and documented in an ongoing log.

5.3 Data Analysis

The biggest challenge in the construction of the database was determining what would be useful data. As stated previously, the type of component was not considered in making this determination, but rather the analysis applied to the data was considered. NUREG/CR–2300 (Hickman, et al., 1983) classifies probability analysis into two categories, the classical and Bayesian approaches. The classical method relies heavily on the data itself, dealing mainly with point estimates and confidence intervals established by mathematical computations. The Bayesian method necessitates a greater contribution by the analyst in the selection of prior and posterior distributions and requires the analyst to take into consideration previously known information when developing the models. A Bayesian analysis would be more appropriate for refining a model after receiving feedback, but is not necessarily appropriate for risk assessment analysis in the context mentioned in other parts of this report. Bayesian analyses can prove to be more specific than their classical counterparts, but must also be defended by the analyst and rely heavily on his judgment.

While both methods have merits, the analyst input required in the Bayesian approach proved to be too subjective for the application of this database, thus, a classical method was pursued. This meant that all of the data taken from the reports had to conform to the classical model so that the database could be used in a classical analysis. The main focus of the search through the reports was to find point estimates of the failure rates and the probability of failure on demand. Most reports followed fairly similar patterns, and almost all used binomial or Poisson distributions, depending on the data examined. For the purpose of this discussion, the Licensee Event Reports [see NUREG/CR–2300 (Hickman, et al., 1983)] will be used as an example. The Licensee Event Reports [see NUREG/CR–2300 (Hickman, et al., 1983)] use the same methodology in almost every report to keep the analysis consistent between components, making them excellent samples to study the analysis process. In the Licensee Event Reports, the failure rate estimates were calculated as

$$\lambda = N / T \tag{5-1}$$

N is the number of failures for all of the reported components during the specified time period and T is the number of hours in the specified time period multiplied by the number of components. These estimates are recorded as the failure rate in the database and are categorized by failure per hours (operating, calendar, or standby where applicable). Operating hours were assumed to be the default mode of hours studied, however, notations were made if the data reflected calendar or standby hours. The failure rates for components that were measured in hours always yielded a large number of hours, thus, the large population size of hours allowed the analysts to approximate the binomial distribution with a Poisson distribution. The estimate of the failure rates for the demands placed on components is given by

$$\lambda = N / D \tag{5-2}$$

Here, N is again the number of failures for all of the reported components and D is the total number of demands placed on all of the components. In most reports, the estimates of the rates of failure on demand were modeled in a binomial distribution when the number of demands was relatively small. After the number of demands exceeded a certain minimum, however, the population of demands became large enough to be modeled by a Poisson distribution. In the Licensee Event Reports, a Poisson distribution was used if $D - N > 100$.

When available, error factors and minimum, maximum, high, and low values, along with standard errors and variances, were entered along with the failure rates to give the user more insight into the applicability of the data.

An important item to note is that no command faults were included with the data unless specifically mentioned in the reference remarks column. Command faults were omitted because they stem from failure of other components. The entire premise of the database assumes that each failure is independent of another and, thus, can be analyzed together in a fault tree. Therefore, command faults were left out of the data whenever possible.

5.4 Current Data in Database

Although the volume of data in the database is relatively large, it is by no means exhaustive. Many components have multiple entries with varying rates taken from different sources. For instance, some reports determine a point estimate or estimated failure rate, which is an aggregate number derived from one of two or three possible statistical distributions applied to a large population of sample data. Oftentimes, these same reports give 90-percent confidence intervals or error factors to aid in determining the applicability of the data. Other reports simply determine a failure rate by dividing the number of failures by the number of operating hours and give no other information. Each entry in the database has potential use in certain types of analysis. It is up to the user to choose the most appropriate set of data. Given the wide range of information available, great care must be exercised in choosing component failure rates.

When selecting data, one must also carefully consider the type of failure associated with each entry. Failure modes can range from spurious operation to catastrophic failure. Whereas some reports consider a failure a lack of ability to perform a task at a certain time or on demand, analysts in the nuclear field are interested in any possible failure, not just a catastrophic failure. While many industries are simply concerned with the ability to perform a task, analysis in a safety assessment is generally much more rigorous. Thus, depending on the use of the components, interpretation of the failure modes could vary.

The components entered into the PCSA Tool database are generally applicable to a nuclear waste fuel repository and the nuclear industry in general. The following are three sample components that represent the type of data available in the database.

<u>Cranes</u>: Entries for various cranes and gantries can be found in the database. Most entries deal with different failure modes of bridge cranes, because it was determined that these might be the most useful in the Yucca Mountain study. Every entry reports a failure rate, and many list high and low values for the failure rates while some give a standard error for the components. The failure rate came from a total of four different primary sources.

<u>Pumps:</u> Pumps are among the most plentiful components in the database with 494 entries. Components include alternating/standby pumps, centrifugal, and positive displacement motor pumps, to name a few. Failure rates as well as high and low values and 90-percent confidence

intervals are available on many of the entries. The failure modes include failure to start on demand and failure during operation, among others.

Human Error: The database contains 89 entries classifying distinct routine human errors from 8 primary sources. Of those entries, 46 have standard error factors recorded and 4 give high values in addition to the failure rates themselves. The errors range from mistakes in recalling instructions to procedural deficiencies.

Wherever possible, equipment and system failure-frequency data have been tabulated as failures per hour of operation and failures per demand. Due to the wide range of components listed in the database, entries are not uniform. Many entries are listed as failures per calendar hour, standby hour, or operational hour. In each case, the units have been clearly indicated. In addition, five different fields of possible failure rates are included in the database: (i) failure rate, (ii) low value, (iii) high value, (iv) 20-percent lower, and (v) 80-percent upper. The failure-rate field generally shows the best estimate or average failure rate given for that component. The high-value and low-value fields give statistically calculated high and low estimates of the failure. The 20-percent lower and 80-percent upper apply only to certain components taken from references that applied a Chi-square analysis to the data, giving a lower and upper limit. Although the last two are similar to the high and low value, they have been included to show a specific application of statistical analysis, rather than lumping these numbers into the more general high and low group. The literature source for each data point has been referenced. The failure-rate data for cranes is included in Appendix C as an example of the type of data available in the database.

To avoid errors and maximize the quality of the database, a rigorous data entry process was used that involves reviews and checks of both the references and the failure rates. All values entered are checked and documented in an ongoing log.

Because available failure-rate data are generic in many cases, the risk analyst must exercise good judgment in their use. The user may choose to use the data if the equipment description, process condition, and failure mode defined in the data cell are similar to the equipment being studied. The user may have to adjust the data to account for differences in equipment design, process conditions, and such. In such cases, it is probably appropriate to apply adjustments only to the first significant number and associated power for generic failure data.

5.5 PCSA Tool Function

The PCSA Tool provides an easy and effective method for accessing the failure rate database. The menu driven tool provides two distinct methods for searching the database: (i) through the use of the taxonomy tree and (ii) with the aid of the search function. Both methods perform a query of the underlying Microsoft Access database using Select statements. The only difference between the methods is that the taxonomy tree automatically provides a search criterion when the user selects a component, and the search function requires the user to specify a search criterion. Searches can be performed on a component name, a component name and description, and the reference name. The search by reference name feature has not yet been activated in the tool. The data are displayed on a form in a grid format, with boxes available to view both the primary and secondary references for each component. The user simply types the code number/letter of the reference displayed with the component, and the resulting reference entry is displayed in the box below the grid.

The taxonomy tree presents all of the categories of components for the user to browse through, similar to a file explorer. Each branch of the tree hides underlying branches, until selected, on which it expands to show the next level of classification. Sublevels can be accessed by clicking on parent nodes in the tree, and individual component entries can be viewed by double clicking on the component in the tree. The tree is displayed each time its menu button is selected underneath the Failure Rate menu on the PCSA Tool. When the tree is opened in the tool, the software creates the first level of the tree with all of the Equipment Types. The sublevels of each Equipment Type are composed of Equipment Groups, which are also read in and placed below the appropriate Equipment Type. Finally, the Equipment Descriptions are placed beneath the appropriate Equipment Groups on the tree. If no Equipment Group exists for a component, however, it is placed at the same level as an Equipment Group.

For example, if one wishes to access data on bridge crane components using the tool, one can do this by using the taxonomy tree or by activating the search feature.

The taxonomy tree is activated by first clicking on the Failure Rate in the main menu, and then clicking on the View Taxonomy option in the submenu. Figure 5-2 is a screen-shot from the tool. The taxonomy tree is shown on the left-hand side. Clicking on Crane and then on Display in the taxonomy tree box will result in the display box with search results for cranes as shown on the right-hand side in the figure. One can then scroll down the display box until the appropriate data are located in Fields 2, 3, and 4. Finally, information on the reference source for the data is obtained by typing the letter U in the Letter ID field, a number in the Number ID field, and then clicking the Find button in the form. The primary and secondary references are displayed in the windows below the grid as shown on the right-hand side in the figure.

Alternatively, the failure rate database can also be accessed by first clicking on the Failure Rate menu in the main menu and then clicking on the Search Database option in the submenu. Figure 5-3 is a screen shot from the tool. The Failure Rate Data Search form is shown on the left-hand side. Typing the component name and description in the Failure Rate Data Search form (i.e., Bridge and Crane) will again result in the display box with search results as shown on the right-hand side in the figure. Finally, information on the reference source for the selected data is obtained by typing the letter U in the Letter ID field and then clicking the Find button on the form. The primary and secondary references are displayed in the windows below the grid as shown on the right-hand side in the figure.

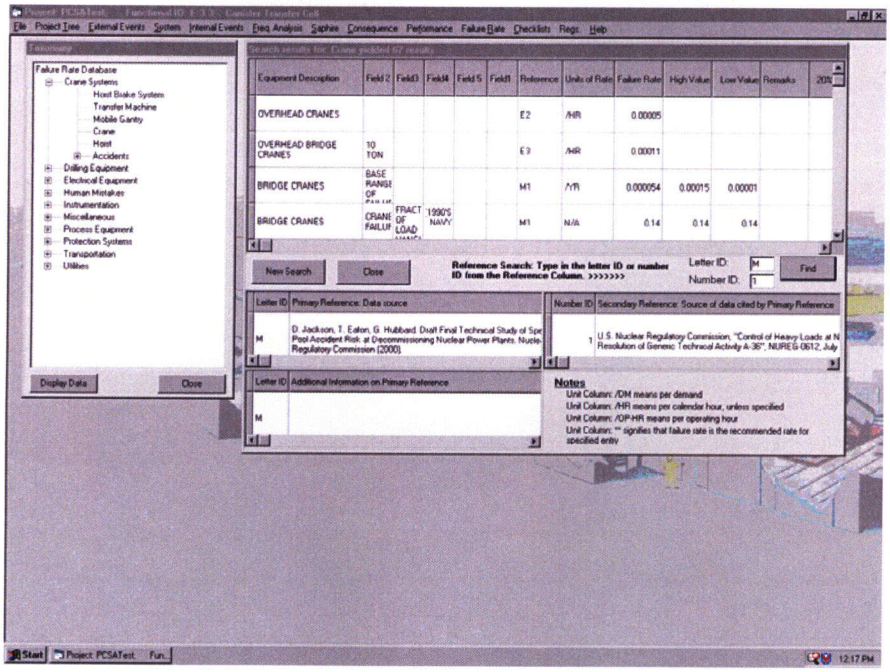


Figure 5-2. Taxonomy and Search Results Table

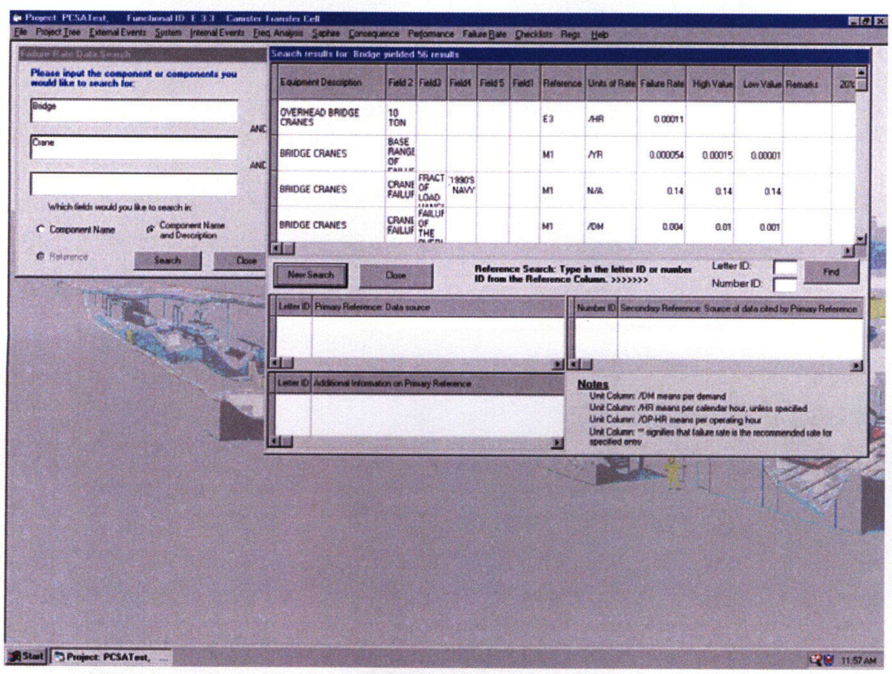


Figure 5-3. Data Search and Search Results Table

6 IDENTIFICATION OF EVENT SEQUENCES

This chapter discusses the application of the PCSA Tool to review the U.S. Department of Energy (DOE) identification of event sequences and categorization of events. The term "event sequence" is defined in 10 CFR 63.2 as a series of actions and/or occurrences within the natural and engineered components of the repository that could potentially lead to exposure of an individual to radiation. The regulation further clarifies that an event sequence includes one or more initiating events and associated combinations of repository system component failures, including those produced by action or inaction of operating personnel. Additionally, the DOE is required to categorize event sequences based on the frequency of occurrences and to demonstrate compliance with dose consequence requirements for Category 1 and Category 2 event sequences. The Yucca Mountain Review Plan (NRC, 2002a) provides guidance in Section 4.1.1.4. on the review of the identification of event sequences considered in the preclosure safety analysis. In accordance with the NRC (2002a), staff will conduct limited independent analyses using the PCSA Tool to confirm that possible event sequences are adequately identified and that DOE analyses and calculations have been performed properly. The staff will use the PCSA Tool, including sensitivity and uncertainty analyses, to verify that (i) assumptions made in identifying event sequences are justified and supported by site-specific and facility data, (ii) analyses considered reasonable combinations of initiating events and associated event sequences that could lead to exposure of an individual to radiation, (iii) relevant human actions were considered, and (iv) categorization was done in accordance with the definition of Category 1 and Category 2 event sequences in 10 CFR 63.2.

6.1 Event Sequence Analysis Techniques

In its preliminary analysis, the DOE evaluated event sequence frequencies for postulated scenarios primarily arising from operations in the proposed facility (CRWMS M&O, 1998a, 1999e,g, 2000f). Event scenarios are combinations of initiating events and subsequent sequences of events that may lead to exposure to radiation. An event scenario is developed by first identifying an initiating event from the site-specific and facility hazards analysis and then postulating progression of event sequences. The scenario development process results in a series of event sequences, each having a specific frequency of occurrence. The PCSA Tool uses analysis methods and tools commonly used in probabilistic risk assessment (e.g., event trees, fault trees, human reliability trees) for event sequence analysis (Hickman, et al., 1983). As shown in Figure 2-2(b), the PCSA Tool modules for identification of event sequences are Development of Event Scenarios and Event Sequence Analysis. In the Development of Event Scenarios submodule, the scenarios and data required for event tree, fault tree, and human reliability tree analyses are generated. These modules require input from the Failure-Rate Database module for probability of component failure, and human error probabilities and performance shaping factors for human reliability tree analysis. The Failure-Rate Database is discussed in Chapter 5. The event trees and fault trees are modeled, analyzed, and quantified using a standalone code, SAPHIRE. In addition, the output of event trees and fault trees from the SAPHIRE code runs are stored in the Event Scenario module. This chapter discusses the event tree, fault tree, human reliability tree analyses techniques, capabilities of SAPHIRE code, PCSA Tool functions along with an example, and categorization processes of the event sequences.

6.1.1 Event Tree Analysis

An event tree analysis is a graphical tool used to characterize and quantify event sequences by postulating an initiating event and propagating its consequences through a series of safety-related system failures or operations (NRC, 1994). An event tree models the sequence of events that result from a single initiating event. Event trees provide a systematic way of recording the event sequence and defining the relationships between the initiating events and subsequent events.

The technique is universally applicable to systems of all kinds and is widely used in the probabilistic risk analysis for nuclear powerplants (Hickman, et al., 1983). Although the technique is exhaustively thorough, the success of the technique is based on three basic presumptions: (i) that all system events have been anticipated, (ii) all consequences of these events have been explored, and (iii) the probabilities of failure for all the events have been correctly estimated.

The probability of events that appear in the event tree are quantified using actuarial data, fault trees, Bayesian analyses, expert judgment, or other methods of estimation. If the system represents a single component or piece of equipment whose failure is modeled in the event tree, the component failure rate can be estimated directly from actuarial data, if available, or by synthesis of data from similar equipment. For multicomponent or complex subsystems, fault trees are used to find the failure probabilities for each node in the event tree. Depending on the nature of the subsystem characterized at a particular node, the fault tree may contain electrical components, mechanical components, human actions, or some combination of these.

The process for event tree analysis is described in Figure 6-1 (Frank, et al., 1998). An event tree begins with an initiating event on the left and ends with one or more end states on the right. Across the top are events that must influence how the initiating event can progress to one of the end states. A scenario is characterized by a line starting at the left under the initiating event, proceeding horizontally and vertically in a continuous line through several nodes, and terminating in a single end state. The initiating event has a frequency of occurrence, f_{IE}, which may have units such as events per year. Each subsequent event is processed as a yes or no question based on the success/failure of the event. If the answer is yes, the scenario proceeds up and then right to the next event. If the answer is no, the scenario proceeds downwards before going right. A number, such as $P(E_1|IE)$, characterizes the fraction of occurrences for which the answer is yes. This number is called the conditional probability of the event or branch point probability. Each scenario has an end state and a scenario frequency. Each node has two branches extending to the right. The sum of the two branch point unconditional probabilities, corresponding to success and failure, must equal unity. The scenario frequencies, therefore, reflect the partitioning of the initiating event frequency such that the sum of the scenario frequencies equals the initiating event frequency.

Because of the complementary nature of using both inductive and deductive reasoning, event trees and fault trees are often combined for system risk analysis. This practice produces more complete, concise, and clearer development and documentation of scenarios than using either one exclusively. High-level events, such as systems or functions, can be depicted in event trees, and fault trees can be used to analyze the causes of system or subsystem failures depicted in the event tree. Thus, event trees generally give an overview of the scenarios

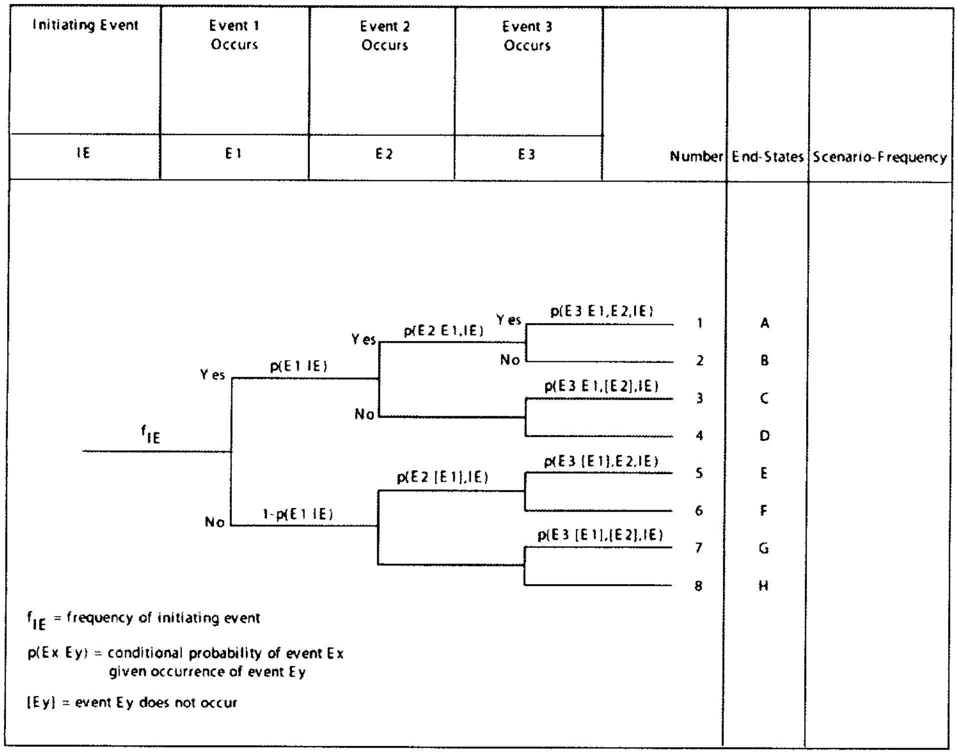


Figure 6-1. Concept of Event Tree (Frank, et al., 1998)

leading to end states, while fault trees are used to analyze causes of failures and development of the probabilities.

6.1.2 Fault Tree Analysis

Construction of a fault tree involves deductive reasoning (Frank, et al., 1998). Deduction constitutes reasoning from general to specific. A fault tree is a graphical tool that is used to depict all the possible ways that an undesired system state (no top event) could occur (NRC, 1994). The initial step in constructing a fault tree involves specifying the top event (shown in Figure 6-2), which is simply the undesired state of a system. The system is then analyzed in the context of its operation and items related to safety to find all credible ways the top event can occur. In the process, all redundancies, controls, software, maintenance, inspection, and other human actions should be considered. A fault tree uses logical gates (AND, OR, NOT) to depict the relationships among events and the top event (NRC, 1981). The lowest level in a fault tree is called a basic event. Each basic event is assigned a probability of occurrence. The probability of failure may be obtained from the actuarial database of failure rates of components, if available. If a fault tree is constructed and analyzed correctly, it will provide the probability of the occurrence of the top event as a combination of the basic event probabilities. Any fault tree has an equivalent Boolean equation that expresses the relationship of the basic events, the component failures, and the top event. To correctly obtain the probability of the top event as a function of basic event frequencies and component failure rates, a fault tree is usually reduced to its Boolean prime implicant (Frank, et al., 1998).

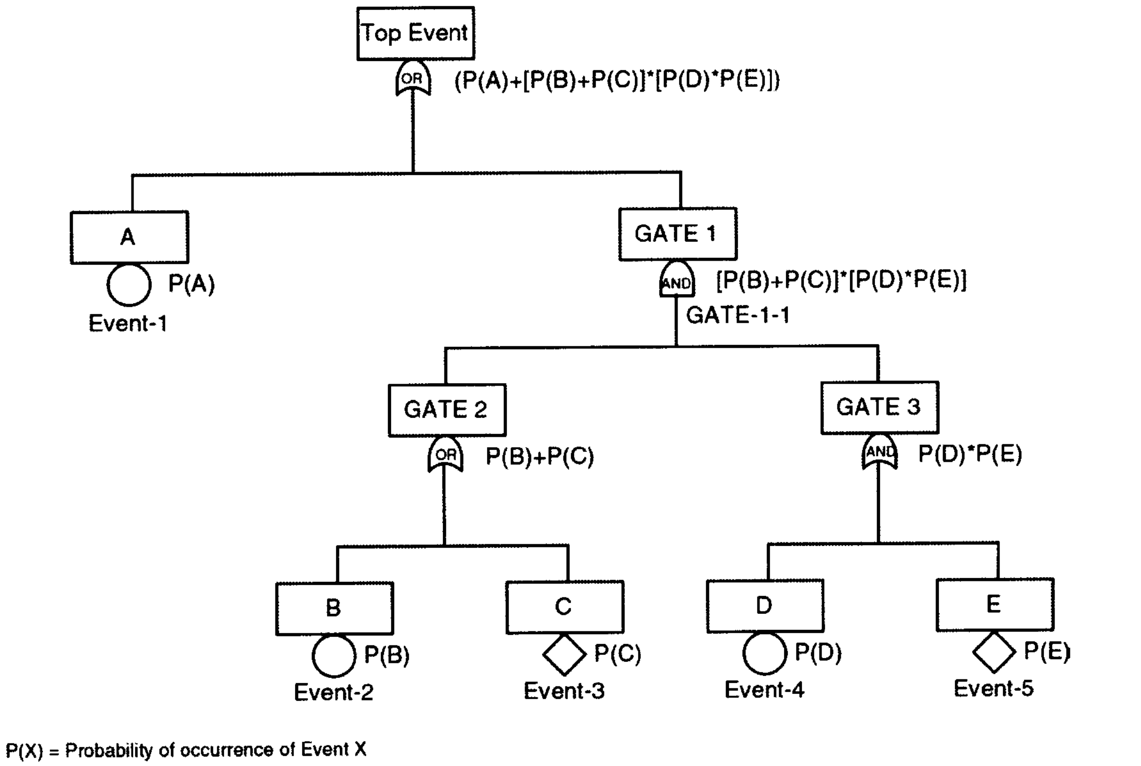


Figure 6-2. Concept of Fault Tree (Frank, et al., 1998)

6.1.2.1 Uncertainty

The frequency of a component failure or initiating event is usually uncertain. Typically, this uncertainty is represented by a probability distribution of frequency of failure or frequency of an initiating event. As described above, the behavior of components and initiating events, combined with system characteristics, are used to generate event sequences, which lead to system failure states. Since the underlying frequencies of the component failures and initiating events are uncertain, the frequencies associated with the resulting event sequences are also uncertain and dependent upon the uncertainty of the constituent frequencies. Categorization of event sequences based on their frequencies is required by 10 CFR Part 63.

A simple way to obtain a single estimate of the frequency of an event sequence is to use the mean values (or other appropriate point estimates) for the constituent frequencies to quantify an event tree, thereby obtaining a point estimate of the event sequence frequency. However, such an approach does not take advantage of the information contained in the probability distributions of the underlying frequencies. Furthermore, by ignoring the uncertainty associated with each frequency or probability estimate, an event sequence and its associated consequences may be incorrectly categorized.

A more complex analysis can provide an estimate of the probability distribution of the event sequence by propagating the uncertainty in the component frequencies through the Boolean computation. Typically, the generation of the uncertainty distribution of event sequence frequency is obtained by Monte Carlo sampling of the underlying component frequency distributions. Then, in order to categorize the event sequence, an appropriate statistic of the event sequence frequency distribution is used (e.g., the mean, median, or 95 percentile). The Statement of Consideration for 10 CFR Part 63 states that the DOE will need to take into account uncertainties in event sequence frequency evaluation. The Statement of Consideration further notes that analyses relying on point estimates will need to discuss how uncertainties are taken into consideration. Alternatively, the DOE could describe component failure frequencies with probability distributions and analyze the propagation of these uncertainties to obtain a probability distribution for event sequence frequency. The NRC has stated its position that if the DOE obtains a probability distribution for the frequency of a preclosure event sequence, the mean value of that distribution can be used to categorize the event sequence, provided that the probability distributions of the component failures are valid and account appropriately for failure frequency uncertainty.[1] Consideration of uncertainty in the probability of failure in the event sequence analysis is shown graphically in Figure 6-3.

6.1.3 Software Used to Perform Event Tree and Fault Tree Analyses

The event tree and fault tree are analyzed in the PCSA Tool using SAPHIRE Version 6.7 code. SAPHIRE Version 6.7 is a Windows® based software developed for the Division of Systems Technology Office, U.S. Nuclear Regulatory Commission, Washington, DC, by Idaho National Engineering and Environmental Laboratory, Idaho. The software is distributed by the Radiation Safety Information Computational Center, Oak Ridge National Laboratory, Oak Ridge, Tennessee. The SAPHIRE program is invoked by clicking Saphire on the main menu bar in the tool. If the user of the PCSA Tool wants to exercise this capability, the user needs to be familiar with the way the SAPHIRE code models event trees and fault trees.

The SAPHIRE software is a collection of programs developed to perform the functions necessary to conduct probabilistic risk assessment for nuclear powerplants (Russel, et al., 1993). The programs included are the Integrated Reliability and Risk Analysis System, (usually designated as IRAS), the System Analysis and Risk Assessment System (usually designated SARA), the Models and Results Database System, and the fault tree, event tree, and PQID graphic editor software. These programs include functions to allow the users to create event trees and fault trees, define event sequences and basic event failure data, solve system and event sequence fault trees, quantify cut sets, perform uncertainty and importance analyses on the results, and perform sensitivity analysis. The program generates reports and displays graphics that can be used to document the results of an analysis.

The SAPHIRE code analyzes a system failure response by the fault tree linking process, a technique whereby the fault tree logic is combined with event tree logic resulting in a logic expression for each sequence in the event tree (Idaho National Engineering Laboratory, 1998). Event trees are generated for a postulated event scenario using a graphical editor starting with an initiating event and branching as various system safety functions are challenged, resulting in the probability of success or failure at each node. Once the event tree is generated, the SAPHIRE code assumes that each top event is represented by a fault tree. The software

[1]Reamer, C.W. "U.S. Nuclear Regulatory Commission/U.S. Department of Energy Technical Exchange and Management Meeting on Preclosure Safety (July 24–26, 2001)." Letter (August 14) to S. Brocoum, DOE, Washington, DC: NRC. 2001.

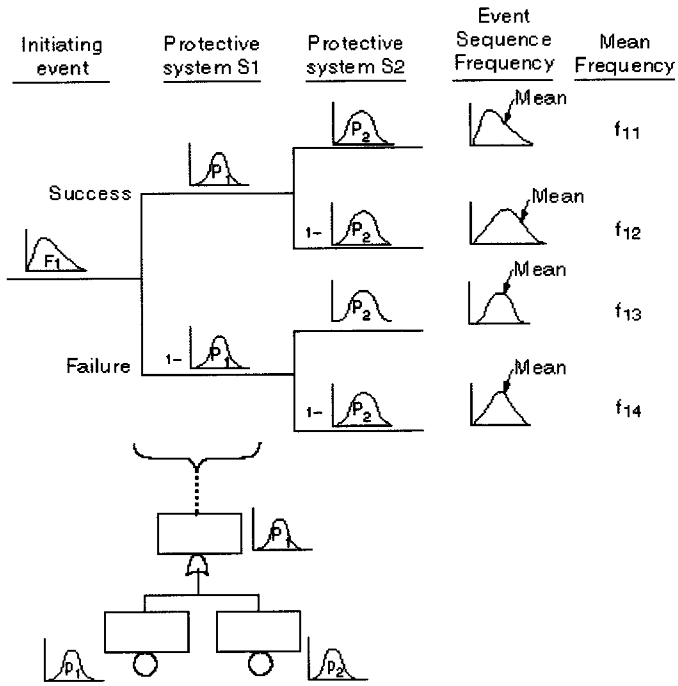


Figure 6-3. Example of Event Tree Linked with Fault Tree with Consideration of Uncertainties

provides the option to analyze an event tree without developing a fault tree logic for a top event. The top event is treated as a basic event for which failure probability or frequency should be assigned. This option is indicated through a process flag.

The fault tree consists of basic events representing faults (e.g., hardware failure, human error or adverse conditions) and logic gates representing Boolean operations (e.g., union [OR], intersection [AND]). The fault tree is modeled in the SAPHIRE code using a graphic editor or logic editor. The code requires failure probability of basic events as input to the model. The user can specify a point estimate or distribution of the basic event probabilities as input. Basic events are always assumed to be independent of each other (i.e., one basic event does not influence the probability of occurrence of any other basic events). Data for the basic event can be obtained from the failure-rate database in the PCSA Tool, if applicable. The failure-rate database, depending on the nature of the component, provides failure rates as either a failure per demand for demand components or a failure per unit time for continuous use components. For operating components with a failure rate, the software requires the user to specify mission time and repair time to develop a failure probability.

The uncertainty analysis in SAPHIRE calculates uncertainty of the top event probability resulting from uncertainties in the basic events probabilities. The user can select from several probability distributions (e.g., normal, log normal, beta, Chi-squared) provided in the software. For all basic events, the SAPHIRE code randomly samples the parameters from their probability distributions and uses these parameters to calculate the probability of the top event. Two types of simulation are used in the software; simple Monte Carlo sampling and Latin

Hypercube Sampling. When fault tree analyses are linked with event tree analyses, the uncertainties in basic events are propagated through the model.

The SAPHIRE code also performs system importance analysis. The importance analysis provides reliability-worth about basic events appearing in the cut sets for a fault tree. The various importance measures used in the software are Fussel-Vessely, Risk Reduction Ratio, Risk Increase Ratio, and Birnbaum.

6.1.4 Human Reliability Tree

The approach to human reliability in the PCSA Tool parallels the approach taken for mechanical components. The initial elements of the approach are qualitative; then, if the analyst so chooses, quantitative elements may be undertaken. The generic elements in the PCSA Tool for these types of analyses are system description, hazard analysis, event tree/fault tree generation, and quantification of trees using the probability database.

An output from the Human Reliability Analysis is a screened list of human actions, indicating the nature and properties of various human actions that may have a significant impact on repository safety. This subset of human actions would then be modeled in one of the three ways: event tree, fault tree, human reliability tree.

For the event tree, the human action would be inserted in a straightforward fashion as either (i) an initiating event, or (ii) as a branch in the tree, describing a mitigation of an event already initiated by human or mechanical failure or an external event. In these cases, the human action would need to be simple and characterized by failure probability. In the event that a human action is more complex (perhaps a sequence of steps) and is also interacting with mechanical components that may fail, expansion of a particular subsystem failure by a fault tree that encompasses both human and mechanical failures is needed. In the limit of no mechanical failures, this fault tree could represent a sequence of human actions. Consideration of human error along with other system failure is integrated with event tree and fault tree generation as discussed in Sections 6.2.1 and 6.2.2. A human reliability tree would be used for a sequence of human actions in which recovery activities are significant.

The basic approach for the human reliability tree 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 6-4 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 6-4 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 Guttman, 1983) suggests that, for an initial analysis, only the fully successful leg needs to be quantified, since it

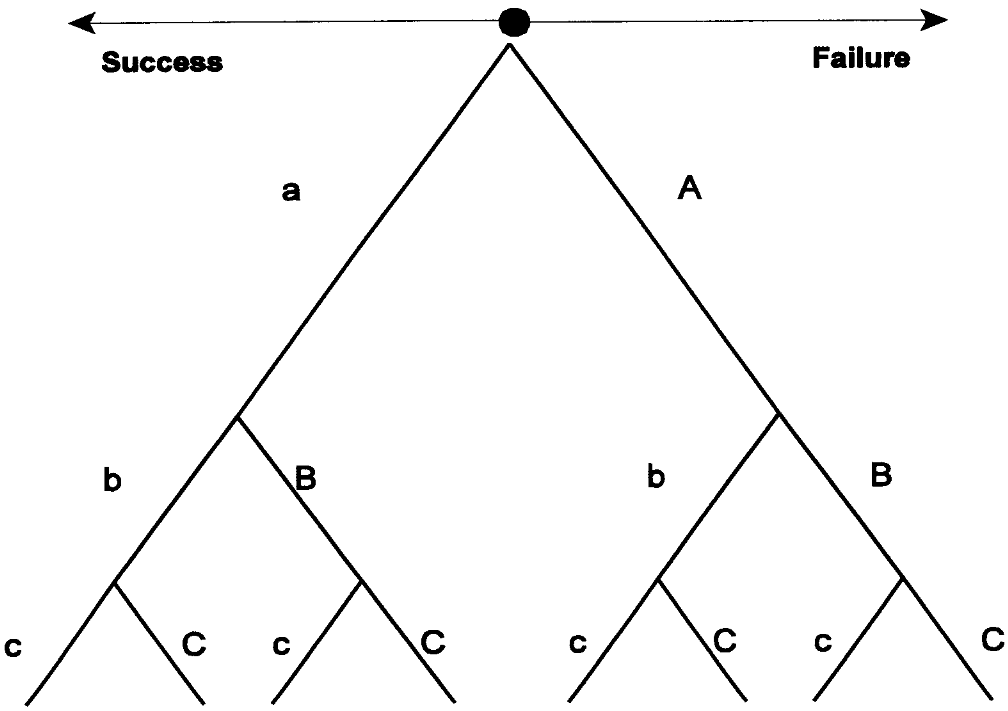


Figure 6-4. Archetypical Human Reliability Analysis Tree

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.

Basic human error probabilities have been compiled as part of the Technique for Human Error Rate Prediction methodology; a sample is provided in Table 6-1. A general classification scheme for human errors used in the Technique for Human Error Rate Prediction 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 the wrong sequence of actions
(v) Implements incorrect timing (early or late)
(vi) Uses the incorrect quantity

Table 6-1. 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. Guttman. NUREG/CR–1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." Washington, DC: NRC. 1983.			

The basic human error probabilities listed in Table 6-1 include a representation of uncertainties inherent in those probabilities. The column labeled "Error Function" represents the error function defined by Swain and Guttman (1983), which is the square root of the ratio of the 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 6-1, 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 6-2. 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 Technique for Human Error Rate Prediction 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, Technique for Human Error Rate Prediction defines four levels of tagging or locking systems (Swain and Guttman, 1983). Three of these levels involve increasing degrees 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, Technique for Human Error Rate Prediction provides modifying factors based on different stress and experience levels (Swain and Guttman, 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 5 for an experienced worker, but by a factor of 10 for a novice.

One additional feature of the Technique for Human Error Rate Prediction 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 6-2, 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 6-4, suppose the three human activities (a,b,c) act in a redundant fashion as follows:

(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 $P(A) \cdot P(B) \cdot P(C)$, 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

Table 6-2. Definitions of Performance Shaping Factors*	
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/control. Is it a video display screen, a rotary control, a meter, etc.
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?
Task dynamic or step-by-step	Is the task performed concurrently with other tasks or is it performed step-by-step?

Table 6-2. Definitions of Performance Shaping Factors* (continued)	
Performance Shaping Factor	**Definition**
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 task?
Local versus remote control	Is the task performed in the control room or locally at a valve, switchgear room, or fuel farm?
Clothing/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.	

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 Technique for Human Error Rate Prediction methodology.

6.2 PCSA Tool Functions for Event Sequence Analysis

6.2.1 Event Tree Analysis

An event tree emphasizes the initial cause of potential events and works from the initiating event to the event final effects. Each branch of the event tree represents a separate event sequence. The initiating events identified from component failure (failure modes and effects analysis), process (What-If), energetics (Energy Method), human action (Human Reliability Analysis), or site-specific naturally occurring or human-induced events analyses, under the Initiating Event menu, are developed into event scenarios. For the purpose of this report, an event scenario is defined as an event that includes an initiating event and a set of subsequent event sequences.

Event scenarios are created in the PCSA Tool to serve as inputs for the event tree diagrams to be modeled and analyzed using the SAPHIRE code. To develop an event scenario, the user selects the Freq. Analysis in the main menu bar and Event Tree drop-down list. The Freq. Analysis menu can be used only after selecting a functional area in the Project Tree menu. The event scenarios are developed using the Event Tree Form as shown in Figure 6-5. The user develops an event scenario based on the initiating event and postulated sequence of events. Event scenario data are entered using the Add Scenario button. The user would assign a unique alphanumeric identification for the scenario at the Scenario ID field and provide (i) description at Event Scenario Description field, (ii) additional information if required, at Additional Description field, (iii) and the name of the directory and path where the SAPHIRE code analysis data of the event tree for current event scenario exist are stored in the SAPHIRE Data Path field. In addition, the Event Tree Form includes a Yes/No button for the user to select whether the postulated event scenario will be used for the safety assessment and risk assessment to be analyzed later. By default, all event scenarios are included in the analysis while event scenarios not required to safety assessment can be deselected. The user, however, can make the choice any time and is not required to decide while developing the event scenario.

This option has been introduced primarily for sensitivity analysis. For example, the user can build alternative event scenarios, which may be based on the same initiating event but with different subsequent events, probabilities or uncertainties. Safety assessment under the alternative scenarios can, thus, be studied. This gives users the flexibility to retain all the postulated event scenarios in the tool database but use selected ones for each specific analysis. The user can change this option any time during the analysis. Data entered in the Event Tree form is saved in the database using the Update button while the Close button will not save data in the database. The information on event scenarios can be edited using the Edit Record button. Next, the user will select the initiating events from the already identified initiating events in the functional area. An initiating event can be selected from the drop-downcombo box, which shows a list of Initiating Event ID identification numbers. Upon selection of an initiating event, other related information such as description and frequency, along with details on associated uncertainty, is displayed. Following the initiating events, the user will postulate subsequent events describing failure of components or systems used for mitigation of an initiating event.

This is achieved in the Subsequent System/Operations Failure frame in the form, subsequent events are entered, edited, and deleted using the Add Subseq Event, Edit Subseq Event, and Delete Subseq Event buttons, respectively. The user will enter a description of the subsequent event, probability, and associated uncertainty information in the respective fields. The subsequent event number is automatically selected. In addition, the user can provide information if the event is linked to a fault tree or human reliability analysis tree and provide information such as description of the fault tree, top event name, and other desired information that help connect to other sections of the tool where further information can be obtained. The summary of the data for each subsequent is displayed at the bottom. The event scenario identification number will then be propagated to the Event Sequence Form under the Freq. Analysis menu. Show Report generates the report, which can be printed.

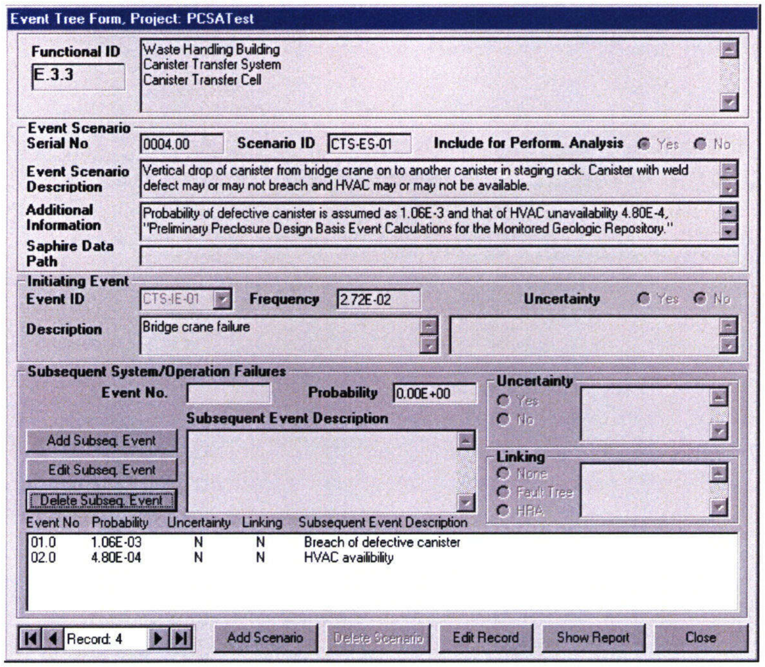


Figure 6-5. Example of Event Tree Form

The event tree models are developed in SAPHIRE. SAPHIRE is a standalone Windows based software where the model development and analysis will be carried out independently based on the information developed in the Event Tree Form.

6.2.2 Fault Tree Analysis

The tool provides means to store information on data used to model fault trees and also the results from the analysis. The Fault Tree sub-menu can be accessed through the Frequency Analysis submenu located under Event Frequency in the main menu bar. The Fault Tree submenu leads to the Fault Tree Form dialog box to allow users to generate data for fault tree analysis. The Fault Tree form, as shown in Figure 6-6, allows data entry using the Add Record button. The user can enter the name and description of a top event, additional information if desired, and the location of the fault tree SAPHIRE files. The Update button will save the data in database. The probabilities or frequencies of the top event derived by SAPHIRE analysis are stored in the fields under the frame entitled Probabilities in the form. The mean, median, and 5 and 95 percentile values of the top event from the uncertainty analysis can be stored; in addition, the point estimate value is stored at the Point estimate field. The Fault Tree Table button brings up a Fault Tree Event Table dialog box that allows users to enter additional information on each top event, e.g., basic events, gates etc. The fields in this form, as shown in Figure 6-7, are Event Name, Type of Event, Description, Probability, Uncertainty, and Additional Information. The Add Record button will add an entire blank row. Data in each cell can be added and edited using the Edit Record button or by double clicking on the cell.

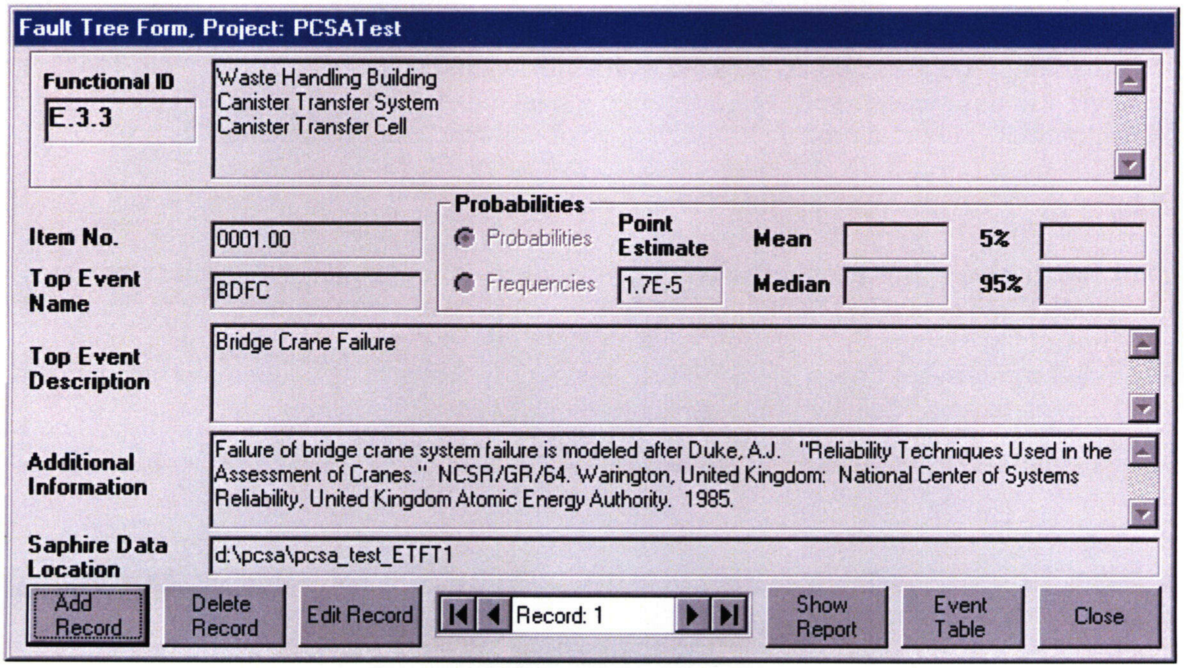
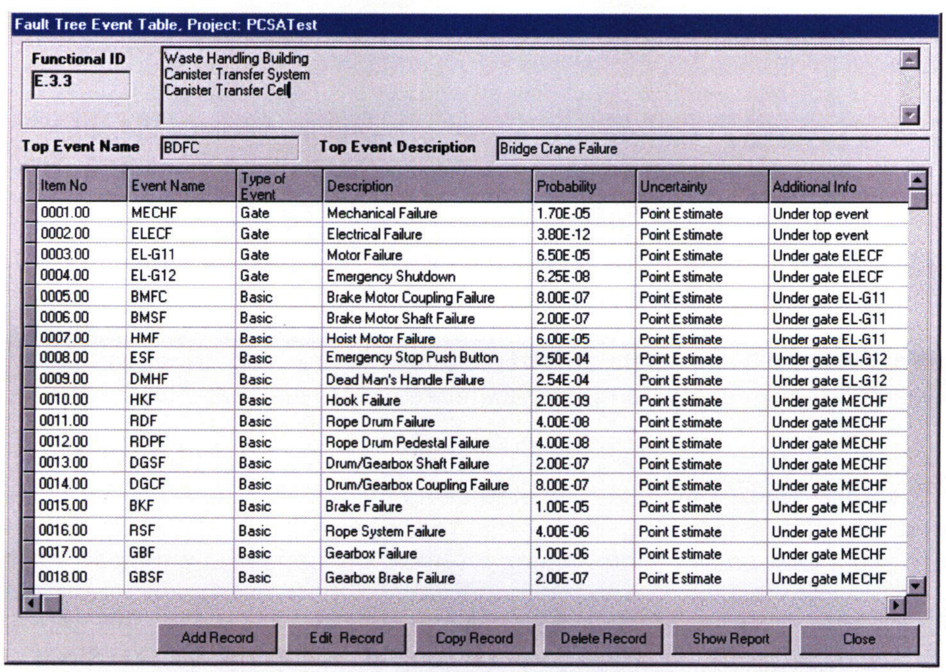


Figure 6-6. Example of Fault Tree Form



Item No	Event Name	Type of Event	Description	Probability	Uncertainty	Additional Info
0001.00	MECHF	Gate	Mechanical Failure	1.70E-05	Point Estimate	Under top event
0002.00	ELECF	Gate	Electrical Failure	3.80E-12	Point Estimate	Under top event
0003.00	EL-G11	Gate	Motor Failure	6.50E-05	Point Estimate	Under gate ELECF
0004.00	EL-G12	Gate	Emergency Shutdown	6.25E-08	Point Estimate	Under gate ELECF
0005.00	BMFC	Basic	Brake Motor Coupling Failure	8.00E-07	Point Estimate	Under gate EL-G11
0006.00	BMSF	Basic	Brake Motor Shaft Failure	2.00E-07	Point Estimate	Under gate EL-G11
0007.00	HMF	Basic	Hoist Motor Failure	6.00E-05	Point Estimate	Under gate EL-G11
0008.00	ESF	Basic	Emergency Stop Push Button	2.50E-04	Point Estimate	Under gate EL-G12
0009.00	DMHF	Basic	Dead Man's Handle Failure	2.54E-04	Point Estimate	Under gate EL-G12
0010.00	HKF	Basic	Hook Failure	2.00E-09	Point Estimate	Under gate MECHF
0011.00	RDF	Basic	Rope Drum Failure	4.00E-08	Point Estimate	Under gate MECHF
0012.00	RDPF	Basic	Rope Drum Pedestal Failure	4.00E-08	Point Estimate	Under gate MECHF
0013.00	DGSF	Basic	Drum/Gearbox Shaft Failure	2.00E-07	Point Estimate	Under gate MECHF
0014.00	DGCF	Basic	Drum/Gearbox Coupling Failure	8.00E-07	Point Estimate	Under gate MECHF
0015.00	BKF	Basic	Brake Failure	1.00E-05	Point Estimate	Under gate MECHF
0016.00	RSF	Basic	Rope System Failure	4.00E-06	Point Estimate	Under gate MECHF
0017.00	GBF	Basic	Gearbox Failure	1.00E-06	Point Estimate	Under gate MECHF
0018.00	GBSF	Basic	Gearbox Brake Failure	2.00E-07	Point Estimate	Under gate MECHF

Figure 6-7. Example Fault Tree Table Showing Fault Tree Analysis Results Summarized

The Copy Record button will copy the entire information and add. Delete Record will purge the information. The fault tree is analyzed in the tool using the SAPHIRE code. SAPHIRE is a standalone Windows based software where the model development and analysis will be carried out independently based on the information developed under the event scenario.

6.2.3 Human Reliability Tree Analysis

The human reliability tree would be used for a sequence of human actions in which recovery activities are significant. The human reliability tree could be performed manually, according to the Technique for Human Error Rate Prediction methodology; alternatively, it could be represented by an event tree in the SAPHIRE code. The tool graphical user interface to develop scenario data for a human reliability tree will be developed in the next version of the tool.

6.2.4 Event Sequences

The results from the event tree analysis from the SAPHIRE code are stored in the database using the Event Sequence submenu located under the Freq. Analysis menu. The Event Sequence menu leads to a Form and Table submenu. As shown in Figure 6-8, the Form submenu displays the Event Sequence Form dialog box which guides the user input on event sequences into the database. The user first selects the Scenario ID from the drop-down list which shows a list of all the scenarios ID in the functional area. Upon selecting an event scenario, the details on an associated initiating event is displayed. The user can enter data on the event sequence with the Add Record button. The fields available for entering the information on event sequence are Event Sequence ID, Event Seq. Frequency, Description, End State, Additional Information, and Saphire Data Location. A unique event sequence identification should be provided using any combination of alphanumeric characters. Event sequence frequency from the event tree analysis either based on a point estimate or uncertainty analysis conducted in the SAPHIRE code is entered in the Event Seq. Frequency field. If the SAPHIRE analysis is based on uncertainty analysis, then mean frequency should be entered. In addition, a description of the event sequence, end state, additional information, and directory and path for the event tree analysis data from the SAPHIRE analysis are entered in their respective field. The end state defines the possible radioactive release scenarios qualitatively, for example, low, high, and moderate. Each event sequence for a given event scenario should be entered by selecting event scenario from the drop-drown list under Scenario ID. This information in this form propagates to the Results table under the Performance menu.

Information in this form can be edited and deleted using the Delete Record and Edit Record buttons at the bottom. The Event Seq. Table button, as shown in Figure 6-9, will display a dialog box with a table view showing information on event sequences in a tabular manner. Data can be further edited from this form. The tool generates a report on the event scenario using the Show Report button. The Event Sequence Form and Event Sequence table also show the category of the event sequence. The category is evaluated based on 10 CFR Part 63 definitions as stated in Section 2.1.

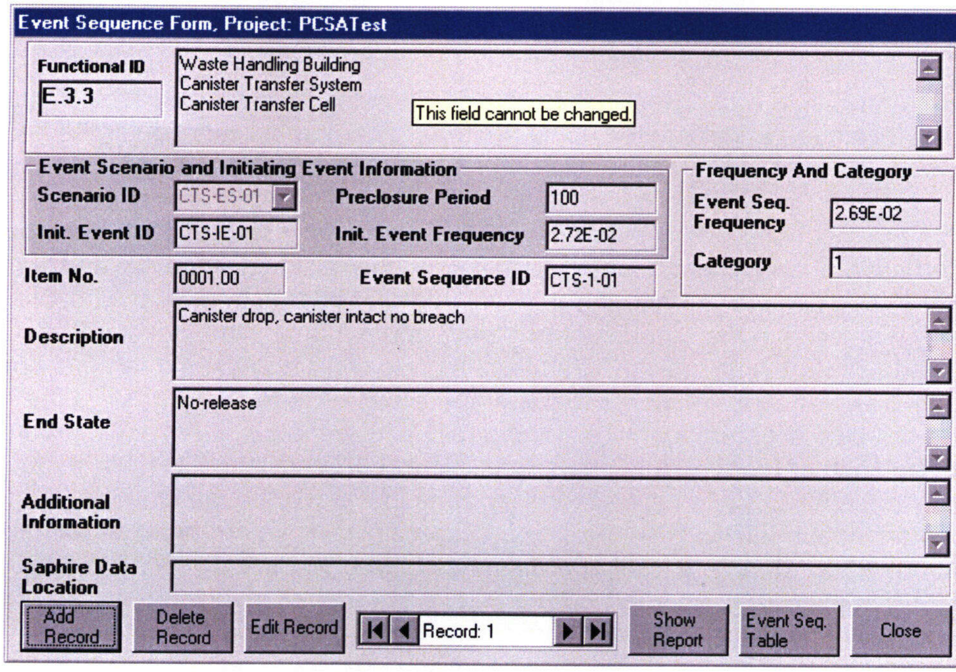
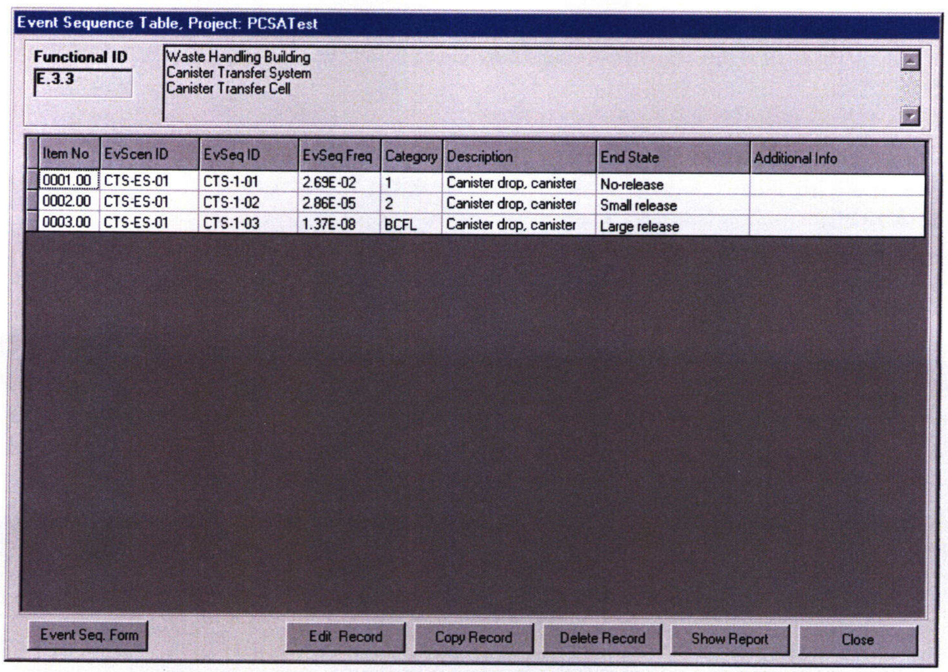


Figure 6-8. Example Event Sequence Form



Item No	EvScen ID	EvSeq ID	EvSeq Freq	Category	Description	End State	Additional Info
0001.00	CTS-ES-01	CTS-1-01	2.69E-02	1	Canister drop, canister	No-release	
0002.00	CTS-ES-01	CTS-1-02	2.86E-05	2	Canister drop, canister	Small release	
0003.00	CTS-ES-01	CTS-1-03	1.37E-08	BCFL	Canister drop, canister	Large release	

Figure 6-9. Example Event Sequence Table

6.3 Example Problem

An event scenario involving a canister drop from a crane in the canister transfer cell, functional area E.3.3, was developed and modeled using the tool. The primary function in the canister transfer cell, which is a part of the canister transfer system, is to move the canisters out of the transportation cask into the disposable containers. The operations in the canister transfer cell are illustrated in the mechanical flow diagram in Figure 3-10. The sequence of operations and equipment used have already been developed based on the facility description and surface facility operations (see Chapter 3), and the relevant information required for preclosure safety analysis has been entered in the database from the System menu. The canister transfer cell area is a shielded structure with 1.5-m [5-ft] thick concrete walls and uses a remotely operated overhead bridge crane and other fixtures to transfer the canisters from the cask to the disposal container. The cell also accommodates a staging rack where the canisters are temporarily stored for heat balance or for schedule operations. The DOE ventilation system layout considers functional area E.3.3 to be a secondary zone that would have high potential for radiological contamination (DOE, 2001b). The DOE preliminary hazard analysis identified canister drop on the floor during normal operations as a potential event (CRWMS M&O, 1999c). The scenario for this event was adopted from a DOE analysis that involves possible breach of a canister, with no active heating, ventilation, or air conditioning operation. In this scenario, there will be a loss of particulate confinement and radioactive particulates will escape from the Waste Handling Building (CRWMS M&O, 1998a). The initiating event for this scenario is a bridge crane failure caused by mechanical or electrical component failure of the crane. It is assumed that on drop, a canister with a weld defect will be breached and radioactive material will be released. It is also assumed that the shielded structure will perform its function and the dose to the public is mitigated by high-efficiency particulate air filter units contained in the heating, ventilation, and air conditioning system. The Event Tree form used to develop the scenario is shown in Figure 6-5.

The Event Tree form also requires frequency and probability data. The probability of the bridge crane failure that may initiate the drop was analyzed using fault tree analysis. The top event of the fault tree, the bridge crane failure, is caused by failure of mechanical components or electrical components. The fault tree model, adopted from Duke (1985), is depicted in Figure 6-10a,b. The mechanical failure of the crane may be caused by failure of 10 independent components connected by an OR gate. The electrical failure is a combination of 6 basic events connected by AND and OR gates. The failure probability per demand for all the failure modes is obtained from the Probability menu. The source of the failure data used in the analysis is Duke (1985). The probability data in the SAPHIRE code analysis were entered as a point estimate without assigning any distribution. The fault tree analysis shows the probability of the top event (i.e., bridge crane failure) to be 1.7×10^{-5} per demand. The largest contributor to the top event is the brake failure, followed by rope system failure obtained from the cutsets generated. The fault tree results are summarized in the database using the Fault Tree menu as displayed in Figure 6-7.

An event tree was modeled with an initiating event (i.e., crane failure) and two event sequences [i.e., canister breach and failure of heating, ventilation and air conditioning system]. In this analysis, the fault tree was not linked to the event tree. The frequency of crane failure per year is evaluated by multiplying the failure probability value of 1.7×10^{-5} by the rate of crane usage per year. The number of canisters handled is expected to vary every year during

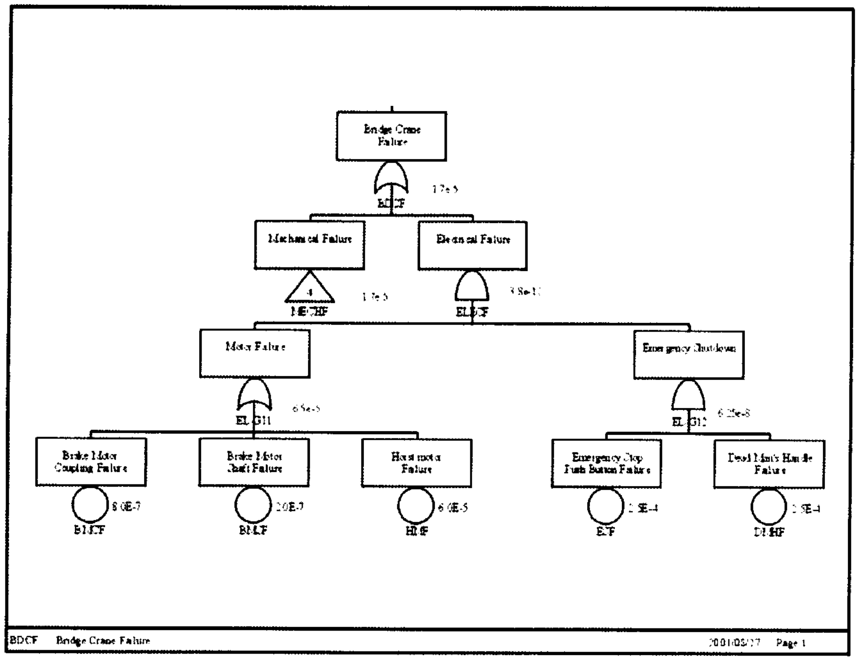


Figure 6-10(a). SAPHIRE Fault Tree Model for Bridge Crane Failure Analysis

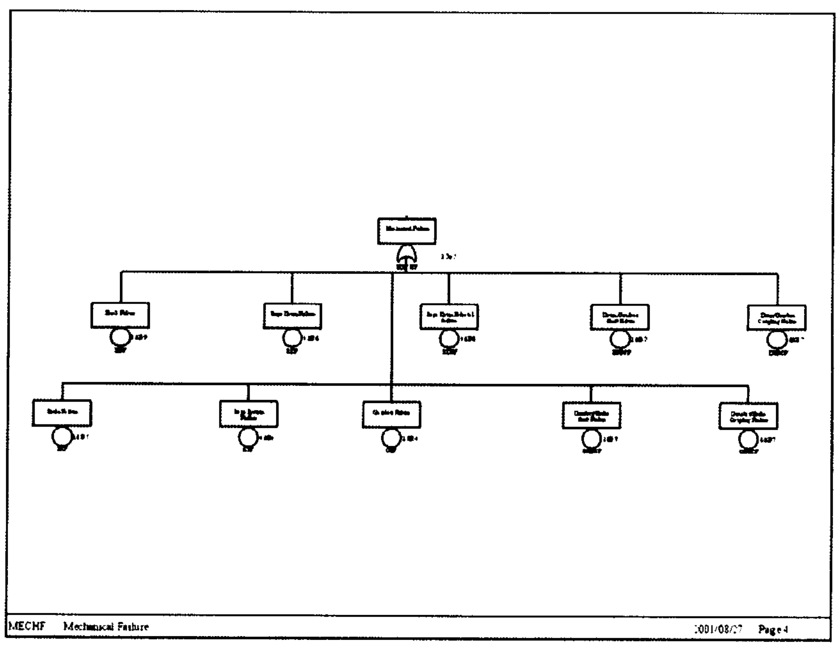


Figure 6-10(b). SAPHIRE Fault Tree Model for Bridge Crane Failure Analysis the operational period (CRWMS M&O, 1999d); however, to fulfill requirements of 10 CFR 63.21(c)(5), the maximum rate of receipt will be used in the analysis. As presented in Table 4-1, the total canisters handled in a peak year is 801. Potentially, each canister could be lifted twice, once out of the cask and placed in the staging rack and then taken out of the staging rack and placed inside the disposal container. It is recognized from the operational sequence that all canisters may not be lifted twice. The larger canisters will be transferred directly from the cask to the disposal container. Thus, the number of canisters lifted twice will be fewer than 801. For the purpose of this analysis, the number of canister lifted is assumed to be 801 and, assuming two lifts per operation, the demand on the crane would be approximately 1,602 lifts. The drop events per year (i.e., frequency of initiating event) are estimated to be 2.72×10^{-2}. The probability of a defective canister because of weld defect has been assumed to be 1.06×10^{-3}, based on DOE analysis (CRWMS M&O, 1998a). Similarly, for secondary confinement zones, the probability of heating, ventilation, and air conditioning unavailability was assumed to be 4.8×10^{-4} (CRWMS M&O, 1998a). In the recent event scenario analyses, DOE used the heating, ventilation, and air conditioning system unavailability as 1.7×10^{-7} (CRWMS M&O, 2000f). These data were not used in this analysis because DOE estimates of failure probability of heating, ventilation, and air conditioning system for the primary confinement area in (CRWMS M&O, 1999j) have not been reviewed by the staff. The probability of canister breach was assumed for illustration purposes and was not reviewed by the staff. The event tree for this event scenario is graphically displayed in Figure 6-11. The event tree generated three event sequences, the event sequence number, end state, and frequency of each event sequence from the SAPHIRE code analysis. Each event sequence can be given a unique name so that the event sequences can be easily identified. The results can be summarized as shown in Figure 6-9 using the Event Sequence form shown in Figure 6-8.

6.4 Categorization (1 and 2) of Event Sequences Based on Frequency

The DOE assumed a preclosure operational period of 100 years (DOE, 1999, 2001a). Based on their expected frequencies of occurrence, events are designated as Category 1 and Category 2 event sequences, as defined in 10 CFR 63.2. Category 1 events are those natural and human-induced event sequences that are expected to occur one or more times before permanent closure of the geologic repository operations area. The frequency of occurrence of a Category 1 event sequence is $\geq 10^{-2}$/year.

Category 2 event sequences are other natural and human-induced events that have at least 1 chance in 10,000 of occurring before permanent closure of the geologic repository. The frequency of occurrence of Category 2 events is $<10^{2}$/year, but $\geq 10^{-6}$/year. Those events that have an expected frequency of $<10^{-6}$/year are excluded from analysis.

The Category of each event sequence is evaluated based on the preclosure period assigned to each initiating event and displayed in the Event Sequence Table dialogbox, as shown in Figure 6-9. On entering the event frequency, the tool will automatically categorize the event sequences under the Category header as 1, 2, or below category frequency (BCFL) limit sequences. The event sequences are designated as below category frequency limit when the frequency of occurrence of an event sequence is less than 10^{-6}. The categories of event sequences in a functional area are also displayed in the Results table accessed from Current

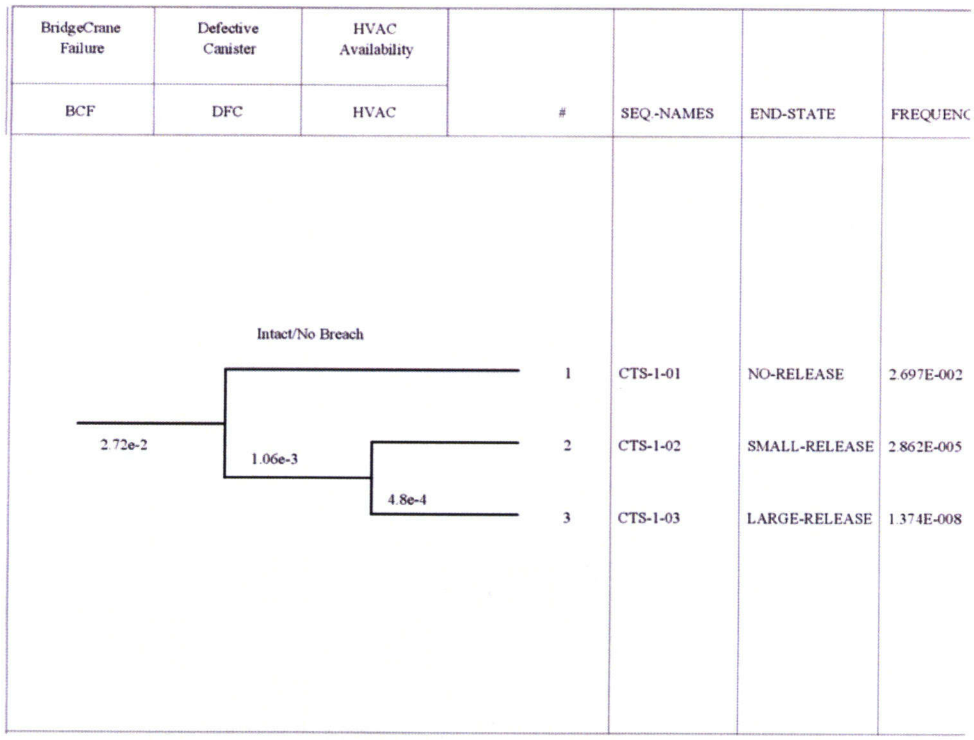


Figure 6-11. SAPHIRE Event Tree Model for Canister Drop Analysis

Level Results under the Performance menu. The Results Table form for functional area E.3.3 is shown in Figure 6-12.

The Categories of event sequences can also be seen from the Safety Analysis submenu located under Project which is invoked from the Performance menu in the main menu bar. These data are displayed under the Results Table Project View Base Case form which shows results from all the functional areas. These data, however, cannot be edited from Results Table Project View Base Case. Changes to the data can be made from the Event Sequence Form, which is active only for a selected functional area. This process will control and protect the data from being modified without sufficient reason. The Results Table Project View Base Case form allows further analysis, such as safety assessment, based on the performance objectives and importance analysis to identify the structures, systems, and components important to safety. These features of the tool are described in Chapter 8.

The DOE is also considering a low-temperature operating mode for the proposed repository (Bechtel SAIC Company, LLC, 2002; DOE, 2001a). Several options are being considered for a low temperature operating mode, some of which would extend the preclosure period to as long as 325 years. Consequently, adopting this option will change the threshold criterion for Category 1 and 2 event sequences given before. For a preclosure period of 325 years, the annual threshold frequency for Category 1 event sequences becomes 3.1×10^{-3} and for Category 2 event sequences the threshold frequency becomes 3.1×10^{-7}. Bechtel SAIC Company, LLC (2002) discussed a two-phase strategy in which Phase 1 would encompass the activities related to the surface and subsurface operations for emplacement of waste, and

Phase 2 would address the period after emplacement activities have been completed. Since DOE consideration of low-temperature facility design is in a conceptual stage, the PCSA Tool currently does not address possible changes in threshold probability.

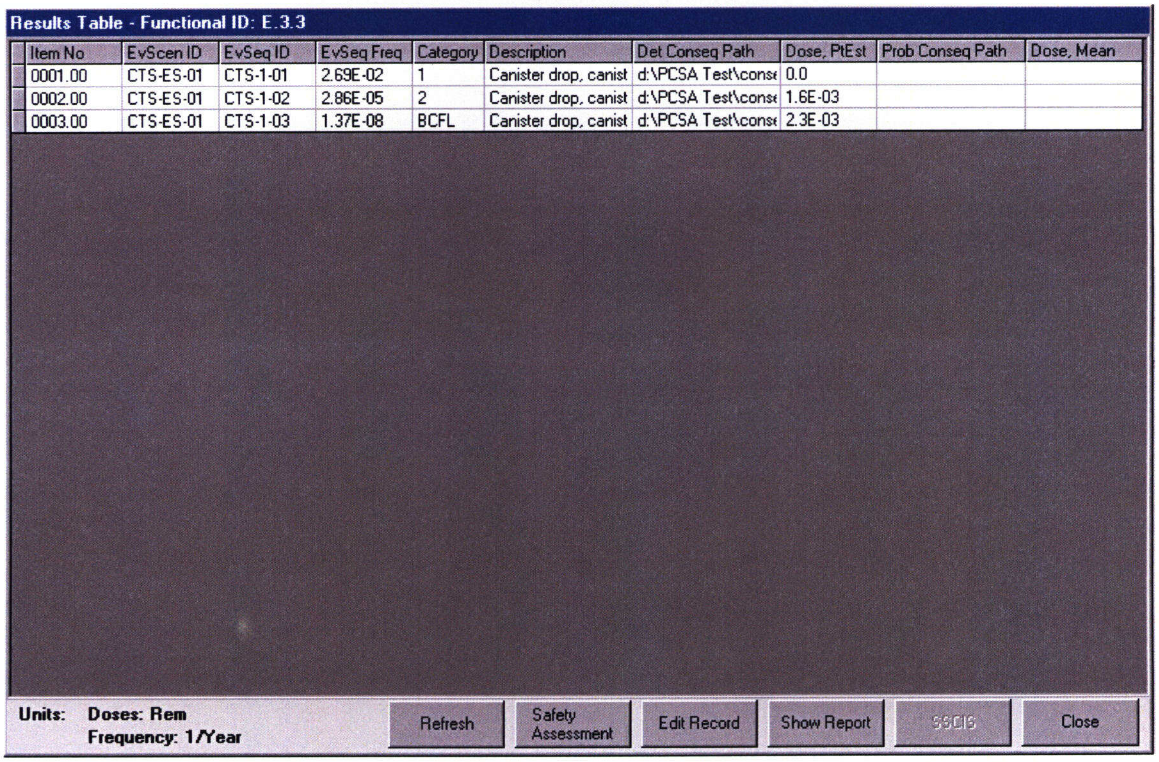


Figure 6-12. PCSA Tool Results Table Form

7 CONSEQUENCE ANALYSIS

This chapter presents the consequence analysis module of the PCSA Tool, which relates to Section 4.1.1.5, Consequence Analyses, of the Yucca Mountain Review Plan (NRC, 2002a). Except for the calculation of direct exposure, the consequence analysis module of the PCSA Tool applies to all six acceptance criteria in Sections 4.1.1.5.1.3 and 4.1.1.5.2.3 (NRC, 2002a). The three acceptance criteria in Section 4.1.1.5.1.3 are based on meeting the requirements of 10 CFR 63.111(a)(1), (a)(2), (b)(1), (c)(1), and (c)(2), relating to consequence analysis methodology and demonstration that the design meets 10 CFR Parts 20 and 63 radiation protection requirements for normal operations and Category 1 event sequences. The three acceptance criteria in Section 4.1.1.5.2.3 are based on 10 CFR 63.111(b)(2) and (c), relating to the design meeting 10 CFR Part 63 radiation protection requirements for Category 2 event sequences.

The functions of the consequence analyses are found under the Consequences menu in the toolbar highlighted in Figure 7-1. The two main calculational options for the consequence analyses are public dose and worker dose. The two codes used for the public dose calculation are RSAC Version 5.2 and MELCOR Version 1.8.5. The RSAC code was used to calculate radiological consequences to an off-site member of the public from an atmospheric release of radioactive material using deterministic and probabilistic approaches. The MELCOR code was used to estimate the building discharge fraction, which serves as an input parameter for the public dose calculation. Using published dose conversion factors (EPA, 1988), a spreadsheet calculation was incorporated into the PCSA Tool to determine the worker doses. The remainder of this chapter presents the approach, assumptions, format (including the numerical units), and parameter default values for the public and worker dose calculations. Descriptions of the functions of the dose calculations in the PCSA Tool are also provided in Sections 8.1.2, 8.1.4, and 8.2.4.

7.1 Public Dose Calculation

The consequence analysis module primarily uses the RSAC code to calculate the radiological dose to an offsite member of the public due to a release of radioactive material. The MELCOR code is not required for calculation of public dose, but can be used to determine a realistic source term. Descriptions of the deterministic and probabilistic calculations of public dose follow.

7.1.1 Deterministic Calculation of Public Dose

This section presents the approach, assumptions, format, and parameter default values for the deterministic calculation of dose to members of the public.

7.1.1.1 Approach

The consequence module of the PCSA Tool uses the RSAC Version 5.2 code to calculate radiological doses to off-site members of the public from atmospheric releases of radioactive material. The RSAC code can be obtained using the CCC–125 code package designation from the Radiation Safety Information Computation Center (Oak Ridge National Laboratory, http://www-rsicc.ornl.gov/rsic.html). Shonka Research Associates, Inc. (1993) verified and

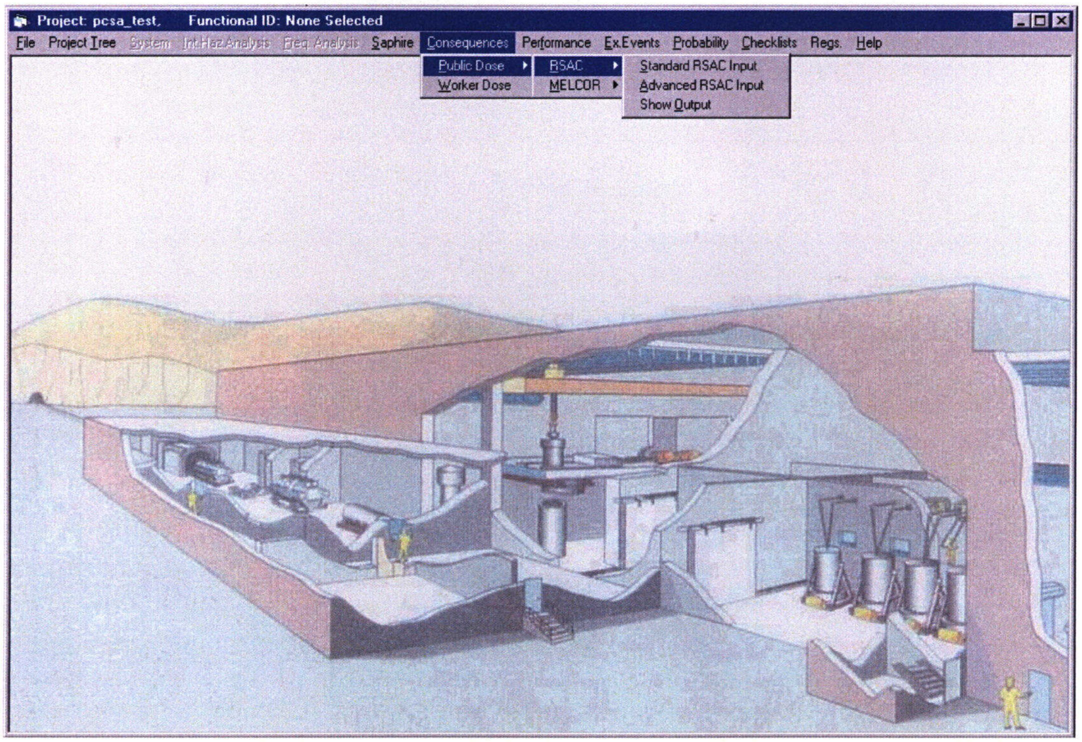


Figure 7-1. Consequence Module Menu

validated the use of RSAC code for safety-related dose calculations in accordance with ANSI/ANS–10.4 (American National Standards Institute, Inc./American Nuclear Society, 1987).

The consequence module conservatively models the breach of spent nuclear fuel assemblies as an instantaneous release of radionuclides into the room air of the Waste Handling Building. The consequence module uses the MELCOR code (Gauntt, et al., 2000) to estimate the fractional release of radionuclides transported through the Waste Handling Building and its ventilation system. The MELCOR code calculates the building discharge fractions for gases, Co-60, and particulate (i.e., the fraction of radionuclides released into the building air that are transported through the building ventilation and subsequently released into the atmosphere). The mitigation provided by high-efficiency particulate air filters is included as a separate factor. The consequence module can also calculate gaseous releases into the atmosphere from the breach of spent nuclear fuel assemblies in a pool.

The consequence analysis module currently considers the receptor to be an adult member of the public located at the closest off-site distance. The consequence analysis module calculates internal and external doses for the receptor. Internal doses can be calculated for the inhalation and ingestion pathways. External doses can be calculated for the pathways of ground surface exposure and submersion. The consequence module currently assumes that the location of the receptor is the same as the location of the receptor's local food production. Thus, caution should be used when calculating ingestion doses for a receptor whose location differs significantly from the location where the receptor's food is produced locally. To account for receptors who eat significant amounts of the contaminated, locally produced food, ingestion doses should be calculated based on the distance from the source to the farm where the food is produced.

7.1.1.2 Source Term

The two components of the source term are the radionuclides in the spent nuclear fuel and the crud on the cladding. The consequence calculations presented in this report are based on the breach of commercial spent nuclear fuel assemblies, and, therefore, the radionuclide inventories are presented as activities per assembly. Although the source term interface has been tailored to commercial spent nuclear fuel (i.e., pressurized water reactor or boiling water reactor), the consequence analysis module provides flexibility for alternative radioactive fuels and source materials through the User Specified Fuel Type option. The User Specified Fuel Type option allows manual entry of the radionuclide inventories. The consequence module not only saves the entered inventories for future use but also saves any updates made to the user-specified inventories. For those instances where interfaces of the PCSA Tool to RSAC do not contain the radionuclides desired for the source term, it is recommended that the user select the Advanced RSAC Input option and add appropriate radionuclides into the input file from the full list available for the RSAC calculations.

7.1.1.2.1 Radionuclides in the Spent Nuclear Fuel

The average pressurized water reactor and boiling water reactor fuel characteristics (CRWMS M&O, 2000f) are presented in Table 7-1. The inventory of radionuclides in the spent nuclear fuel was generated for the average fuel characteristics using the light water reactor radiological database (CRWMS M&O, 1993). The light water reactor radiological database reports radionuclide activities (curie per metric ton of uranium) for a decay time of 20 or 30 years. Because radioactive decay is described by an exponential relationship, the activity per metric ton of uranium for a specific radionuclide with a 25-year decay time was determined from the results with decay times of 20 and 30 years using the following logarithmic interpolation approach:

$$A_{25\text{-year}} = 10^{\left[\frac{\mathrm{Log}_{10}(A_{20\text{-year}})+\mathrm{Log}_{10}(A_{30\text{-year}})}{2}\right]} \qquad (7\text{-}1)$$

where

$A_{25\text{-year}}$ represents the activity per metric ton of uranium (Ci/MTU) for a decay time of 25 years

$A_{20\text{-year}}$ represents the activity per metric ton of uranium (Ci/MTU) for a decay time of 20 years

$A_{30\text{-year}}$ represents the activity per metric ton of uranium (Ci/MTU) for a decay time of 30 years

Table 7-1. Average Pressurized Water Reactor and Boiling Water Reactor Fuel Characteristics*		
Fuel Type	**Pressurized Water Reactor**	**Boiling Water Reactor**
Burnup	48,000 MWd/MTU	40,000 MWd/MTU
U-235 Enrichment	4.00 percent	3.50 percent
Decay Time	25 yr	25 yr
*CRWMS M&O. "Design Basis Event Frequency and Dose Calculation for Site Recommendation." CAL–WHS–SE–000001. Revision 01. Las Vegas, Nevada: CRWMS M&O. 2000		

For the three criticality groupings of infinite multiplication factors, the largest average values for the number of metric tons of uranium per assembly—specifically 0.429 MTU/assembly for pressurized water reactor fuel and 0.1775 MTU/assembly for boiling water reactor fuel, (CRWMS M&O, 1998b)—were used to convert the radionuclide inventories into activity per assembly. The radionuclide activities per assembly for average pressurized water reactor and boiling water reactor fuel are presented in Table 7-2.

The release fractions from breached fuel for specific radioisotopes were obtained from NUREG–1536 (NRC, 1997). For the other radionuclides, the release fractions for an impact rupture were set to their maximum values based on values in Tables 11.4 and 11.5 of NUREG–1536, namely at 2×10^{-6} for volatiles and at 0.4 for noble gases. In addition, the release fraction for solids was conservatively scaled up from 1×10^{-6} to 2×10^{-6} to match the value for volatiles. This adjustment avoided the need to determine the fraction of radionuclide inventories as volatiles and solids. The release fractions used in the source term calculation are listed by radionuclide group in Table 7-3 and assume all fuel rods involved in the event contribute to the source term. These release fractions compare well with those presented in NUREG–1567 (NRC, 2000a) for off-normal conditions. In general, the release fractions in Table 7-3 are greater than those presented in NUREG–1567 for off-normal conditions, except for ruthenium and fuel fines, whose release fractions are lower by factors of 1.3 and 1.5, respectively.

The source term calculation considers radionuclides with released activities from breached fuel that were greater than 185 Bq/MTU [5.00×10^{-9} Ci/MTU]. It is important to note that 13 isotopes, with released activities greater than 185 Bq/MTU [5.00×10^{-9} Ci/MTU], were not contained in the RSAC radionuclide database. These 13 radionuclides (Kr-81, Rh-102, Ag-108m, Cd-113m, Pm-146, Ho-166m, Po-212, Np-238, Am-242, Am-242m, Cm-242, Cm-243, and Cm-244) accounted for less than 0.0001 percent of the released activity and were not expected to make significant contributions to the calculated doses, except for Cm–244. Because the committed dose equivalent per unit intakes (Sv/Bq) for inhalation and ingestion tends to be large for the curium isotopes relative to the other radionuclides in spent nuclear fuel, the curium isotopes can contribute significantly to the inhalation and ingestion doses from releases of spent nuclear fuel. For both average pressurized water reactor and boiling water reactor spent nuclear fuel, Cm-244 accounts for more than 98 percent of the activity from the

Table 7-2. Average Radionuclide Inventories of Spent Nuclear Fuel from Pressurized Water and Boiling Water Reactors Aged 25 Years. The Inventories in Fuel Values Were Determined for the Fuel Characteristics Shown in Table 7-1 Using the Light Water Reactor Radiological Database*				
	Average Pressurized Water Reactor		Average Boiling Water Reactor	
Radionuclide	Bq/Assembly	Ci/Assembly	Bq/Assembly	Ci/Assembly
H-3	4.07×10^{12}	1.10×10^{2}	1.57×10^{12}	4.25×10^{1}
C-14	2.65×10^{10}	7.17×10^{-1}	1.23×10^{10}	3.32×10^{-1}
Cl-36	2.20×10^{8}	5.93×10^{-3}	8.64×10^{7}	2.34×10^{-3}
Ar-39	1.25×10^{6}	3.39×10^{-5}	5.33×10^{5}	1.44×10^{-5}
Fe-55	7.91×10^{10}	2.14×10^{0}	2.01×10^{10}	5.42×10^{-1}
Ni-59	5.21×10^{10}	1.41×10^{0}	1.39×10^{10}	3.76×10^{-1}
Co-60	6.50×10^{12}	1.76×10^{2}	1.99×10^{12}	5.39×10^{1}
No-63	7.31×10^{12}	1.98×10^{2}	1.83×10^{12}	4.94×10^{1}
Se-79	9.32×10^{9}	2.52×10^{-1}	3.52×10^{9}	9.51×10^{-2}
Kr-85	3.94×10^{13}	1.06×10^{3}	1.42×10^{13}	3.83×10^{2}
Y-90	8.76×10^{14}	2.37×10^{4}	3.18×10^{14}	8.61×10^{3}
Sr-90	8.76×10^{14}	2.37×10^{4}	3.18×10^{14}	8.60×10^{3}
Zr-93	4.73×10^{10}	1.28×10^{0}	2.12×10^{10}	5.74×10^{-1}
Mo-93	4.40×10^{8}	1.19×10^{-2}	6.29×10^{6}	1.70×10^{-4}
Nb-93m	3.33×10^{10}	9.01×10^{-1}	1.51×10^{10}	4.07×10^{-1}
Nb-94	2.39×10^{10}	6.45×10^{-1}	8.84×10^{8}	2.39×10^{-2}
Tc-99	2.87×10^{11}	7.74×10^{0}	1.09×10^{11}	2.95×10^{0}
Ru-106	3.44×10^{8}	9.29×10^{-3}	1.25×10^{8}	3.38×10^{-3}
Rh-106	3.44×10^{8}	9.29×10^{-3}	1.25×10^{8}	3.38×10^{-3}
Pd-107	2.74×10^{9}	7.39×10^{-2}	1.13×10^{9}	3.06×10^{-2}

Table 7-2. Average Radionuclide Inventories of Spent Nuclear Fuel from Pressurized Water and Boiling Water Reactors Aged 25 Years. The Inventories in Fuel Values Were Determined for the Fuel Characteristics Shown in Table 7-1 Using the Light Water Reactor Radiological Database.* (continued)

	Average Pressurized Water Reactor		Average Boiling Water Reactor	
Radionuclide	Bq/Assembly	Ci/Assembly	Bq/Assembly	Ci/Assembly
Sn-121m	1.32×10^{10}	3.57×10^{-1}	1.01×10^{10}	2.73×10^{-1}
Te-125m	1.52×10^{11}	4.11×10^{0}	6.40×10^{10}	1.73×10^{0}
Sb-125	6.23×10^{11}	1.68×10^{1}	2.63×10^{11}	7.10×10^{0}
Sn-126	1.83×10^{10}	4.93×10^{-1}	7.17×10^{9}	1.94×10^{-1}
Sb-126	2.56×10^{9}	6.91×10^{-2}	1.00×10^{9}	2.71×10^{-2}
Sb-126m	1.83×10^{10}	4.93×10^{-1}	7.17×10^{9}	1.94×10^{-1}
I-129	7.21×10^{8}	1.95×10^{-2}	2.82×10^{8}	7.61×10^{-3}
Cs-134	1.02×10^{12}	2.75×10^{1}	3.88×10^{11}	1.05×10^{1}
Cs-135	1.08×10^{10}	2.92×10^{-1}	5.05×10^{9}	1.37×10^{-1}
Cs-137	1.31×10^{15}	3.55×10^{4}	4.96×10^{14}	1.34×10^{4}
Ba-137m	1.24×10^{15}	3.36×10^{4}	4.70×10^{14}	1.27×10^{4}
Pm-147	2.68×10^{12}	7.23×10^{1}	9.74×10^{11}	2.63×10^{1}
Sm-147	8.29×10^{4}	2.24×10^{-6}	3.22×10^{4}	8.70×10^{-7}
Sm-151	7.02×10^{12}	1.90×10^{2}	2.97×10^{12}	8.02×10^{1}
Eu-152	4.52×10^{10}	1.22×10^{0}	2.36×10^{10}	6.38×10^{-1}
Eu-154	3.61×10^{13}	9.76×10^{2}	1.43×10^{13}	3.86×10^{2}
Eu-155	5.52×10^{12}	1.49×10^{2}	2.30×10^{12}	6.22×10^{1}
Tl-208	3.65×10^{8}	9.85×10^{-3}	1.54×10^{8}	4.16×10^{-3}
Pb-212	1.01×10^{9}	2.74×10^{-2}	4.29×10^{8}	1.16×10^{-2}
BI-212	1.01×10^{9}	2.74×10^{-2}	4.29×10^{8}	1.16×10^{-2}

Table 7-2. Averaged Radionuclide Inventories of Spent Nuclear Fuel from Pressurized Water and Boiling Water Reactors Aged 25 Years. The Inventories in Fuel Values Were Determined for the Fuel Characteristics Shown in Table 7-1 Using the Light Water Reactor Radiological Database.* (continued)				
	Average Pressurized Water Reactor		Average Boiling Water Reactor	
Radionuclide	Bq/Assembly	Ci/Assembly	Bq/Assembly	Ci/Assembly
Po-216	1.01×10^{9}	2.74×10^{-2}	4.29×10^{8}	1.16×10^{-2}
Rn-219	3.04×10^{5}	8.23×10^{-6}	1.42×10^{5}	3.83×10^{-6}
Rn-220	1.01×10^{9}	2.74×10^{-2}	4.29×10^{8}	1.16×10^{-2}
Rn-222	3.06×10^{4}	8.28×10^{-7}	1.19×10^{4}	3.22×10^{-7}
Ra-224	1.01×10^{9}	2.74×10^{-2}	4.29×10^{8}	1.16×10^{-2}
Th-228	1.01×10^{9}	2.74×10^{-2}	4.28×10^{8}	1.16×10^{-2}
Th-231	2.26×10^{8}	6.12×10^{-3}	9.00×10^{7}	2.43×10^{-3}
U-232	9.93×10^{8}	2.68×10^{-2}	4.19×10^{8}	1.13×10^{-2}
Pa-233	1.01×10^{10}	2.73×10^{-1}	3.81×10^{9}	1.03×10^{-1}
U-234	2.40×10^{10}	6.49×10^{-1}	9.14×10^{9}	2.47×10^{-1}
Th-234	4.94×10^{9}	1.33×10^{-1}	2.05×10^{9}	5.55×10^{-2}
Pa-234m	4.94×10^{9}	1.33×10^{-1}	2.05×10^{9}	5.55×10^{-2}
U-235	2.27×10^{8}	6.12×10^{-3}	9.00×10^{7}	2.43×10^{-3}
U-236	5.36×10^{9}	1.45×10^{-1}	1.96×10^{9}	5.30×10^{-2}
Pu-236	4.74×10^{7}	1.28×10^{-3}	1.85×10^{7}	5.00×10^{-4}
U-237	1.92×10^{10}	5.18×10^{-1}	8.45×10^{9}	2.28×10^{-1}
Np-237	1.01×10^{10}	2.73×10^{-1}	3.81×10^{9}	1.03×10^{-1}
Pu-238	8.82×10^{13}	2.38×10^{3}	3.81×10^{13}	1.03×10^{3}
U-238	4.94×10^{9}	1.33×10^{-1}	2.05×10^{9}	5.55×10^{-2}
Pu-239	6.72×10^{12}	1.82×10^{2}	2.54×10^{12}	6.86×10^{1}

Table 7-2. Averaged Radionuclide Inventories of Spent Nuclear Fuel from Pressurized Water and Boiling Water Reactors Aged 25 Years. The Inventories in Fuel Values Were Determined for the Fuel Characteristics Shown in Table 7-1 Using the Light Water Reactor Radiological Database.* (continued)				
	Average Pressurized Water Reactor		Average Boiling Water Reactor	
Radionuclide	Bq/Assembly	Ci/Assembly	Bq/Assembly	Ci/Assembly
Np-239	6.37×10^{11}	1.72×10^{1}	3.06×10^{11}	8.27×10^{0}
Pu-240	1.14×10^{13}	3.08×10^{2}	4.22×10^{12}	1.14×10^{2}
Pu-241	7.82×10^{14}	2.11×10^{4}	3.44×10^{14}	9.31×10^{3}
Am-241	6.17×10^{13}	1.67×10^{3}	2.74×10^{13}	7.40×10^{2}
Pu-242	4.25×10^{10}	1.15×10^{0}	1.88×10^{10}	5.07×10^{-1}
Am-243	6.37×10^{11}	1.72×10^{1}	3.06×10^{11}	8.27×10^{0}
Cm-245	1.34×10^{10}	3.63×10^{-1}	7.97×10^{9}	2.15×10^{-1}
Cm-246 + Cm-244†	2.60×10^{13}	7.03×10^{2}	1.38×10^{13}	3.72×10^{2}

*CRWMS M&O. "Light Water Characteristics Database. LWR Radiological Module, Version 1.1." CSCIA000000000–02268–1200–20002. Las Vegas, Nevada: CRWMS M&O. 1993.
†Refer to description in Section 8.1.1.2.1 on how the Cm-244 activity was included.

Table 7-3. Radionuclide Release Fractions by Radionuclide Group. The Release Fractions Are Based on Guidance.*	
Radionuclide Group	Release Fraction
H-3	3.0×10^{-1}
Co-60 crud	1.5×10^{-1}
Strontium	2.3×10^{-5}
Ruthenium	1.5×10^{-5}
Iodine	1.0×10^{-1}
Cesium	2.3×10^{-5}
Noble gases	4.0×10^{-1}
Other particulates and fuel fines	2×10^{-6}

*NRC. NUREG–1536, "Standard Review Plan for Dry Cask Storage Systems." Washington, DC: NRC. January 1997.

curium isotopes and was included in the RSAC calculations under Cm-246. The committed dose equivalent per unit intake via inhalation for Cm-246 is 1.22×10^{-4} Sv/Bq [4.51×10^{8} rem/Ci] and for Cm-244 is 6.70×10^{-5} Sv/Bq [2.48×10^{8} rem/Ci], with a ratio of 1.82. The committed dose equivalent per unit intake (Sv/Bq) via ingestion for Cm-246 is 1.00×10^{-6} Sv/Bq [3.70×10^{6} rem/Ci] and for Cm-244 is 5.45×10^{-7} Sv/Bq [2.02×10^{-6} rem/Ci], with a ratio of 1.83. Cm-244 was included in the RSAC code calculation by dividing the Cm-244 activity by a factor of 1.825 and adding the result to the activity for Cm-246. In other words, the inventory for Cm-246 in Table 7-1 has been modified to represent the contributions from Cm-244 and Cm-246. The modified inventories for Cm-246 became 703 and 372 Ci per assembly for average pressurized water reactor and boiling water reactor fuel, respectively.

Except for Co-60, the radionuclide activity in curies released into the environment from the event was calculated from the following expression:

$$A_{rel} = A_{fuel} \times N \times RF \times F_{vent} \times MF \tag{7-2}$$

where A_{rel} represents the radionuclide activity released from the Waste Handling Building (Ci); A_{fuel} represents the radionuclide inventory in the fuel (Ci/assembly); N represents the number of spent nuclear fuel assemblies ruptured in the event (assembly); RF represents the fraction of the radionuclide activity released from the spent nuclear fuel assembly (unitless); F_{vent} represents the fraction of radionuclide activity released from the event into the air that enters the building ventilation and is released into the atmosphere (unitless), called the building discharge fraction, and MF represents the mitigation factor for the high-efficiency particulate air filter (unitless). The MELCOR computer code (Gauntt, et al., 2000) estimated F_{vent} for 25 hours following the breach as 0.2 for gases, 0.01 for crud, and 0.002 for particulates. To account for larger fractional discharges of gases for a long time period, F_{vent} was assigned default values 1.0 for gases, 0.01 for crud, and 0.002 for particulates for incorporation into the PCSA Tool. The efficiency of the high-efficiency particulate air filters was assumed to be 99.97 percent for particulates (Oak Ridge national Laboratory, 1976), which led to a default value of 3×10^{-4} for MF that was applied to crud and particulates. An MF value of one was applied to noble gases, tritium, and iodine.

7.1.1.2.2 Co-60 Crud on the Fuel Cladding

A separate RSAC dose computation considered doses from Co-60 crud on the cladding. The amount of Co-60 crud on the pressurized water reactor fuel cladding was determined from NUREG/CR–6487 (Anderson, et al., 1996) by multiplying the Co-60 activity per unit area {1.4×10^{-4} Ci/cm^2 [5.18×10^{6} Bq/cm^2]} with the bounding estimate of the surface area per assembly (449,003 cm^2/assembly) (CRWMS M&O, 2000f). Similarly, the amount of Co-60 crud on the boiling water reactor fuel cladding was determined by multiplying the Co-60 activity per unit area of {1.254×10^{-3} Ci/cm^2 [4.64×10^{7} Bq/cm^2]} (Anderson, et al., 1996) with the bounding estimate of the surface area per assembly (168,148 cm^2/assembly) (CRWMS M&O, 2000f). The NUREG/CR–6487 data were based on spent nuclear fuel with a burnup of 33,000 MWd/MTU, a U-235 enrichment of 3.2 percent, and a decay time of 5 years. Differences in enrichment were assumed not to impact the Co-60 crud calculation. A scaling factor for the crud activity was, however, calculated to account for differences in the burnup and decay times compared to the average pressurized water reactor and boiling water reactor fuel characteristics with a total decay time of 25 years (i.e., an additional 20 years of decay were calculated):

$$SA_{crud,25year} = SA_{crud,5year} \times \frac{B}{33\ \text{GWd/MTU}} \times e^{-\left[\frac{\ln 2 \times (20\text{year})}{5.263\text{year}}\right]} \tag{7-3}$$

where $SA_{crud,25year}$ represents the Co-60 crud activity per unit surface area (Ci/cm^2) for a decay time of 25 years, $SA_{crud,5year}$ represents the Co-60 crud activity per unit surface area (Ci/cm^2) for a decay time of 5 years, and B represents the spent nuclear fuel burnup (GWd/MTU).

Based on the activity and surface area data for pressurized water reactor and boiling water reactor fuel, the Co-60 crud activities for the average fuel characteristics in Table 7-1 were calculated using Eq. (7-3), which resulted in a Co-60 crud inventory of 2.43×10^{11} Bq [6.57 Ci] per pressurized water reactor assembly and 6.81×10^{11} Bq [18.4 Ci] per boiling water reactor assembly.

The total Co-60 activity, in the fuel and as crud, released in curies into the environment from the event was calculated from the following expression:

$$A_{rel,\,^{60}Co} = N \times \left(A_{fuel} \times RF_{fuel} + A_{crud} \times RF_{crud}\right) \times F_{vent} \times MF \tag{7-4}$$

where RF_{fuel} represents the release fraction for the Co-60 in fuel (unitless), A_{crud} represents the radionuclide inventory in the fuel (Ci/assembly), and RF_{crud} represents the release fraction for the Co-60 in crud (unitless). As stated in NUREG–1536 (NRC, 1997), a release fraction of 0.15 for the Co-60 crud was used as RF_{crud} in the calculation of the total released activity of Co-60.

7.1.1.2.3 Incorporation of MELCOR Simulations

MELCOR is a sophisticated U.S. Nuclear Regulatory Commission (NRC) accident analysis code (Gauntt, et al., 2000). Typically, consequence analyses for members of the public use an initial and overly conservative assumption that all of the radioactive material released from a spent nuclear fuel handling accident is carried out of the building by the ventilation system. By using MELCOR to model the aerosol dynamics (e.g., gravitational settling and agglomeration), a realistic source term was developed for calculations of the dose to off-site members of the public. Ultimately, the MELCOR simulations estimate the F_{vent} term in Eqs. (7-2) and (7-4) for gases, crud, and particulates at a user-specified time after the event.

A custom MELCOR simulation was designed for the breach of spent nuclear fuel assemblies in the room air of the Waste Handling Building. The MELCOR simulation consisted of a single control volume divided into three horizontal layers (lower, middle, and upper). The room dimensions and thicknesses of the horizontal layers are user-specified. A ventilation duct was placed in the control volume to flow a user-specified amount of air out of the control volume and into the environment. The inlet of the ventilation duct was placed at a user-specified height in the middle or upper layer. The user also specifies (i) initial conditions (i.e., temperature, pressure, relative humidity, and dew point) of the control volume and environment; (ii) the simulation run time; and (iii) parameters on particle size and density. Table 7-4 displays the

MELCOR simulation and control volume input parameters and their default values. To simulate a release of radioactive material into the room air from the breach of spent nuclear fuel assemblies, radionuclides are released as aerosols or vapors into the middle layer, and the remaining fuel assembly debris is uniformly distributed in the lower layer. MELCOR tracks the transport of mass as groups consisting of isotopes with the same chemical behavior. MELCOR required a source term consistent with its radionuclide groups. Therefore, a grouped source term was calculated as the released mass of a radionuclide group for a single fuel assembly of average pressurized water reactor or boiling water reactor characteristics in Table 8-1. In addition to the user's selection of the fuel type (i.e., pressurized water reactor and boiling water reactor) and the number of assemblies breached, Table 7-5a,b presents the MELCOR source term inputs and their default values. For the MELCOR simulations, this normalized source term was scaled by the user-specified number of spent nuclear fuel assemblies breached to yield the released source mass for each radionuclide group.

MELCOR also uses particle size distributions to characterize the particulate source term. Reference particle size distributions for released spent nuclear fuel fines and particulates from an impact rupture and for crud were obtained (CRWMS M&O, 1999h) and are presented in Table 7-6. Large particle sizes were assumed for the assembly debris. Particle size distributions are not required for vapor sources. Table 7-6 highlights the MELCOR particle size distribution inputs and their default values.

The decay heat from the released spent nuclear fuel particulates, fines, and gases as well as from the assembly debris were included in the MELCOR simulation. Because radionuclide groups are used by MELCOR, the decay heat from individual radionuclides was converted into a decay heat power per unit group mass. Table 7-7 displays the MELCOR decay heat inputs and the default decay heat powers for average pressurized water reactor and boiling water reactor spent nuclear fuel characteristics provided in Table 7-1.

7.1.1.3 Input Parameters and Assumptions

The released radionuclide activities serve as the source term input to the RSAC calculation of the dose to an off-site member of the public. In addition to the radionuclide inventories presented in the previous section, the RSAC code requires inputs for the (i) meteorological data, (ii) inhalation dose calculation, (iii) ingestion dose calculation, (iv) ground surface dose calculation, and (v) submersion dose calculation. These five input series are presented in the following subsections. Those parameters requiring specific user inputs or involving site-specific information are discussed in the following sections. Where site-specific data were not available, the RSAC default values are thought to be reasonably conservative and appropriate for the Yucca Mountain site. The RSAC and its default weather data were stated to be applicable to other high, flat desert terrains such as the Nevada Test Site (Shonka Research Associates, Inc., 1993).

7.1.1.3.1 Meteorological Data

The meteorological data input parameters and their default values are displayed in Table 7-8. Although the Waste Handling Building design has not been finalized, a 40-m [130-ft] stack

Table 7-4. MELCOR Simulation and Control Volume Input Parameters and Default Values for the PCSA Tool	
Input Parameter	**PCSA Tool Default Value**
Room length	10 m [32.8 ft]
Room width	13.4 m [44.0 ft]
Room height	15.24 m [50.0 ft]
Indoor atmospheric pressure	1.013×10^5 Pa [14.7 psi]
Indoor relative humidity	0.5
Indoor temperature	300 K [80 °F]
Height of lower/middle layer interface	0.5 m [1.6 ft]
Height of middle/upper layer interface	15.0 m [49.2 ft]
Outdoor atmospheric pressure	1.013×10^5 Pa [14.7 psi]
Outdoor temperature	300 K [80 °F]
Outdoor dew point temperature	280 K [44 °F]
Height of ventilation inlet	4.0 m [13.1 ft]
Stack height, ventilation outlet	40.0 m [131 ft]
Ventilation inlet area	1.0 m^2 [10.8 ft^2]
Ventilation volumetric flow rate	14.16 m^3/s [500 ft^3/s]
Ventilation maximum pressure head	312.7 Pa [0.0453 psi]
Volumetric flow rate at zero pressure head	14.16 m^3/s [500 ft^3/s]
Volumetric flow rate at maximum pressure head	5.0 m^3/s [177 ft^3/s]
Minimum particle size	1.00×10^{-8} m [3.94×10^{-7} in]
Maximum particle size	1.00×10^{-2} m [0.394 in]
Nominal particle density	1000.0 kg/m^3 [62.4 lb/ft^3]
Initial time step	0.1 s
Run time	9000 s

Table 7-5. MELCOR Source Term Input (a) Radionuclides Released into the Room Air from the Spent Nuclear Fuel or Cladding and (b) Remaining Radionuclides in Assembly Debris Not Released into the Room Air (a).

MELCOR Radionuclide Group	Group Mass Released				Elements in Group
	Pressurized Water Reactor		Boiling Water Reactor		
	kg/assembly	lb/assembly	kg/assembly	lb/assembly	
Noble Gases	1.41×10^{0}	3.10×10^{0}	5.30×10^{-1}	1.17×10^{0}	H, He, N, Ne, Ar, Kr, Xe, Rn
Alkali Metals	3.55×10^{-5}	7.84×10^{-5}	1.39×10^{-5}	3.07×10^{-5}	Li, Na, K, Cu, Rb, Cs, Fr
Alkaline Earths	3.90×10^{-5}	8.60×10^{-5}	1.48×10^{-5}	3.27×10^{-5}	Be, Mg, Ca, Sr, Ba, Ra
Halogens	1.64×10^{-2}	3.62×10^{-2}	6.41×10^{-3}	1.41×10^{-2}	F, Cl, Br, I, At
Chalcogens	5.81×10^{0}	1.28×10^{1}	2.41×10^{0}	5.31×10^{0}	O, S, Se, Te, Po
Plantinoids	1.09×10^{-4}	2.40×10^{-4}	5.87×10^{-5}	1.29×10^{-4}	Ru, Rh, Pd, Re, Os, Ir, Pt, Ni
Early Transition Elements	2.35×10^{-4}	5.18×10^{-4}	1.30×10^{-3}	2.88×10^{-3}	V, Cr, Mn, Fe, Co, Nb, Mo, Tc, Ta, W
Tetravalents	2.34×10^{-4}	5.16×10^{-4}	1.93×10^{-4}	4.25×10^{-4}	C, Ti, Zr, Ce, Hf, Th, Pa, Np, Pu
Trivalents	1.11×10^{-5}	2.45×10^{-5}	4.89×10^{-6}	1.08×10^{-5}	Al, Sc, Y, La, Pr, Nd, Pm, Sm, Eu, Gd, Tb, Dy, Ho, Er, Tm, Yb, Lu, Ac, Am, Cm, Bk, Cf
Uranium	8.04×10^{-4}	1.77×10^{-3}	3.34×10^{-4}	7.37×10^{-4}	U
More Volatile Main Group	2.46×10^{-7}	5.42×10^{-7}	1.03×10^{-7}	2.26×10^{-7}	Zn, As, Cd, Sb, Tl, Pb, Bi
Less Volatile Main Group	3.73×10^{-6}	8.24×10^{-6}	3.12×10^{-6}	6.87×10^{-6}	Ga, Ge, Ag, In, Sn
Boron Group	4.84×10^{-7}	1.07×10^{-6}	1.74×10^{-7}	3.83×10^{-7}	B, Si, P

(b)

Radionuclide Group	Mass Not Released				Elements in Group
	Pressurized Water Reactor		Boiling Water Reactor		
	Kg/assembly	lb/assembly	Kg/assembly	lb/assembly	
Remaining Assembly Debris	6.18×10^{2}	1.36×10^{3}	3.06×10^{2}	6.75×10^{2}	all elements retained in the breached assembly debris

Table 7-6. MELCOR Particle Size Distribution Input

Particle Type	Mean Mass Diameter	Geometric Standard Deviation
Released spent nuclear fuel	1.80×10^{-2} m [0.709 in]	8.18
Released crud	9.70×10^{-6} m [3.82×10^{-4} in]	1.87
Remaining assembly debris	5.00×10^{-2} m [1.97 in]	0.10

Table 7-7. MELCOR Decay Heat Input

MELCOR Radionuclide Group	Major Decay Heat Contributors in 25-Year Aged Average Spent Nuclear Fuel	Decay Heat Power Per Unit Group Mass			
		Pressurized Water Reactor		Boiling Water Reactor	
		W/Kg	Btu/hr lb	W/Kg	Btu/hr lb
Noble Gases	Kr	4.53×10^{-1}	7.01×10^{-1}	4.34×10^{-1}	6.72×10^{-1}
Alkali Metals	Cs	2.56×10^{1}	3.96×10^{1}	2.47×10^{1}	3.82×10^{1}
Alkaline Earths	Sr, Ba	9.40×10^{1}	1.45×10^{2}	9.27×10^{1}	1.43×10^{2}
Early Transition Elements	Co	1.44×10^{-1}	2.23×10^{-2}	1.03×10^{1}	1.59×10^{1}
Tetravalent	Pu	8.10×10^{-1}	1.25×10^{0}	4.16×10^{-1}	6.44×10^{-1}
Trivalents	Y, Eu, Am, Cm	4.37×10^{1}	6.76×10^{1}	4.11×10^{1}	6.36×10^{1}
More Volatile Main Group	Sb	4.27×10^{-1}	6.61×10^{-1}	4.32×10^{-1}	6.68×10^{-1}
Remaining Assembly Debris	Sum of all groups	8.78×10^{-1}	1.36×10^{0}	7.11×10^{-1}	1.10×10^{0}

Table 7-8. Meteorological Data Input for the RSAC Code		
Input Parameter	**PCSA Tool Default Value**	**Remarks**
Average wind velocity	3 m/s [7 mi/hr]	Most-probable velocity (site-specific estimate)
Stack release height	40 m [130 ft]	Estimation of stack height
Mixing depth	1,420 m [4,660 ft]	Average mixing height based data from Desert Rock, Nevada*
Air density	1.29×10^3 g/m^3 [80.5 lb/ft^3]	Site-specific mean value†
Wet deposition scavenging coefficient	0 1 s	No plume depletion by wet deposition, RSAC code
Plume depletion by dry deposition	1	Yes
Deposition velocity for solids	0.001 m/s [0.003 ft/s]	RSAC code default value
Deposition velocity for halogens	0.01 m/s [0.03 ft/s]	RSAC code default value
Deposition velocity for noble gases	0.0 m/s [0.0 ft/s]	RSAC code default value
Deposition velocity for cesium	0.001 m/s [0.003 ft/s]	RSAC code default value
Deposition velocity for ruthenium	0.001 m/s [0.003 ft/s]	RSAC code default value
Downwind distance	11,000 m [6.8 mi]	Site-specific approximation‡
Linear constant in decay function	1 1/s	RSAC code default value for instantaneous release
Exponential constant in decay function	0.0 1/s	RSAC code default value for instantaneous release

Table 7-8. Meteorological Data Input for the RSAC Code (continued)		
Input Parameter	PCSA Tool Default Value	Remarks
Crosswind distances to be entered	No	Assuming critical group is directly downwind
Diffusion definition	2	Program calculates standard deviations
Type of sigma (standard deviation) set	1	Hilsmeier-Gifford for <15-minute releases at desert sites
Building width	0 m [0 ft]	RSAC code default value, option only if stack height is 0 m
Building height	0 m [0 ft]	RSAC code default value, option only if stack height is 0 m
Building wake coefficient	0	If zero, RSAC code default value of 1 is used
Weather class	6	6 relates to class F, the most-probable class (site-specific estimate)
Plume rise indicator	0	No plume rise

*DOE. "Draft Environmental Impact Statement for a Geological Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada." Volume II. DOE/EIS–0250D. Las Vegas, Nevada: DOE. 1999.
†Weast, R.C. *CRC Handbook of Chemistry and Physics*. Cleveland Ohio: CRC Press. p. F-11. 1976.
‡CRWMS M&O. "Design Basis Event Frequency and Dose Calculation for Site Recommendation." CAL–WHS–SE–000001. Rev. 01. Las Vegas, Nevada: CRWMS M&O. 2000.

height was assumed to be appropriate. For releases less than 15 minutes over desert terrain, the Hilsmeier-Gifford plume diffusion is recommended (Wenzel, 1994) and was selected as the default for the dose calculation. An average wind velocity of 3 m/s [7 mi/hr] and a weather Class of F represent most-probable estimates from data taken at Desert Rock, Nevada in 1997 and were selected as defaults for the deterministic RSAC Calculations. A site-specific value of 1.29×10^3 g/m^3 [0.0805 lb/ft^3] was input for the air density (Weast, 1976). Due to the arid climate of the site, plume depletion by dry deposition was selected. Based on the most recent description of the site boundary (CRWMS M&O, 2000f), a downwind distance of 11 km [6.8 mi] from the Waste Handling Building was chosen for the closest off-site member of the public. It was assumed that the receptor was located directly downwind of the release, and, therefore, no crosswind distances were input. Plume rise was not selected for this calculation. The inclusion of plume rise requires data on the stack that were not available at this time (i.e., internal stack diameter and speed of efflux gases emitted from the stack or gas heat emission rate from the stack). Plume rise effectively increases the stack height and would be expected to result in greater atmospheric dispersion and a reduction in the dose results.

7.1.1.3.2 Inhalation Dose Calculation

The input parameters and their default values for the inhalation dose calculation are presented in Table 7-9. The 50-year committed effective dose equivalent is calculated for the inhalation pathway. The inhalation committed effective dose equivalent represents the total dose received for a 50-year time period from the radionuclides inhaled as a result of the event and retained within the body. Although the inhalation committed effective dose equivalent is defined for 50 years, it represents an event dose within the regulatory framework. Inherent assumptions of the inhalation dose calculation are that the receptor is located offsite as the radionuclide plume passes, and the outdoor radionuclide concentration is used (i.e., no protection is given for the receptor spending time indoors as the plume passes). The default RSAC dose calculation for inhalation is based on International Commission on Radiological Protection (1979) and was Publication 60 of selected to calculate the inhalation dose equivalents in units of rem for all elements and all organs. The default inhalation parameter values are a breathing rate of 3.33×10^{-4} m^3/s [0.0118 ft^3/s] and an activity mean aerodynamic diameter of 1 µm [4×10^{-5} in] (Wenzel, 1994).

7.1.1.3.3 Ingestion Dose Calculation

Table 7-10 lists the input parameters and their default values for the ingestion dose calculation. This calculation determined the ingestion dose equivalent in units of rem for all elements and all organs. When available, Yucca Mountain site-specific values were used for the ingestion parameters. The RSAC code does not consider egg consumption. Using a mean local egg consumption rate of 6.7 kg/yr [15 lb/yr] (LaPlante and Poor, 1997) and a hen dry feed consumption rate of 0.0216 kg/day [0.0476 lb/day] per day, the egg consumption pathway was estimated to contribute an additional 5 percent to the committed effective dose equivalent for ingestion and an additional 7 percent at most to any individual organ receiving a dose greater than 10^{-2} µSv [10^{-3} mrem] (for boiling water reactor or pressurized water reactor fuel releases in air or in the pool). Because the egg consumption pathway was found not to significantly increase the ingestion dose results, the egg consumption pathway was not included in the RSAC dose calculations.

7.1.1.3.4 Ground Surface Dose Calculation

Calculations of the external dose from exposure to the ground surface were also performed. Table 7-11 presents the input parameters for the ground surface dose calculation. The dose equivalents from exposure to the contaminated ground surface were calculated in units of rem for all elements and all organs. The default exposure time for the ground surface dose calculation is 1 year, which is appropriate and conservative for an annual dose calculation without evacuation and remediation. The exposure time of 1 year is also considered to be a sufficiently long period of time before remediation activities would be completed at the off-site locations. An inherent assumption for the ground surface dose calculation is that the receptor lives and works at the closest off-site distance from the Waste Handling Building. To account

Table 7-9. Inhalation Dose Calculation Input for the RSAC Code		
Input Parameter	**PCSA Tool Default Value**	**Remarks**
Type of dose calculation	1	International Commission on Radiological Protection-30 inhalation with user-specified parameters
Output control for dose	-2	Only dose summaries
Dose unit	1	Output in rem
Elements for calculation	0	All elements
Organ choice	1	All organs
For inhalation, breathing rate	3.33×10^{-4} m^3/s [1.18×10^{-2} ft^3/s]	Inhalation dose input default value, average daily breathing rate
Decay time for exponential decay function	0 s	RSAC code default value for instantaneous release
Activity mean aerodynamic diameter	1 μm [4×10^{-5} in]	RSAC code default value
Clearance classes	1	RSAC code default classes

Table 7-10. Ingestion Dose Calculation Input for the RSAC Code		
Input Parameter	PCSA Tool Default Value	Remarks
Type of dose calculation	3	Ingestion with user-specified parameters
Output control for dose	-2	Only dose summaries
Dose unit	1	Output in rem
Elements for calculation	0	All elements
Organ choice	1	All organs
Decay time for exponential decay function	0 s	RSAC code value for instantaneous release
Plant midpoint of operating life	1 yr	Dose during year of intake for acute releases
Ingestion transfer parameter control	0	RSAC code default transfer parameters used
Ingestion parameter control	2	User-specified ingestion parameters
Time crops are exposed to contamination during the growing season	7 day	Times <60 days are interpreted as acute releases
Harvest duration following acute release	7. day	RSAC code default value
Stored (other) vegetable consumption rate includes fruits and grains	23.8 wet kg/yr [52.5 wet lb/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents*
Fresh (leafy) vegetable consumption rate	15 wet kg/yr [33.1 wet lb/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents*
Meat consumption rate includes beef and poultry	3.7 kg/yr [8.2 lb/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents*
Milk consumption rate	4.1 L/yr [1.1 U.S. gal/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents* assuming a milk density of 1 Kg/L

Table 7-10. Ingestion Dose Calculation Input for the RSAC Code (continued)		
Input Parameter	**PCSA Tool Default Value**	**Remarks**
Fraction of stored vegetables from garden	0.76	RSAC code default value
Fraction of fresh vegetables from garden	1	RSAC code default value
Retention factor for activity on forage	0.57	RSAC code default value
Retention factor for activity on vegetables	0.2	RSAC code default value
Retention factor for iodines on forage	1.0	RSAC code default value
Removal rate constant for crops	0.0021 1/hr	RSAC code default value
Vegetable exposure time for chronic releases	7 day	Set equal to the time crops are exposed to contamination during the growing season
Forage exposure time for chronic releases	7 day	Set equal to the time crops are exposed to contamination during the growing season
Tritiated water, removal half-time	1 day	RSAC code default value
Effective surface density for soil	225 kg/m^3 [14.0 lb/ft^3]	RSAC code default value
Stored vegetable holdup time after harvest	14 day	Site-specific value*
Fresh vegetable holdup time after harvest	1 day	Site-specific value*
Animals daily forage feed	16 dry kg/day [35 dry lb/day]	RSAC code default value
Feed-milk receptor transfer time	2 day	RSAC code default value
Slaughter to consumption time	20 day	Site-specific value*
Fraction of year that animals graze	0.4	RSAC code default value
Fraction of feed that is pasture when grazing	0.43	RSAC code default value

Table 7-10. Ingestion Dose Calculation Input for the RSAC Code (continued)		
Input Parameter	**PCSA Tool Default Value**	**Remarks**
Stored feed holdup time	14 day	Set equal to stored vegetable holdup time
Vegetable vegetation yield	3.0 wet kg/m^2 [0.61 wet lb/ft^2]	Average of leafy vegetable (2.0) other vegetable (4.0), and fruit (3.0) yields*
Forage vegetation yield	1.23 dry kg/m^2 [0.252 wet lb/ft^2]	Consistent with site-specific vegetation value*
Absolute humidity	4.9 g/m^3 [0.31 lb/ft^3]	RSAC code default value
Fraction of annual stored vegetables that are contaminated by acute release	0.5	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
Fraction of annual fresh vegetables that are contaminated by acute release	0.33	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
Fraction of annual stored forage that is contaminated by acute release	0.5	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
Fraction of annual fresh forage that is contaminated by acute release	0.33	RSAC code value for crops exposed to contamination between 1 hour and <30 days

*LaPlante, P.A. and K. Poor. "Information and Analysis to Support Selection of Critical Groups and Reference Biosphere for Yucca Mountain Exposure Scenarios." CNWRA 97–009. San Antonio, Texas: CNWRA. 1997.

for the receptor spending some time indoors, the RSAC code default value of 0.7 was used for the building shielding factor.

For the ground surface pathway, the RSAC code did not contain dose rate conversion factors for H-3 and C-14, and, therefore, external doses from this pathway were not calculated for H-3 and C-14. Because H-3 is a pure emitter of low-energy beta particles, the H-3 dose rate conversion factor is zero for ground surface exposure (EPA, 1993). C-14 is also a pure beta emitter. C-14 emits beta particles at higher energy than H-3, however, and, therefore, is assigned larger, nonzero dose coefficients for ground surface exposure. To qualitatively assess the impact of C-14 on the ground surface results, a comparison was made with Cs-137. The inventory of Cs-137 is more than five orders of magnitude greater than for C-14 (see Table 7-2), and the dose rate conversion factors for ground surface exposure are larger for Cs-137 than for C-14 (EPA, 1993). The RSAC default deposition velocities are the same for Cs-137 and C-14. The half-lives are significantly different for C-14 and Cs-137, but the longer

Table 7-11. Ground Surface Calculation Dose Input for the RSAC Code		
Input Parameter	**PCSA Tool Default Value**	**Remarks**
Type of dose calculation	4	Ground surface dose calculation
Output control for dose	-2	Only dose summaries
Dose unit	1	Output in rem
Elements for calculation	0	All elements
Organ choice	1	All organs
Decay time for exponential calculations	0 s	RSAC code default value for instantaneous release
Ground surface exposure time	1 yr	Dose is calculated for 1year after the event
Building shielding factor (dimensionless)	0.7	RSAC code default value

half-life of C-14 over Cs-137 will not manifest in significantly smaller decay of C-14 for the short 1-year occupation time for ground surface exposure. Therefore, the missing ground surface dose rate conversion factors for H-3 and C-14 are expected to have a negligible effect on the dose results.

7.1.1.3.5 Submersion Dose Calculation

Submersion refers to the external dose resulting from exposure to the passing airborne radionuclide plume. The input parameters for the submersion dose calculation are displayed in Table 7-12. Based on a finite plume model (Slade, 1968), the RSAC code cloud dose calculation was selected to compute the effective dose equivalent from submersion. The submersion dose represents an event dose. Inherent assumptions of the submersion dose calculation are that the receptor is located at the off-site location as the radionuclide plume passes (i.e., no protection is given for the receptor spending time indoors as the plume passes).

7.1.2 Function of the Deterministic Calculation of Public Dose

As displayed in Figure 7-1, the RSAC and MELCOR codes are used in the public dose calculation. In the Consequences menu for the RSAC code, the three main options for the public dose calculation are Standard RSAC Input, Advanced RSAC Input, and Show Output. The Standard RSAC Input option presents the user with an interface for the RSAC parameter inputs to calculate the dose to members of the public. The consequence analysis module of the PCSA Tool automates the RSAC computation by (i) transferring the input data to the RSAC, (ii) running the RSAC in the background, (iii) transferring the output data from the RSAC, as well as (iv) saving and retrieving the input and output data. Changes made to the input data within the PCSA Tool automatically invoke a new RSAC run that subsequently updates the consequence analysis output, thereby alleviating the need for the user to manually load, run

Table 7-12. Submersion Dose Calculation Input for the RSAC Code		
Input Parameter	**PCSA Tool Default Value**	**Remarks**
Gamma cloud model selection	0	All calculations are made using a finite model
Decay time for exponential decay function	0 s	RSAC code default value for instantaneous release
Type of dose calculation	2	Calculate external effective dose equivalent

input files, and review the output files within the RSAC code. Depicted in Figure 8-1, the Show Output option presents the results of the public dose calculation.

To provide the user with maximum flexibility, the Advanced RSAC Input option allows the user to access the input files for the RSAC directly. Currently, a RSAC calculation made via the Advance RSAC Input option will automatically display the RSAC output file.

Figure 7-2 displays the Fuel Selection/Assemblies Breached input folder within the Standard RSAC Input and shows the run type option (at the bottom of the page) where the user specifies whether a deterministic or probabilistic consequence analysis is desired. The input screens for the public dose calculations are organized into nine folders with the following names:

- Fuel Selection/Assemblies Breached
- Release Fraction by Group
- HEPA, Bldg Discharge, Others
- Meteorological Data
- Inhalation Dose
- Ingestion Dose
- Ground Surface Dose
- Submersion Dose
- View Source Term

Selection of the Done/Run button initiates the MELCOR calculation. The calculated building discharge fractions are automatically extracted from the MELCOR output file and displayed in a popup window so the user can manually transfer the information into the appropriate input cells for the RSAC dose calculation.

Selection of the Done/Run button at the bottom right corner of the input folders spawns the RSAC for the deterministic calculation of the public dose. Selecting the Show Output option under Public Dose in the Consequence menu displays a chart of the effective dose equivalents for each of the four dose pathways. In addition to a tabulation of the organ doses summed over all four pathways, tabulations of the organ doses for the inhalation, ingestion, and ground surface pathways are displayed on different folders in the same output screen. Figures titled

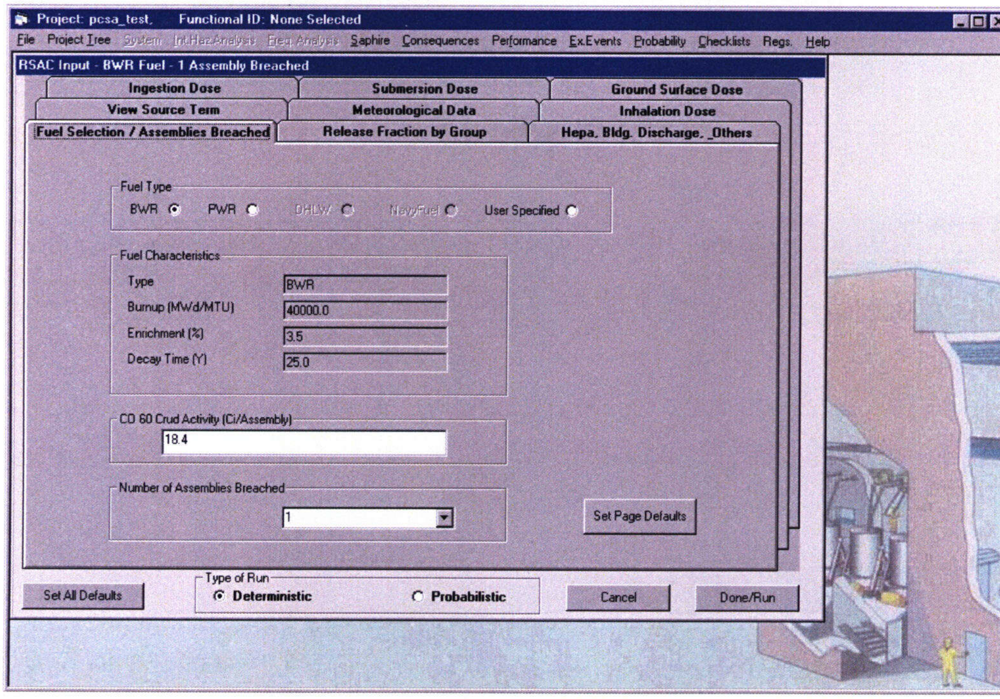


Figure 7-2. Standard RSAC Input Interface

RSAC Output in Appendix D present the output screens for an example deterministic calculation of dose to an off-site member of the public described in Chapter 10 of this report.

7.1.3 Probabilistic Calculation of Public Dose

In the preparation and execution of large codes, such as RSAC, that require a large number of physical parameters, it may be found that several parameters are not constant for the problem domain or that the selected values are uncertain or variable for other reasons. When the values of some RSAC input parameters are uncertain or variable, it is desirable to present the dose in the form of a complementary cumulative distribution function. A complementary cumulative distribution function displays the probability that the dose will exceed a given value when the parameters are specified with a range and distribution function. This probabilistic approach is incorporated into the PCSA Tool to assess the uncertainty and variability in the hazard and consequence analyses.

In this approach, probability density functions are assigned to the sampled input parameters. The range of this function is also specified by the user to reflect the parameter uncertainty or variability. Based on these characteristics, a family of values is randomly generated (sampled) for those parameters and used to make several calculations of public dose. Each individual calculation is called a realization. In essence, each realization is a single deterministic calculation based on a set of sampled values. The consequence analysis module provides the user with additional interfaces for the selection of distribution functions and ranges for the RSAC input parameters. The module can also initiate the execution of the sampling process and the RSAC dose calculations. The output from the probabilistic calculation considers the results from multiple realizations. The consequence analysis module allows saving and retrieving the input and output data for the probabilistic calculation.

The following outlines the steps of the process for the probabilistic dose calculation.

(1) Specify uncertain parameters along with their ranges and distributions.
(2) Generate the sampled parameter set.
(3) Run the RSAC code for the requested number of realizations.
(4) Retrieve and store the dose values from each realization.
(5) Generate the complementary cumulative distribution function displays.

Flow diagrams of the process for the probabilistic dose calculation and its stand-alone FORTRAN program are shown in Figure 7-3(a),(b), respectively. The following subsections describe the components of the probabilistic dose calculation in more detail.

7.1.3.1 Specifying Uncertain Parameters

The consequence analysis module provides the user with additional interfaces for the selection of distribution types and values for the RSAC code input parameters. Although distributions can be assigned to other input parameters, default probability distributions have been assigned to the radionuclide release fractions from breached spent nuclear fuel, radionuclide deposition velocities, and meteorological parameters. Table 7-13 presents the sampled parameters with their default probability distributions for the probabilistic dose calculation. This information is sent to the auxiliary code called PCSA_LHSINP. This code uses this information to prepare an input file for the stand-alone utility module called PCSA_LHS. Parameters that are not listed here retain their constant value as described in the deterministic calculation section.

7.1.3.2 Generating the Sampled Parameter Values

As mentioned in the previous section, the sampled parameter set is generated by the PCSA_LHS utility module. This code uses a Latin Hypercube Sampling scheme from Sandia National Laboratory (Iman and Shortencarier, 1984). The Latin Hypercube Sampling scheme is designed to sample the entire range and, therefore, converges with a fewer number of realizations than if pure random sampling is used. The PCSA_LHS module used in the PCSA Tool contains several enhancements, including the ability to change a sampled parameter to a constant without disrupting the random numbers used for the remaining sampled parameter set, and a new distribution type, called User Supplied Discrete.

The PCSA_LHS utility module is run after the PCSA_LHSINP module has created the input file called *lhs.inp*. The output file from PCSA_LHS is called *lhs.out* and contains all the sampled parameter values for all the realizations grouped by realization number. On termination of the PCSA_LHS module, control is returned to the PCSA Tool. Future versions of the PCSA Tool may provide the capability for a user to investigate the sampled parameter values from PCSA_LHS and their distributions before proceeding further with the analysis.

The new User Supplied Discrete distribution function permits the user to specify a discrete probability distribution function by using up to 20 entries. Each entry consists of a (value,

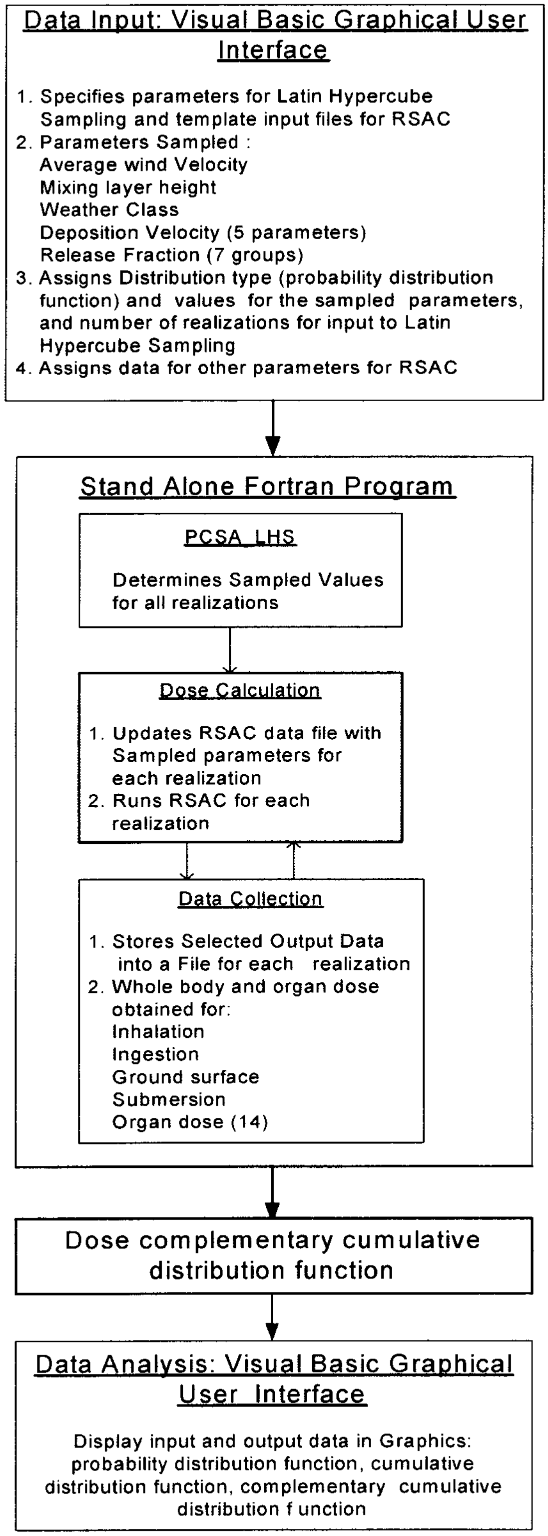


Figure 7-3 (a). Probabilistic Dose Calculation Flow Chart

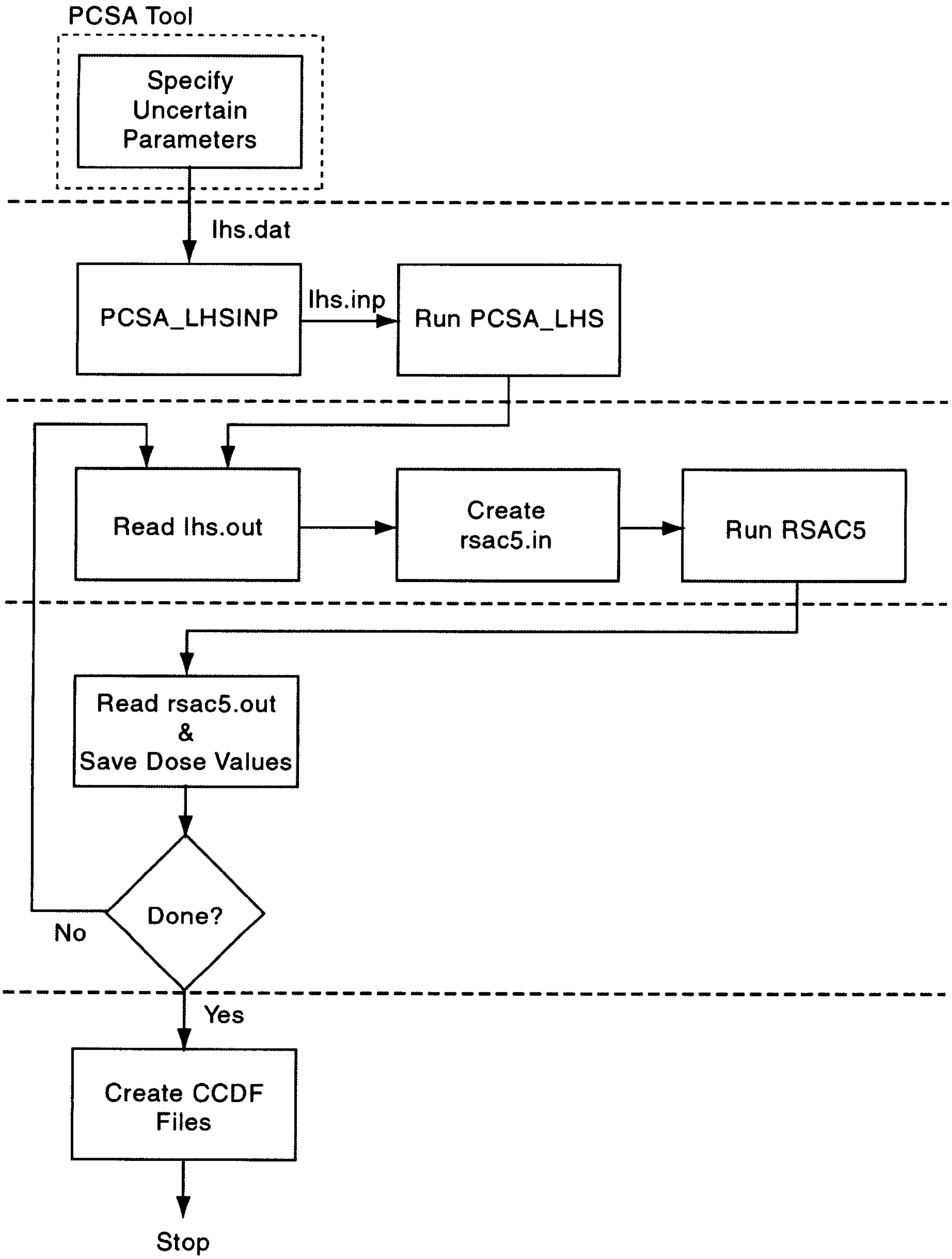


Figure 7-3 (b). Flow Chart of the Stand-Alone FORTRAN Program. The Dashed Lines Demarcate the Steps of the Probabilistic Dose Calculation.

Table 7-13. PCSA Tool Default Distributions for the Probabilistic Calculation			
Parameter	**Distribution**	**Distribution Values**	**Supporting Information**
Average wind velocity	logtriangular	0.978, 2.13, 13.2 m/s [3.21, 6.99, 43.3 ft/s]	Based on minimized Chi-squared fit to 1997 Desert Rock wind speed data performed by CNWRA.
Mixing Layer Height	logtriangular	140, 1,420, 3,000 m [460, 4,660, 9,840 ft]	The Draft Environmental Impact Statement* reported an average mixing height of 1,420 m [4,660 ft] for Desert Rock, Nevada, the location of the nearest upper air meteorological station, and this value was selected as the mode of the distribution. U.S. Department of Energy (DOE) assumed one-tenth of the Desert Rock average mixing height 140 m [460 ft] would represent the mixing height for stable conditions, and this value was selected as the minimum value for the distribution. The Draft Environmental Impact Statement did not imply a maximum mixing height or mixing height distribution for Yucca Mountain. Therefore, the logtriangular distribution was selected based on an analog desert site, Idaho National Engineering Laboratory† whose data are presented in Table A–1 (p. A–6) of the RSAC Version 5.2 User's Manual.‡ A logtriangular distribution appeared to fit the data better. Although the analog data suggested a maximum mixing height of 3,300 m [1,800 ft], the maximum of 3,000 m [980 ft] was assigned because it corresponds to the maximum mixing layer height allowed by the RSAC code. Such a change would also tend to be conservative but is not expected to impact the results, which are insensitive to these large values of the mixing height parameter.

Table 7-13. PCSA Tool Default Distributions for the Probabilistic Calculation (continued)

Parameter	Distribution	Distribution Values	Supporting Information
Weather Class	user defined discrete	sampled from (1,2,3,4,5,6) with the respective probabilities of (0.04101, 0.00631, 0.02524, 0.13249, 0.39432, 0.40063)	Weather classes were selected from the 1997 Desert Rock temperature data at different heights based on Table 2 of the Regulatory Guide 1.23[§]
Deposition Velocity for Solids	uniform	0.000026, 0.02 m/s [0.000085, 0.066 ft/s]	Range from Report 76, Table 2.8 (p. 49)[‖]
Deposition Velocity for Halogens	logtriangular	0.0002, 0.01, 0.26 m/s [0.00066, 0.033, 0.85 ft/s]	Range for iodine gas from Report 76, Table 2.8 (p. 49)[‖]; mode assigned the typically accepted value of 0.01 equal to RSAC Version 5.2 User's Manual default value[‡]; logtriangular was selected because the accepted value did not bound the range
Deposition Velocity for Noble Gases	constant	0 m/s [0 ft/s]	Assigned to the RSAC Version 5.2 User's Manual default value[‡]
Deposition Velocity for Cesium	uniform	0.0004, 0.006 m/s [0.0013, 0.020 ft/s]	Range from Report 76, Table 2.8 (p. 49)[‖]
Deposition Velocity for Ruthenium	uniform	0.0002, 0.023 m/s [0.00066, 0.075 ft/s]	Range from Report 76, Table 2.8 (p. 49)[‖]

Table 7-13. PCSA Tool Default Distributions for the Probabilistic Calculation (continued)			
Parameter	**Distribution**	**Distribution Values**	**Supporting Information**
Release Fraction (unitless) for Noble Gases (Ar, Kr, Rn)	triangular	0.05, 0.40, 0.40	Minimum assigned to free-fall spill value in Table A1[¶]; mode assigned to Table 3.3 value of NUREG/CR–6451[#]; maximum assigned to free-fall spill value in Table 11.4 of NUREG–1536[**]
Release Fraction (unitless) for H	uniform	0.01, 0.3	Minimum assigned to the high-energy crush/impact value (free-fall spill value was not provided for H) in Table A1[¶]; maximum assigned to Table 7.1 value of NUREG-1536[**]
Release Fraction (unitless) for I	triangular	1.5×10^{-5} 2.3×10^{-3} 0.3	Minimum assigned to value from Table 3.3 of NUREG/CR–6451[#]; mode assigned to free-fall spill value for iodine I_2 in Table A1[†,¶]; maximum assigned to the value in Table 9.2 of NUREG–1567[††] and in Table 4-1 of NUREG–1617[‡‡]
Release Fraction (unitless) for Cs & Sr	triangular	2×10^{-6} 2.3×10^{-5} 2.5×10^{-4}	Minimum assigned to impact rupture value in Table 11.4 and mode assigned to Table 7.1 value of NUREG–1536[**]; maximum assigned to free-fall spill value for Cs vapor in Table A1[†,¶]
Release Fraction (unitless) for Ru	triangular	2×10^{-6} 1.5×10^{-5} 2.4×10^{-4}	Minimum assigned to impact rupture value in Table 11.4 and mode assigned to Table 7.1 value of NUREG–1536[**]; maximum assigned to free-fall spill value in Table A1[†,¶]
Release Fraction (unitless) for Fuel Fines	triangular	2×10^{-6} 2×10^{-6} 2.4×10^{-4}	Minimum and mode assigned to impact rupture values in Table 11.4 of NUREG–1536[**]; maximum assigned to free-fall spill value in Table A1[†,¶]

Table 7-13. PCSA Tool Default Distributions for the Probabilistic Calculation (continued)

Parameter	Distribution	Distribution Values	Supporting Information
Release Fraction (unitless) for Co-60 Crud	uniform	0.001, 1.0	Minimum assigned to shock/vibration value from Table A1[†,¶]; maximum assigned to the value in Table 9.2 of NUREG–1567[‡‡] and in Table 4-1 of NUREG–1617[§§]

*DOE. "Draft Environmental Impact Statement for a Geological Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County." 1999.
†Clawson, K.L., G.E. Start, and N.R. Ricks. "Climatography of the Idaho National Engineering Laboratory." 2nd Edition. DOE/ID–12118. Idaho Falls, Idaho: U.S. Department of Commerce. 1989.
‡Wenzel, D.R. "The Radiological Safety Analysis Computer Program (RSAC–5) User's Manual, WINCO–1123." Revision 1. Idaho Falls, Idaho: Idaho National Engineering Laboratory. 1994.
§NRC. Regulatory Guide 1.23, "Onsite Meteorological Programs (Safety Guide 23)." Washington, DC: NRC. 1972.
||National Council on Radiation Protection and Measurements. "Radiological Assessment: Predicting the Transport, Bioaccumulation, and Uptake by Man of Radionuclides Released to the Environment." NCRP Report 76. Bethesda, Maryland: NCRP. 1984.
¶American Nuclear Society. "Airborne Release Fractions at Non-Reactor Nuclear Facilities." ANSI/ANS–5.10–1998. La Grange, Illinois. American Nuclear Society. 1998.
#Travis, R.J., R.E. Davis, E.J. Grove, M.A. Azarm. NUREG/CR–6451, "A Safety and Regulatory Assessment of Generic BWR and PWR Permanently Shutdown Nuclear Power Plants." Washington, DC: NRC. April 1997.
**NRC. NUREG–1536, "Standard Review Plan for Dry Cask Storage Systems." Washington, DC: NRC. January 1997.
††Table A1 cites J. Mishima, "LANL TA-55 Particles Generated by Impact of Bare Fuel Pellets." Richland, Washington. Pacific Northwest Laboratory. March 1995.
‡‡NRC. NUREG–1567, "Standard Review Plan for Spent Fuel Storage Facilities." Washington, DC: NRC. March 2000.
§§NRC. NUREG–1617, "Standard Review Plan for Transportation Packages for Spent Nuclear Fuel." Washington, DC: NRC. 2000.
†For loose surface contamination, Table A1 cites Subsection 4.4.3.3.1 of the DOE Handbook (1994).

probability) pair. The sum of the probabilities must be equal to one. Note that the sampled values returned from PCSA_LHS will be one of the up to 20 values supplied. Note, that interpolation is not required for the discrete distribution function.

For example, suppose there are eight data values with the probabilities shown in Table 7-14. The cumulative distribution function that would be used to generate the sample values for this example is shown in Figure 7-4. A cumulative distribution function has the characteristic of being monotonically increasing. The increase in the cumulative distribution function curve from one of the supplied discrete values to the next varies according to the probability associated with the next discrete value. Samples from this distribution will be one of the eight input values. If a continuous distribution function is desired, the user should use a nondiscrete distribution function.

7.1.3.3 Running the RSAC Code for the Requested Number of Realizations

The consequence analysis module prepares the RSAC input file and controls the realization loop for multiple invocations of the RSAC code. In addition to the *lhs.out* file mentioned in the

Table 7-14. Example Data for User Supplied Discrete Distribution Function	
Variable Value	**Probability**
0.0	0.037
0.55	0.153
1.1	0.300
2.3	0.092
4.9	0.063
6.6	0.010
8.3	0.045
9.36	0.300

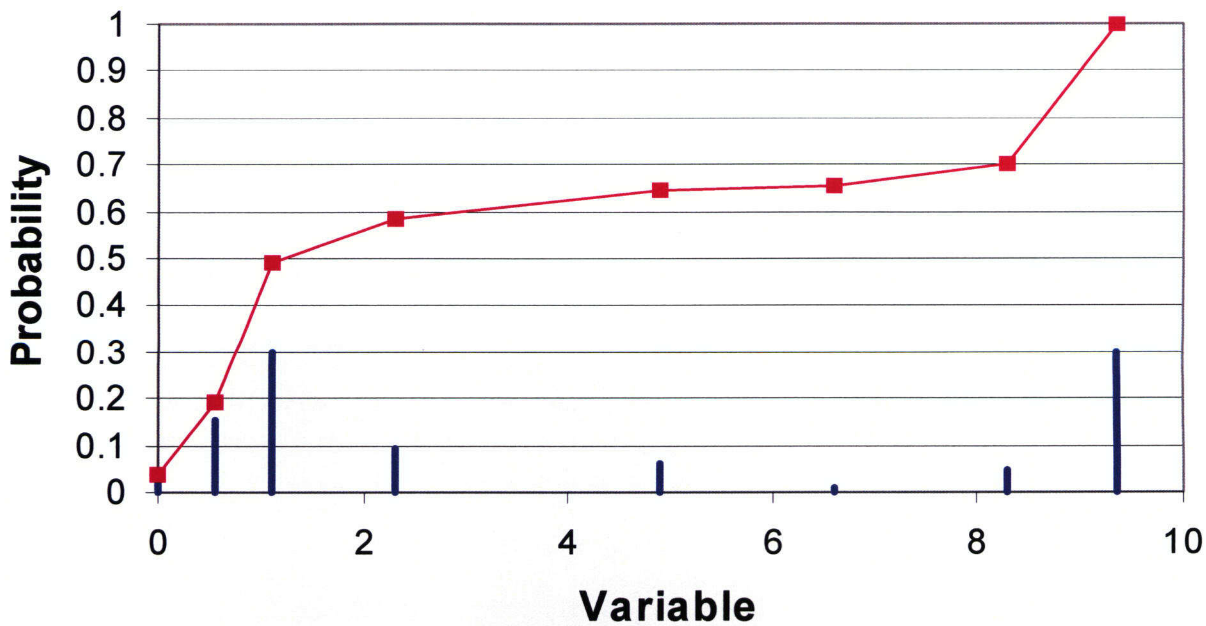


Figure 7-4. Cumulative Distribution Function Corresponding to the Example Data in Table 7-14

previous section, the PCSA Tool provides files *rsac5.def* and *varnames.dat* to the consequence analysis module. These files convey values from the user dialog boxes necessary for the control of the RSAC code. File *rsac5.def* is a radiological safety analysis computer program input file filled with the deterministic and default values. Some of these values will be overwritten by the sampled values before being submitted for processing. The parameters involved in the sampling process are listed in the *varnames.dat* file. Both of these files are automatically created by the PCSA Tool and do not need the attention of the user. The multiple realization loop for the RSAC dose calculation is controlled by using the number of realizations extracted from the *lhs.inp* file and running a local batch file to invoke the RSAC code in a loop for the requested number of executions.

7.1.3.4 Retrieving and Storing the Dose Results from Each Realization

After each realization, the consequence analysis module scans the RSAC output file *rsac5.out* and collects the committed effective dose equivalents for inhalation and ingestion pathways and the external effective dose equivalents for the ground surface and air submersion pathways. Individual organ doses are also saved for all calculations, except the air submersion case for which the RSAC only calculates the effective dose equivalent. All values from all realizations are stored in internal arrays within the consequence analysis module until the realization loop is complete.

7.1.3.5 Generating the Complementary Cumulative Distribution Function Displays

After the realization loop is complete, a complementary cumulative distribution function is generated for each organ analyzed in each pathway calculation, as well as for the effective dose equivalent of each pathway. Each complementary cumulative distribution function is written to a separate file as a list of dose values paired with a probability. The complementary cumulative distribution function output files are flat ASCII files that are returned to the PCSA Tool for display. The dose values are listed in order from the smallest to largest. In the Latin Hypercube Sampling method each sample is equally probable. Therefore, the probabilities associated with the dose from each realization is $1/r$, where r is the number of realizations. For display purposes, it is desirable to combine realizations that have identical dose values. Combining is accomplished by summing the probabilities from those results being combined and associating the sum with a single dose value. This process is most beneficial for calculations that produce many realizations with a dose of 0 mrem, because the distortion at the lower end of the curve is reduced by combining realizations with the same dose value. When realizations are combined, however, the listed doses must be weighted by their probabilities.

7.1.4 Initiating Probabilistic Calculation of Public Dose with the PCSA Tool

The probabilistic calculation is enabled by selecting the Probabilistic button under the Type of Run header at the bottom of the input screens for the Standard RSAC Input (see Figure 7-2). As shown in the HEPA, Bldg Discharge, Others folder by Figure 7-5, the user must specify two control inputs, the number of realizations and a random seed, for the Latin Hypercube Sampling scheme. The number of realizations must be at least one greater than the number of sampled variables. This requirement of the Latin Hypercube Sampling scheme is because it can only

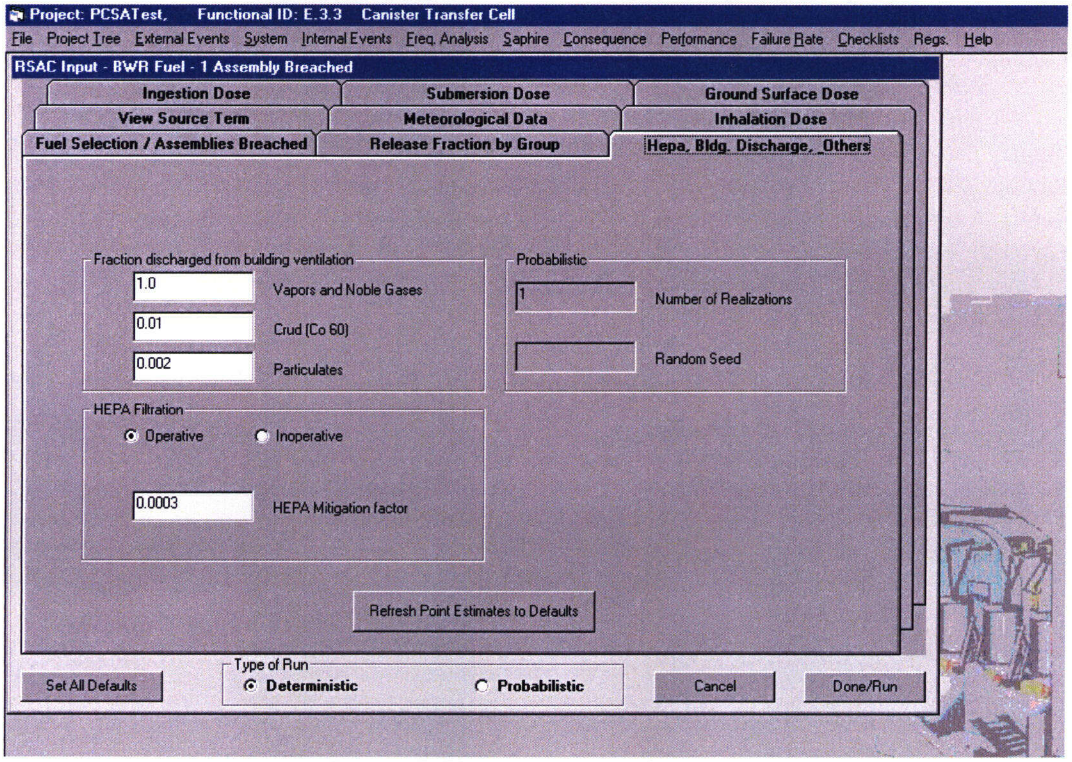


Figure 7-5. HEPA, Building Discharge, Others Input Folder Highlighting the Three Input Cells for Fractions of Airborne Radionuclides that Discharged from the Building Ventilation for Vapors and Noble Gases, Crud (Co-60), and Particulates

perform the stratified sampling with this minimum number of realizations. If a smaller number is used, the sampling scheme automatically reverts to Monte Carlo sampling, which is not recommended, without a warning message to the user. The PCSA Tool permits the number of realizations to be increased until statistical convergence is observed in the computed public dose. For identified parameter settings, the random seed from two separate runs must be the same to yield the same set of sampled values.

The input parameters for probabilistic dose calculation are the same parameters as those used for the deterministic dose calculation, except that the probabilistic dose calculation requires additional input information (i.e., distribution type and its values) for the sampled parameters. Selecting the Done/Run button on the input screens initiates the probabilistic dose calculation. The probabilistic dose calculation is not currently available for the Advanced RSAC Input option.

7.2 Worker Dose Calculation

The consequence analysis module also includes a Worker Dose calculation for an underwater release of radioactive material. During dry transfer operations, it was expected that workers would be located in the operator galleries and not in the transfer cell. In contrast, workers were expected to be present in the transfer cell during wet transfer operations. For the assumed operational procedures, a release of radioactive gases and particulates into the cell air from dry transfer operations would result in smaller worker doses in the galleries than the doses to workers present in the cell above the pool following the release of radioactive gases from wet transfer operations. Wet transfer operations account for 9 of the 14 Category 1 event sequences identified by the U.S. Department of Energy (DOE) (CRWMS M&O, 2000f). For these reasons, the worker dose calculation focused on underwater releases. This section presents the spreadsheet calculation for worker dose. This dose calculation is appropriate for workers located in the same room as an open pool in which spent nuclear fuel assemblies have been breached.

7.2.1 Approach

A dose calculation was performed for a worker near the pool after an underwater breach of spent nuclear fuel assemblies (e.g., in the assembly transfer cell) based on the calculation of radionuclide air concentrations in the breathing zone. An underwater assembly breach would expose workers in the cell to the gaseous radionuclides via the pathways of inhalation and submersion.

7.2.2 Source Term

The calculation considered that the following gaseous radionuclides were released into the air of the assembly transfer cell as a result of a breach of spent nuclear fuel cladding in the pool: H-3, Ar-39, Kr-85, I-129, Rn-220, and Rn-222. Due to its short 4-second half-life, Rn-219 was assumed to decay before it would be released into the air of the assembly transfer cell. The inventories for the selected radionuclides were obtained from Table 7-2.

7.2.3 Calculation and Assumptions

With the exception of Rn-219, all gaseous radionuclides in the pool were assumed to be immediately transported to the pool surface and released into the mixing volume of air above the pool surface (i.e., implying a pool release fraction of unity). Although a pool release fraction of unity may be acceptable for the noble gases, it may not be appropriate for tritium and iodine and could introduce significant conservatism. Tritium and iodine together account for the majority of the inhalation dose. If the pool release fraction for tritium and iodine is much less than one, the inhalation dose could be overestimated by as much as a factor of three.

For the purposes of calculating inhalation doses, instantaneous equilibrium of airborne Rn-220 and Rn-222 was assumed for their decay progeny Pb-212 and Pb-214, respectively. In other words, the airborne concentrations of Pb-212 and Pb-214 were set equal to the airborne concentrations of Rn-220 and Rn-222. Gravitational settling and deposition of Pb-212 and Pb-214 were not considered. This instantaneous equilibrium assumption is conservative. The conservatism added by the radon decay progeny assumption should be no greater than the fraction of the total inhalation dose that corresponds to the radon decay progeny (roughly 30 percent).

The airborne concentration of the i^{th} radionuclide, C_i (Bq m^{-3}), was calculated from the following expression:

$$C_i = \left(3.7\times10^{10}\,\frac{\text{Bq}}{\text{Ci}}\right)\left(\frac{A_{gas,i} \times N \times RF_{fuel}}{V}\right) \tag{7-5}$$

where $A_{gas,i}$ represents the inventory in the fuel for the i^{th} radionuclide (Ci/assembly), and RF_{fuel} represents the fraction of the gaseous radionuclide activity released from the fuel into the pool into the air mixing volume (unitless), and V represents the mixing air volume (m^3).

The worker was assumed to be present in the mixing volume, V, for a time, t (min), and breathe the air in the mixing volume, V, at a rate of BR ($m^3\ min^{-1}$). Therefore, the total inhalation committed effective dose equivalent, in rem, was calculated as the summation of all gaseous radionuclides released in the following manner:

$$\text{Inhalation } CEDE = \left(100\frac{\text{rem}}{\text{Sv}}\right)\sum_i DCF_{inh,i} \times C_i \times BR \times t \qquad (7\text{-}6)$$

where $DCF_{inh,i}$ represents the inhalation dose conversion factor for the i^{th} radionuclide (Sv Bq^{-1}). The total submersion effective dose equivalent, in rem, was calculated as the summation for all gaseous radionuclides released:

$$\text{Submersion } EDE = \left(100\frac{\text{rem}}{\text{Sv}}\right)\left(0.0167\frac{\text{h}}{\text{min}}\right)\sum_i DCF_{sub,i} \times C_i \times t \qquad (7\text{-}7)$$

where $DCF_{inh,i}$ represents the submersion dose conversion factor for the i^{th} radionuclide (Sv h^{-1} per Bq m^{-3}). The dose conversion factors for inhalation and submersion were obtained from EPA (1988) and are presented in Table 7-15.

For Ar-39 and Kr-85, submersion dose conversion factors were specifically given for the skin (as the critical organ), and total skin dose equivalent from submersion, in rem, was calculated as summation of the individual contributions from Ar-39 and Kr-85:

$$\text{Skin dose equivalent} = \left(100\frac{\text{rem}}{\text{Sv}}\right)\left(0.0167\frac{\text{h}}{\text{min}}\right)\left(DCF_{\text{skin,Ar}} \times C_{\text{Ar}} + DCF_{\text{skin,Kr}} \times C_{\text{Kr}}\right) \times t \qquad (7\text{-}8)$$

where $DCF_{skin,Ar}$ represents the submersion dose conversion factor for the skin from Ar-39 (Sv h^{-1} per Bq m^{-3}), C_{Ar} represents the airborne concentration of Ar-39, (Bq m^{-3}), $DCF_{skin,Ar}$ represents the submersion dose conversion factor for the skin from Kr-85 (Sv h^{-1} per Bq m^{-3}), and C_{Kr} represents the airborne concentration of Kr-85 (Bq m^{-3}). Tritium was assumed to be in the form of water vapor for the inhalation calculation. Although the submersion calculation used the sole dose conversion factor listed, corresponding to elemental tritium, tritium had a negligible effect on the total effective dose equivalent from submersion. The submersion dose conversion factors (EPA, 1988) are based on a semi-infinite geometry. Use of these submersion dose conversion factors for a finite mixing volume is conservative. Because the conservative submersion calculation accounts for roughly 10 percent of the total effective dose equivalent, the conservatism added by using semi-infinite dose conversion factors for submersion is not expected to have a large effect on the total effective dose equivalent to

Table 7-15. Dose Conversion Factors for Inhalation and Submersion.* Inhalation and Submersion Dose Conversion Factors for H-3 Were Listed for Water Vapor and Elemental Forms, Respectively.			
Radionuclide	**Inhalation, dose conversion $factor_{inh}$**	**Submersion, dose conversion $factor_{sub}$**	**Submersion Skin Dose, dose conversion $factor_{skin}$**
H-3	1.73×10^{-11} Sv/Bq [6.40×10^{1} rem/Ci]	1.19×10^{-15} Sv h^{-1} per Bq m^{-3} [1.55×10^{-1} rem h^{-1} per Ci ft^{-3}]	(no value)
Ar-39	(no value)	5.54×10^{-14} Sv h^{-1} per Bq m^{-3} [7.24×10^{0} rem h^{-1} per Ci ft^{-3}]	3.75×10^{-11} Sv h^{-1} per Bq m^{-3} [4.90×10^{3} rem h^{-1} per Ci ft^{-3}]
Kr-85	(no value)	4.70×10^{-13} Sv h^{-1} per Bq m^{-3} [6.14×10^{1} rem h^{-1} per Ci ft^{-3}]	4.66×10^{-11} Sv h^{-1} per Bq m^{-3} [6.09×10^{3} rem h^{-1} per Ci ft^{-3}]
I-129	4.69×10^{-8} Sv/Bq [1.74×10^{5} rem/Ci]	(no value)	(no value)
Pb-212 (from Rn-220)	4.56×10^{-8} Sv/Bq [1.69×10^{5} rem/Ci]	(no value)	(no value)
Pb-214 (from Rn-222)	2.11×10^{-9} Sv/Bq [7.81×10^{3} rem/Ci]	(no value)	(no value)
*EPA. "Limiting Values of Radionuclide Intake and Air Concentration and Dose Conversion Factors for Inhalation, Submersion, and Ingestion." Federal Guidance Report No. 11, EPA 520/1–88–020. Washington, DC: EPA, Office of Radiation Programs. 1988.			

the worker. Table 7-16 displays the input parameters and default values for the worker dose calculation in the PCSA Tool. A mixing air volume was chosen to roughly correspond to the air space 3.0 m [10 ft] above the pool in the assembly transfer cell {i.e., 26 × 13 × 3.0 m [85 × 44 × 10 ft]. Selection of a smaller mixing volume would tend to concentrate the radionuclides into a smaller air volume around the worker and increase the worker doses.

7.2.4 Initiating the Worker Dose Calculation

As shown in Figure 7-1, the worker dose calculation is accessed by the Worker Dose option under the Consequence header on the toolbar of the PCSA Tool. The input parameters and outputs for the Worker Dose calculation are consolidated on a single screen, shown in Figure 7-7. Based on the previously described assumptions for this scenario and the default values in Table 7-16, the resulting worker doses for a case with no respiratory protection are presented in Table 7-17. Respiratory protection could reduce the total inhalation committed effective dose equivalent; however, it would not reduce the submersion dose.

Table 7-16. Input Parameter Values for an Example Worker Dose Calculation	
Parameter	**PCSA Tool Default Value**
Fuel assemblies breached, N	8 assemblies
Release fraction from fuel, RF_{fuel}	0.4
Worker inhalation rate, BR	3.33×10^{-4} m^3 s^{-1} [1.18×10^{-2} ft^3/s]
Mixing air volume, V	1059.1 m^3 [1385.5 $yard^3$]
Time spent in mixing volume after release, t	2 minute

Table 7-17. Example Dose Calculation for a Worker, without Respiratory Protection, Present for 2 Minutes after the Breach of Eight Pressurized Water Reactor Assemblies in the Spent Nuclear Fuel Pool	
Inhalation Committed Effective Dose Equivalent	0.018 Sv [1.8 rem]
Submersion Effective Dose Equivalent	0.0019 Sv [0.19 rem]
Inhalation + Submersion Total Effective Dose Equivalent	0.020 Sv [2.0 rem]
Skin Dose Equivalent	0.18 Sv [18 rem]

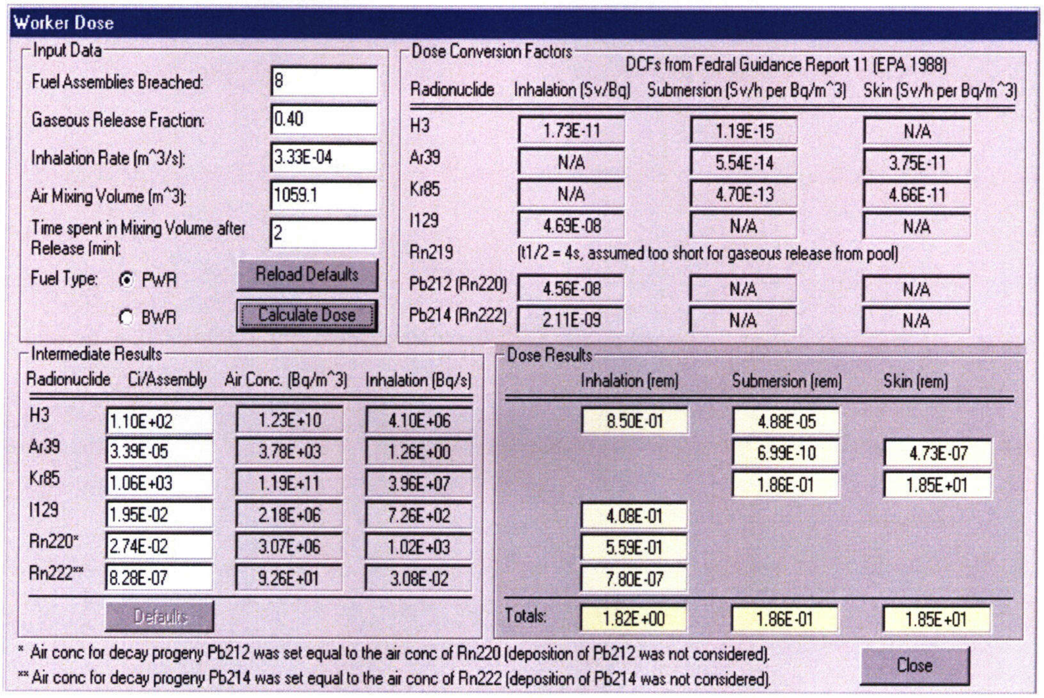


Figure 7-6. Interface for the Worker Dose Calculation

8 SAFETY AND RISK ASSESSMENTS

This chapter presents the preclosure safety and risk assessments in the PCSA Tool. The safety and risk assessments combine the results of hazard and consequence analyses of the preclosure event sequences. This chapter is divided into two Sections, 8.1 and 8.2, for separate discussion of the safety and risk assessments, respectively.

The safety assessment relates to the third acceptance criterion in Section 4.1.1.5.1.3 and the third acceptance criterion in Section 4.1.1.5.2.3 of the Yucca Mountain Review Plan (NRC, 2002a), which are based on meeting the requirements of 10 CFR 63.111(c)(1) and (c)(2).

The risk assessment is not required by the U.S. Nuclear Regulatory Commission (NRC) regulation in 10 CFR Part 63 (66 Federal Register 55732) and augments the review methods and acceptance criteria of NRC (2002a).

8.1 Safety Assessment

The safety assessment utility in the PCSA Tool enables a review for compliance with the relevant preclosure performance requirements of 10 CFR Part 63. To that end, the preclosure safety assessment presents the relevant performance requirements along with event sequence results for easy comparison and evaluation. The preclosure safety assessment utility treats the Category 1 and 2 event sequences separately.

8.1.1 Category 1 Event Sequences

The PCSA Tool currently has the capability of calculating (i) doses to offsite members of the public from releases of radioactive material into air or water and (ii) doses to workers located in the assembly transfer cell following an underwater breach of spent nuclear fuel cladding.

8.1.1.1 Public Dose from Category 1 Event Sequences

The safety assessment utility of the PCSA Tool can invoke two different approaches for evaluating compliance with the public dose performance requirements for Category 1 event sequences. The two approaches calculate (i) the frequency-weighted annual dose and (ii) the summation of doses from combinations of multiple event sequences within a single year of operation. Because the performance requirements for Category 1 event sequences are specified as a total effective dose equivalent, the preclosure safety assessment is based on total effective dose equivalent to members of the public from Category 1 event sequences and normal operations. In addition to the two safety assessment approaches, the conditional dose (i.e., not frequency weighted) from each Category 1 event sequence must be compared to the annual dose limit specified in 10 CFR 63.204 and summarized in Section 8.1.4 of this chapter.

8.1.1.2 Frequency-Weighted Annual Dose

Based on the results of the most recent preclosure safety assessments by the U.S. Department of Energy (DOE) (CRWMS M&O, 2000e,f), this approach sums the frequency-weighted annual doses from all Category 1 event sequences and normal operational releases from the surface (e.g., the Waste Handling Building and Waste Transfer Building) and subsurface facilities. The frequency-weighted annual dose from all Category 1 event sequences is calculated from the following relationship:

$$D_{\text{Category1}}^{\text{Frequency-weighted}} = \sum_{i=1}^{n} f_i \cdot D_i \tag{8-1}$$

where D_i represents the public dose resulting from the i^{th} Category 1 event sequence (rem), f_i represents the frequency of the i^{th} Category 1 event sequence (year^{-1}), and n represents the total number of Category 1 event sequences.

Reproduced from Eq. (5-2) of CRWMS M&O (2000e), the following equation determined the total Category 1 frequency-weighted annual dose in rem per year and is currently used by DOE to make its Category 1 safety case. For Category 1 event sequences and normal operations

$$D_{\text{Category 1}}^{\text{TOT}} = D_{\text{Category 1}}^{\text{Frequency-weighted}} + D_{\text{NO}}^{\text{Surface}} + D_{\text{NO}}^{\text{Subsurface}} \tag{8-2}$$

where $D_{\text{NO}}^{\text{Surface}}$ represents the annual dose due to normal operational releases from the surface facilities (rem per year^{-1}), and $D_{\text{NO}}^{\text{Subsurface}}$ represents the annual dose due to normal operational releases from the subsurface repository (rem per year^{-1}).

8.1.1.3 Combination of Event Sequences

For screening purposes, this simplified approach considers combinations of Category 1 event sequences that could occur in the same year. For such combinations of Category 1 event sequences, the doses from those particular event sequences can be summed together with the anticipated releases from normal operations to yield a total annual dose in that year. This approach assumes that the Category 1 event sequences are independent; therefore, the probability of multiple event sequences occurring in the same year is equal to the product of the annual probabilities of occurrence. To ensure potential occurrence of events and their consequences are not underestimated, this simplified screening approach has been coded into the PCSA Tool to use the annual frequencies for the event sequences in place of the annual probabilities in the equations presented in this section. Additional discussion is provided after the equations.

A combination of Category 1 event sequences is considered only if its annual probability of occurrence equals or exceeds the cutoff probability. In symbolic form, the combination of m event sequences occurring in a single year is considered only if the following probability criterion is satisfied:

$$P_{\text{Cutoff}} \leq \begin{cases} p_j & \text{if } m = 1, \quad j \quad \in \{1,2,\ldots,n\} \\ p_j \times p_k & \text{if } m = 2, \quad j,k \quad \in \{1,2,\ldots,n\} \\ p_j \times p_k \times p_l & \text{if } m = 3, \quad k,j,l \quad \in \{1,2,\ldots,n\} \\ \vdots & \end{cases} \tag{8-3}$$

where m represents the number of event sequences considered in the combination, and p_j represents the annual probability of occurrence for the j^{th} Category 1 event sequence (unitless). The j^{th} Category 1 event sequence is chosen m times from the full set of n Category 1 event sequences. If the condition in Eq. (8-3) is met, the total dose from Category 1 event sequences in that year (rem) is calculated as the sum of the event doses for the event sequences in the combination:

$$D_{\text{Category 1}}^{\text{Combination}} = \begin{cases} D_j & \text{if } m=1, \quad j \quad \in \{1, 2, ..., n\} \\ D_j + D_k & \text{if } m=2, \quad j,k \quad \in \{1, 2, ..., n\} \\ D_j + D_k + D_l & \text{if } m=3, \quad j,k,l \quad \in \{1, 2, ..., n\} \\ \vdots & \end{cases} \tag{8-4}$$

where D_j represents the event dose for the j^{th} Category 1 event sequence (rem). For a given number of event sequences in a combination, the total combination dose in that year, $D_{\text{Combination}}$ (rem), is calculated from the following expression:

$$D_{\text{Combination}} = \left(D_{\text{NO}}^{\text{Surface}} + D_{\text{NO}}^{\text{Subsurface}}\right)(1 \text{ year}) + D_{\text{Category 1}}^{\text{Combination}} \tag{8-5}$$

The maximum number of event sequences for which the probability criterion is satisfied for any combination of that number of event sequences [i.e., the maximum value of m for which Eq. (8-3) is true, m_{max}] can be obtained by solving the following expression:

$$m_{\text{max}} = \text{truncate}\left[\frac{\log(p_{\text{cutoff}})}{\log(p_{\text{max}})}\right] \tag{8-6}$$

where p_{max} represents the annual probability of occurrence for the Category 1 event sequence with the greatest frequency. Starting with the combination of one Category 1 event sequence ($m = 1$) in a year, the combination algorithm determines the Category 1 event sequences whose individual probabilities of occurrence are equal to or exceed p_{Cutoff} and organizes the single Category 1 event sequence in descending order of the event doses. The algorithm then advances to combinations of two Category 1 event sequences ($m = 2$). The algorithm determines the combinations of two Category 1 event sequences that satisfy Eq. (8-3) and organizes those combinations of two event sequences in descending order of the sum of their event doses. The algorithm then advances to the combinations of three Category 1 event sequences ($m = 3$), determines which combinations of three event sequences satisfy the probability criterion, and organizes those combinations of three event sequences in descending order of the sum of their event doses. The algorithm continues to advance the number of event sequences considered in a combination, m, until the probability criterion in Eq. (8-3) cannot be satisfied (i.e., until $m + 1 > m_{\text{max}}$).

In addition to entering the name, annual frequency, and dose for each Category 1 event sequence, the user can specify the annual cutoff probability for combinations of event sequences, p_{Cutoff}. Although the combination algorithm allows the user to specify different annual cutoff probabilities, the annual cutoff probability of 0.01 was selected as the default value because it is nearly equivalent to the Category 1 definition, for event sequences that are expected to occur 1 or more times during an assumed 100-year preclosure operational period before permanent closure. Actually, annual probabilities are not exactly equal to the expected number of occurrences within one year for a Poisson process. For small expected numbers of occurrences within a time period, the number of occurrences expected per year can be approximated by the annual probability of occurrence. A frequency of 0.02 year^{-1} is used in the following example. The expected number of occurrences within 1 year is 0.02. The probability of at least 1 occurrence within 1 year is $1 \times 10^{-0.02} = 0.0198$. For expected numbers of occurrences near the categorization boundary (between the Category 1 and Category 2), the difference between the number of occurrences expected per year and the annual probability of occurrence is typically less than a few percent. The approximation is less accurate for more frequent occurrences. To overcome this shortcoming, and to avoid results that could underestimate the potential occurrence of events and their consequences, the annual frequencies for the event sequences have been substituted for the annual probabilities, for screening purposes. Use of annual frequencies in place of annual probabilities ensures the occurrence of events and their consequences are not underestimated in this simplified approach (annual frequency is greater than or equal to the annual probability of occurrence, by definition).

For each number of event sequences in a combination, the combination algorithm tabulates the sum of event doses within a single year in descending order and the event sequences whose combinations correspond to the sums of event doses. The algorithm can also tabulate the sum of event doses in descending order and the event sequences that correspond to the sums of event doses for all numbers of event sequences in a combination. For a screening comparison to the public dose performance requirements, the maximum public dose in a single year expected to occur during the preclosure period was calculated by adding the largest sum of event doses, determined from all numbers of event sequences in a combination, to the user-specified annual doses for routine releases from the surface and subsurface facilities.

8.1.1.4 PCSA Tool Functions for the Compliance Assessment of Category 1 Event Sequences

The compliance assessment utility in the PCSA Tool is invoked from the Performance menu in the main menu bar followed by selection of the Project Results and Safety Assessment submenus. This operation will launch a dialog box with a form view entitled Results Table–Project View Base Case which displays, as shown in Figure 7-1, frequency and dose for all event sequences from the entire project (i.e., all functional areas). The frequency-weighted annual dose calculation and combination of event sequences are initiated by pressing the Safety Assessment button located at the bottom of the dialog box. The data displayed in Results Table–Project View Base Case cannot be edited from the dialog box. The frequency data for event sequences must be entered and edited from the Event Sequence, as discussed in Chapter 6, and total effective dose equivalent data must be entered and edited into the database from the Current Level Results menu. By default, event sequences associated with all listed event scenarios will be analyzed for compliance assessment; however, event scenarios and related event sequences can be deselected from the calculations from the Event Tree menu. This feature allows the user to conduct sensitivity analyses by choosing alternate event scenarios for safety assessment. In addition, the tool allows the user to select point estimate doses or mean doses (from probabilistic analysis) in safety assessment calculations.

As an illustrative example of a safety assessment, Figure 8-1 lists the event sequences, their frequencies, and their total effective dose equivalents to the public from the DOE preclosure analyses (CRWMS M&O, 2000b). Because the total effective dose equivalents were not reported by DOE for each Category 1 event sequence, the event doses were estimated from other Category 1 results based on the assumption that all Category 1 event sequences occurred with boiling water reactor fuel (use of the DOE results in this example does not imply acceptance of the DOE analysis or results).

The Safety Assessment button launches a small dialog box, which prompts the user to enter either 1, 2, or beyond Category 2 frequency limit (BCFL) for the category of the event sequence. Entering 1 and pressing the Search Now button modifies the Results table to only display the Category 1 event sequences, as shown in Figure 8-2. At the same time, a form, Safety Assessment Category 1 Event Sequences, opens up and allows the user to analyze Annualize Dose and Combination of Events.

The Frequency-Weighted Annual Dose section of the safety assessment displays the sum of the frequency-weighted doses for all Category 1 event sequences. After the user has entered the dose from releases due to normal operations, the Calculate button will then display the sum of the Frequency Weighted Sum and Normal Release doses in the Total Dose field. The total dose represents the frequency-weighted annual dose from all Category 1 event sequences and normal operations and can be compared with the regulatory dose limit (in rem/year) indicated in the field on the form just below the total dose field.

In the Combination of Events section of the safety assessment form, the user is prompted to enter the annual cutoff probability in the Frequency Cutoff field. The tool shows a default value of 0.01 for Category 1 event sequences. The Calculate button will execute a FORTRAN routine *Comban.exe* developed to evaluate the combination of event sequences based on the algorithm discussed in Section 8.1.1.3. At the completion of the calculation, the tool will automatically display the results on a Notepad window, as shown in Figure 8-3. In addition to the total number of possible combination sets, the tool shows the combination frequency, combination dose, and the event names sequences corresponding to each combination set of event sequences. The event-name listings in Figure 8-3 identify the event sequences by the functional identification and the event number.

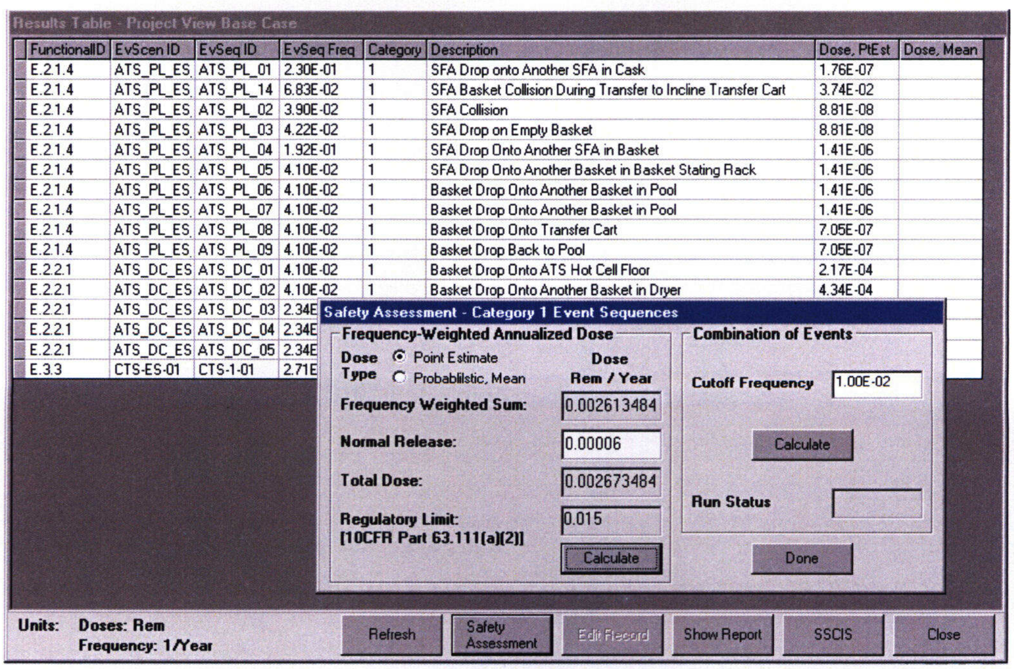
8.1.2 Worker Dose from Category 1 Event Sequences

The preclosure safety assessment utility of the PCSA Tool presents the hazard and consequence results for workers from those event sequences that include a release of radioactive gases into the assembly transfer cell from an underwater breach of spent nuclear fuel cladding. Because 10 CFR Part 63 does not stipulate any performance requirements for worker dose beyond the requirements of 10 CFR Part 20, the PCSA Tool allows the user to calculate the worker doses for each event sequence separately, so the results can be compared to the occupational dose requirements of 10 CFR Part 20. A detailed description of the worker dose calculation is presented in Section 8.2.

Results Table - Project View Base Case

FunctionalID	EvScen ID	EvSeq ID	EvSeq Freq	Category	Description	Dose, PtEst	Dose, Mean
E.2.1.2	ATS-CPP-ES	ATS_CPP_0	8.68E-03	2	Shipping Cask Drop Into Preparation Pit	2.36E-02	
E.2.1.3	ATS-PUL-ES	ATS_PUL_0	8.68E-03	2	Unsealed Shipping Cask Drop Into Cask Unloading Pool	2.39E-03	
E.2.1.4	ATS_PL_ES	ATS_PL_01	2.30E-01	1	SFA Drop onto Another SFA in Cask	1.76E-07	
E.2.1.4	ATS_PL_ES	ATS_PL_10	6.83E-03	2	ATS Basket Collision During Transfer	3.74E-01	
E.2.1.4	ATS_PL_ES	ATS_PL_11	6.83E-03	2	Uncontrolled Descent of Incline Transfer Cart	3.74E-01	
E.2.1.4	ATS_PL_ES	ATS_PL_12	1.74E-03	2	Handling Equip Drop Onto SFA Basket in Pool	3.74E-01	
E.2.1.4	ATS_PL_ES	ATS_PL_13	2.38E-03	2	Handling Equip Drop Onto SFA in Pool	9.36E-02	
E.2.1.4	ATS_PL_ES	ATS_PL_14	6.83E-02	1	SFA Basket Collision During Transfer to Incline Transfer Cart	3.74E-02	
E.2.1.4	ATS_PL_ES	ATS_PL_02	3.90E-02	1	SFA Collision	8.81E-08	
E.2.1.4	ATS_PL_ES	ATS_PL_03	4.22E-02	1	SFA Drop on Empty Basket	8.81E-08	
E.2.1.4	ATS_PL_ES	ATS_PL_04	1.92E-01	1	SFA Drop Onto Another SFA in Basket	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_05	4.10E-02	1	SFA Drop Onto Another Basket in Basket Stating Rack	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_06	4.10E-02	1	Basket Drop Onto Another Basket in Pool	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_07	4.10E-02	1	Basket Drop Onto Another Basket in Pool	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_08	4.10E-02	1	Basket Drop Onto Transfer Cart	7.05E-07	
E.2.1.4	ATS_PL_ES	ATS_PL_09	4.10E-02	1	Basket Drop Back to Pool	7.05E-07	
E.2.2.1	ATS_DC_ES	ATS_DC_01	4.10E-02	1	Basket Drop Onto ATS Hot Cell Floor	2.17E-04	
E.2.2.1	ATS_DC_ES	ATS_DC_02	4.10E-02	1	Basket Drop Onto Another Basket in Dryer	4.34E-04	
E.2.2.1	ATS_DC_ES	ATS_DC_03	2.34E-01	1	SFA Drop Onto Another SFA in Dryer	5.42E-05	
E.2.2.1	ATS_DC_ES	ATS_DC_04	2.34E-01	1	SFA Drop Onto ATS Hot Cell Floor	2.71E-05	
E.2.2.1	ATS_DC_ES	ATS_DC_05	2.34E-01	1	SFA Drop Onto Another SFA in DC	5.47E-05	
E.2.2.1	ATS_DC_ES	ATS_DC_06	6.95E-05	2	Handling Equip Drop Onto SFA in Hot Cell	2.78E-03	
E.2.2.1	ATS_DC_ES	ATS_DC_07	2.38E-03	2	Handling Equip Drop Onto SFA Basket in Hot Cell	7.46E-04	
E.3.3	CTS-ES-01	CTS-1-01	2.71E-02	1	Canister drop, canister intact no breach	0.0	
E.3.3	CTS-ES-01	CTS-1-02	2.88E-05	2	Canister drop, canister breach, HEPA available	1.6E-03	
E.3.3	CTS-ES-01	CTS-1-03	4.95E-12	BCFL	Canister drop, canister breach HEPA unavailable	2.3E-03	
E.4.1	DHS_CL_ES	DHS_CL_01	2.00E-03	2	Unsealed DC collision	1.53E-02	

Figure 8-1. Results Table with Example Data Based on the Results of the DOE Preclosure Analyses (CRWMS M&O, 2000b)



Results Table - Project View Base Case

FunctionalID	EvScen ID	EvSeq ID	EvSeq Freq	Category	Description	Dose, PtEst	Dose, Mean
E.2.1.4	ATS_PL_ES	ATS_PL_01	2.30E-01	1	SFA Drop onto Another SFA in Cask	1.76E-07	
E.2.1.4	ATS_PL_ES	ATS_PL_14	6.83E-02	1	SFA Basket Collision During Transfer to Incline Transfer Cart	3.74E-02	
E.2.1.4	ATS_PL_ES	ATS_PL_02	3.90E-02	1	SFA Collision	8.81E-08	
E.2.1.4	ATS_PL_ES	ATS_PL_03	4.22E-02	1	SFA Drop on Empty Basket	8.81E-08	
E.2.1.4	ATS_PL_ES	ATS_PL_04	1.92E-01	1	SFA Drop Onto Another SFA in Basket	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_05	4.10E-02	1	SFA Drop Onto Another Basket in Basket Stating Rack	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_06	4.10E-02	1	Basket Drop Onto Another Basket in Pool	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_07	4.10E-02	1	Basket Drop Onto Another Basket in Pool	1.41E-06	
E.2.1.4	ATS_PL_ES	ATS_PL_08	4.10E-02	1	Basket Drop Onto Transfer Cart	7.05E-07	
E.2.1.4	ATS_PL_ES	ATS_PL_09	4.10E-02	1	Basket Drop Back to Pool	7.05E-07	
E.2.2.1	ATS_DC_ES	ATS_DC_01	4.10E-02	1	Basket Drop Onto ATS Hot Cell Floor	2.17E-04	
E.2.2.1	ATS_DC_ES	ATS_DC_02	4.10E-02	1	Basket Drop Onto Another Basket in Dryer	4.34E-04	
E.2.2.1	ATS_DC_ES	ATS_DC_03	2.34E				
E.2.2.1	ATS_DC_ES	ATS_DC_04	2.34E				
E.2.2.1	ATS_DC_ES	ATS_DC_05	2.34E				
E.3.3	CTS-ES-01	CTS-1-01	2.71E				

Figure 8-2. Safety Assessment Interface for Category 1 Event Sequences Consisting of a Frequency-Weighted Annual Dose Calculation and an Analyses of Combination of Multiple Event Sequences within a Single Year where Doses Are Presented in Units of rem

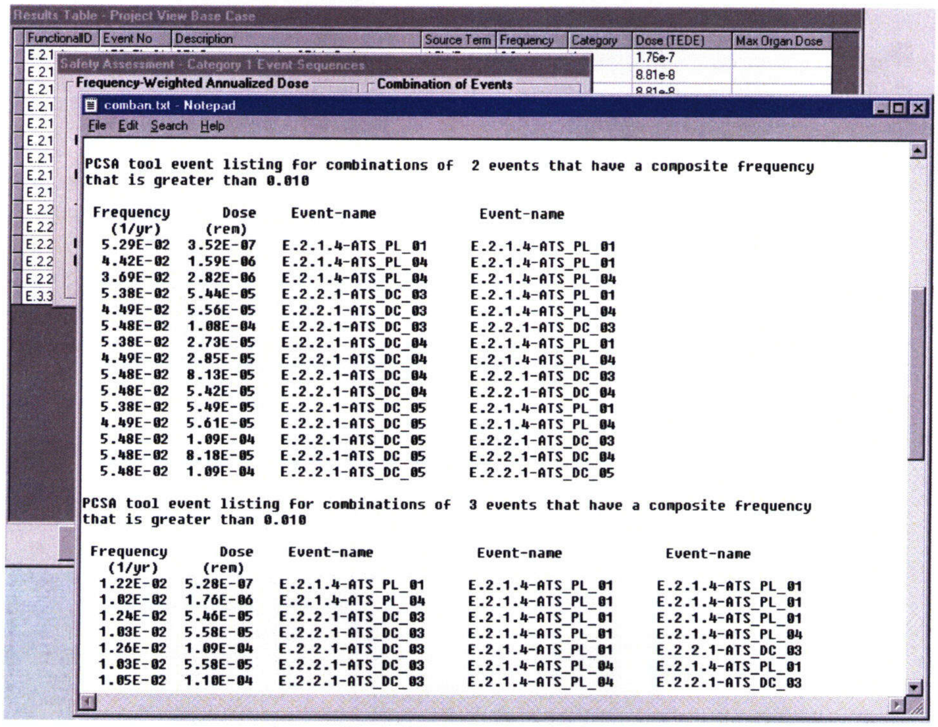


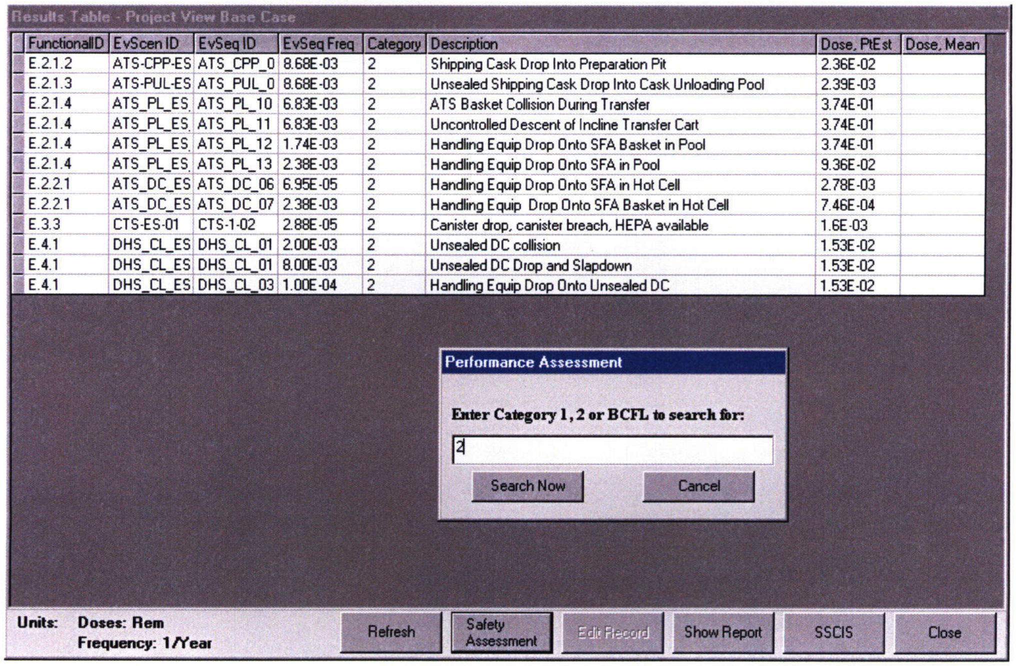
Figure 8-3. Output Screen for the Combination Anaysis

8.1.3 Category 2 Event Sequences

The regulation at 10 CFR Part 63 casts the performance requirement for Category 2 event sequences as an event dose limit to an offsite member of the public. Because there are no additional worker dose limits for Category 2 event sequences, the preclosure safety assessment utility of the PCSA Tool allows the user to tabulate the event doses to the public resulting from each Category 2 event sequence. The total effective dose equivalent, as well as the doses to individual organs, are compared with the performance requirements in 10 CFR Part 63 for Category 2 event sequences. Under the Performance header on the main toolbar, and after the search function is used, the total effective dose equivalent and maximum organ dose are displayed in the Results Table for each Category 2 event sequence (see Figure 8-4).

8.1.4 Preclosure Dose Limits

Category 1 event sequences are defined in 10 CFR 63.2 as those event sequences that are expected to occur one or more times before permanent closure of the geologic repository operations area. During normal operations and for Category 1 event sequences, 10 CFR 63.111(a)(2) stipulates that the annual total effective dose equivalent to any real member of the public (located beyond the site boundary and outside the Yucca Mountain site, Nellis Air Force Range, and the Nevada Test Site) shall not exceed 150 μSv [0.015 rem] specified in 10 CFR 63.204. The proposed repository at Yucca Mountain would be subject to the radiation regulations of 10 CFR Part 20, as invoked by 10 CFR 63.111(a). The regulations of 10 CFR Part 20 apply to normal operations and Category 1 event sequences.



Results Table - Project View Base Case

FunctionalID	EvScen ID	EvSeq ID	EvSeq Freq	Category	Description	Dose, PtEst	Dose, Mean
E.2.1.2	ATS-CPP-ES	ATS_CPP_0	8.68E-03	2	Shipping Cask Drop Into Preparation Pit	2.36E-02	
E.2.1.3	ATS-PUL-ES	ATS_PUL_0	8.68E-03	2	Unsealed Shipping Cask Drop Into Cask Unloading Pool	2.39E-03	
E.2.1.4	ATS_PL_ES	ATS_PL_10	6.83E-03	2	ATS Basket Collision During Transfer	3.74E-01	
E.2.1.4	ATS_PL_ES	ATS_PL_11	6.83E-03	2	Uncontrolled Descent of Incline Transfer Cart	3.74E-01	
E.2.1.4	ATS_PL_ES	ATS_PL_12	1.74E-03	2	Handling Equip Drop Onto SFA Basket in Pool	3.74E-01	
E.2.1.4	ATS_PL_ES	ATS_PL_13	2.38E-03	2	Handling Equip Drop Onto SFA in Pool	9.36E-02	
E.2.2.1	ATS_DC_ES	ATS_DC_06	6.95E-05	2	Handling Equip Drop Onto SFA in Hot Cell	2.78E-03	
E.2.2.1	ATS_DC_ES	ATS_DC_07	2.38E-03	2	Handling Equip Drop Onto SFA Basket in Hot Cell	7.46E-04	
E.3.3	CTS-ES-01	CTS-1-02	2.88E-05	2	Canister drop, canister breach, HEPA available	1.6E-03	
E.4.1	DHS_CL_ES	DHS_CL_01	2.00E-03	2	Unsealed DC collision	1.53E-02	
E.4.1	DHS_CL_ES	DHS_CL_01	8.00E-03	2	Unsealed DC Drop and Slapdown	1.53E-02	
E.4.1	DHS_CL_ES	DHS_CL_03	1.00E-04	2	Handling Equip Drop Onto Unsealed DC	1.53E-02	

Figure 8-4. Tabulation of the Category 2 Event Sequences

Category 2 event sequences are defined as those other event sequences that have at least 1 chance in 10,000 of occurring before permanent closure. The regulation at 10 CFR Part 63 requires that the consequence from each Category 2 event sequence not exceed a limit based on radiological dose equivalents but does not mandate calculations of risk (i.e., the product of consequence and frequency of occurrence). As a result of any single Category 2 event sequence until permanent closure has been completed, 10 CFR 63.111(b)(2) stipulates that no individual located on, or beyond, any point on the site boundary will receive the more limiting of a 0.05-Sv [5-rem] total effective dose equivalent or 0.5 Sv [50 rem] dose equivalent to any individual organ or tissue, including a shallow dose equivalent to the skin, but with the exception of a 0.15-Sv [15-rem] dose equivalent to the lens of the eye.

8.2 Assessment of Aggregate Risk

This section presents a risk assessment methodology incorporated into the PCSA Tool for evaluating aggregate risk from a potential repository during the preclosure period. The methodology also can be used to evaluate the reliance on structures, systems, and components that are important to safety as well as to investigate risk-based performance measures. Estimation of aggregate risk is not required by the NRC regulation in 10 CFR Part 63 (66 Federal Register 55732) and will not be used in compliance determination. However, estimation of aggregate risk is incorporated in the PCSA Tool for completeness and will be used for gaining risk insights. The preclosure risk assessment utility can treat Category 1 and 2 event sequences separately or together.

8.2.1 Risk Assessment Methodology

The geologic repository is composed of both active components, assumed to perform in a binary manner (i.e., it either functions or it does not), and passive components, some of which may not have a specific failure state, or where the failure is a matter of degree (e.g., 20 percent of function lost). During preclosure handling operations, the repository largely depends on active components whose failure could lead to the postulated top event and release radioactive material into the environment. For those structures, systems, and components that can be described as binary, the PCSA Tool can calculate importance measures that are typically used in nuclear power reactor evaluation such as Fussell-Vesley, Risk Reduction Worth, and Birnbaum. In contrast to the frequency-based importance measures for the nuclear power reactors, the methodology described in this paper investigates risk-based importance measures more suited to a geologic repository.

A complete list of n initiating events (E_x , x = 1,2,...,n) together with their annual frequencies (f_x) is generated. This list may be pruned based on a cutoff probability before proceeding any further. Through the use of event trees or alternate methods, a list of event sequences that may lead to an undesirable consequence (e.g., release of radioactive material to the environment) is developed for each E_x. Let us call these event sequences $s_{x,i}$, = 1,2, ...,m_x where m_x is the number of event sequences (these may be called release scenarios) for the x^{th} initiating event, E_x. A conditional probability $p_{i|x}$ for each $s_{x,i}$ (probability of $s_{x,i}$ occurring given that initiating event E_x occurs) is then estimated based on data or expert judgment or both.

For estimating the aggregate risk, we consider the possibility of multiple initiating events in the same year. In the most general case, the same initiating event may occur multiple times or a combination of different initiating events may occur simultaneously. Thus, there may be a very large number of scenarios that should be accounted for in the estimation of aggregate risk. To do this, we note that the annual frequencies, f_x, can be converted into initiating event probabilities by assuming the initiating event occurrences follow a Poisson process.

The basic steps for calculating the aggregate risk are:

(1) Convert the initiating event frequencies into initiating event probabilities

(2) Compute the initiating event consequences from their event sequence consequences and the conditional probabilities of the event sequences

(3) Identify the set of possible outcome states based on the occurrence of the initiating events, and

(4) Calculate the risk of each outcome state and the total risk from all outcome states using the initiating event probabilities and consequences.

<u>Step 1</u>. Convert the initiating event frequencies into initiating event probabilities

Due to large repetitions of handling operations and low component failure rates for a binomial process, Poisson statistics can be applied to determine $p(k)$, the probability of k occurrences of a particular initiating event within a given time duration:

$$p(k) = \frac{(np)^k}{k!} e^{-np} \tag{8-7}$$

where n represents the number of lifts in the year of interest (lifts) and p represents the failure probability (drops/lift or collisions/lift). Recognize, np represents the expected number of failures and is equivalent to the product of the failure rate (drops/year or collisions/year) and time duration (year). In the case of handling operations, failure data (recorded as failures per demand or as failures per hour of operation) are multiplied by the annual equipment usage at the facility (demands per year or hours of operation per year) to yield annual failure rates. Based on these annual failure rates and the fact that 10 CFR Part 63 stipulates annual dose requirements, 1 year is assigned as the time duration. The probability of k initiating events (of type x) occurring in 1 year becomes:

$$p_x(k) = \frac{(f_x \bullet 1 \text{ year})^k}{k!} e^{-(f_x \bullet 1 \text{ year})} \tag{8-8}$$

where f_x represents the frequency of the initiating event x (1 year). For $k = 0$, Eq. (8-2) reduces to $p_x(0) = e^{-f_x}$. Thus, the probability of at least one initiating event x occurring within the year of interest, denoted by P_x, is equal to $1 - e^{-f_x}$.

<u>Step 2.</u> Compute the initiating event consequences

The consequences arising from at least one initiating event x are calculated as the product of two components. The first component is the probability-weighted average of the event sequences corresponding to initiating event x:

$$c_x = \sum_{i=1}^{m_x} p_i|_x \, c_{x,i} \tag{8-9}$$

where $p_{i|x}$ represents the conditional probability of the ith event sequence occurring given initiating event x occurs, $c_{x,i}$ represents the consequence (rem) from the ith event sequence corresponding to initiating event x, and m_x represents the total number of event sequences for initiating event x. The second component is a multiplication factor to account for at least one initiating event occurring:

$$\frac{c_x \sum_{k=0}^{\infty} k \cdot p_x(k)}{P_x} \tag{8-10}$$

By definition, the product of the occurrence frequency and the time duration is also equal to the expected number of occurrences within the time duration. Using the Poisson notation in

Eq. (8-8) and letting $\lambda_x = (f_x \bullet 1 \text{ year})$, the expected number of occurrences of initiating event x can be described by:

$$\begin{aligned}
\sum_{k=0}^{\infty} k \cdot p_x(k) &= p_x(1) + 2p_x(2) + 3p_x(3) + \ldots \\
&= \frac{\lambda_x}{1!} e^{-\lambda_x} + 2\frac{\lambda_x^2}{2!} e^{-\lambda_x} + 3\frac{\lambda_x^3}{3!} e^{-\lambda_x} + \ldots \\
&= \lambda_x e^{-\lambda_x}\left[1 + \frac{\lambda_x}{1!} + \frac{\lambda_x^2}{2!} + \ldots\right] \\
&= \lambda_x e^{-\lambda_x} e^{\lambda_x} \\
&= \lambda_x
\end{aligned} \tag{8-11}$$

Recall, P_x is equal to $1 - e^{-f_x}$. Therefore, the multiplication factor in Eq. (8-10) can be simplified to:

$$\frac{(f_x \cdot 1 \text{ year})}{1 - e^{-(f_x \cdot 1 \text{ year})}} \tag{8-12}$$

Due to a mathematical simplification $\left(1 - e^{-z} \cong z, \text{ for small } z\right)$, the multiplication factor approaches unity as f_x becomes small.

Combining the two components, the consequences arising from at least one occurrence of initiating event x are described by the following relationship:

$$C_x = \frac{(f_x \cdot 1 \text{ year})}{1 - e^{-(f_x \cdot 1 \text{ year})}} \sum_{i=1}^{m_x} P_x|_x C_{x,i} \tag{8-13}$$

Step 3. Identify the set of outcome states

Each outcome state is based on the initiating events either not occurring or occurring at least once. The combinations of the outcome state must be determined. Because order is not important, the total number of combinations equals 2^n where n is the number of initiating events.

Step 4. Calculate the risk of each outcome state and the total risk from all outcome states

The outcome state probability is the product of the probabilities of each initiating event either not occurring or occurring at least once. For example, $P_1(1 - P_2)P_3(1 - P_4)$ represents the outcome probability for Initiating Events 2 and 4 not occurring and Initiating Events 1 and 3 occurring at least once. The outcome state consequence is simply the summation of the initiating event consequences occurring at least once. Following the earlier example, the outcome state consequence is equal to $C_1 + C_3$. The outcome state risk is calculated from the product of outcome state probability and outcome state consequence. The total risk is the summation of all outcome state risks.

By following the four steps above, the contributions to the aggregate risk from combinations can be condensed into generalized equations.

Risk from Combinations of One

$$\sum_{i=1}^{n} \lambda_i c_i \left(\prod_{\substack{x=1;\\ x \neq i}}^{n} e^{-\lambda_x} \right) \tag{8-14}$$

Risk from Combinations of Two

$$\sum_{\substack{i,j=1;\\ i \neq j}}^{n} \left[\lambda_i c_i \left(1 - e^{-\lambda_j}\right) + \lambda_j c_j \left(1 - e^{-\lambda_i}\right) \right] \left(\prod_{\substack{x=1;\\ x \neq i,j}}^{n} e^{-\lambda_x} \right) \tag{8-15}$$

Risk from Combinations of Three

$$\sum_{\substack{i,j,k=1;\\ i \neq j \neq k}}^{n} \begin{bmatrix} \lambda_i c_i \left(1 - e^{-\lambda_j}\right)\left(1 - e^{-\lambda_k}\right) \\ +\lambda_j c_j \left(1 - e^{-\lambda_i}\right)\left(1 - e^{-\lambda_k}\right) \\ +\lambda_k c_k \left(1 - e^{-\lambda_i}\right)\left(1 - e^{-\lambda_j}\right) \end{bmatrix} \left(\prod_{\substack{x=1;\\ x \neq i,j,k}}^{n} e^{-\lambda_x} \right) \tag{8-16}$$

And so forth.

It can be shown that summation of all contributions (i.e., the aggregate risk calculated here) equals the aggregate risk calculated by a simpler method (NRC, 1994). Such lengthy demonstrations, however, will not be presented in this report.

Over the operational period of the facility, the annual dose fluctuates with the number of event sequences occurrences. For example, some years will result in no radiological consequences; some years will result in radiological consequences from a single event sequences; and still other years will result in radiological consequences from multiple event sequences. The operational dose limit is an annual quantity which may not be exceeded in any year of operation. The degree to which the fluctuation in the event sequence occurrences lead to larger total annual doses (and their associated probabilities) is, therefore, of interest to the regulator. The methodology presented here provides this type of detailed information, which can not be obtained from the simple method.

An illustrative example of this methodology consisting of four initiating events has been previously presented (Benke, et al., 2002). Although the example data were from the Yucca Mountain project, there is no implication here that this methodology will be used by the NRC for regulatory compliance determination. Results of the risk assessment methodology can be applied in conjunction with a hypothetical "take-away" analysis that assumes the failure of a structure, system, or component to rank its importance with respect to safety. The resulting risk insights can serve as valuable information for highlighting aspects of facility design, applying quality controls, and focusing regulatory reviews.

8.2.2 PCSA Tool Functions for Risk Assessment

The risk assessment capability in the PCSA Tool is not fully functional. In this section, the proposed functionality is described. For calculating this aggregate risk, the tool executes the four steps described in Section 8.2.1.

The risk assessment capability in the tool would be exercised from the Performance menu in the main menu bar and by subsequently choosing the Project Results and the Risk Assessment submenus. Upon selecting the Risk Assessment, the tool would display a form labeled Risk Analysis as shown in Figure 8-5. The form shows a text field, Time for Risk Analysis, Calculation, which is an input for time of duration for risk evaluation. The default value is 1 year. The risk assessment formulation described in Section 8.2.1 is based on annual risk. In the Input Cutoff Limit for Combination of Probability of Events field, a cutoff limit is assigned for probability combinations as described in Step 4 in Section 8.2.1. The form would display a grid that shows the data for every event scenario from all functional areas chosen for risk assessment. As described in Section 6.2.1, all event scenarios are selected for risk assessment by default. Scenarios excluded from this analysis are deselected from the Event Tree form. The grid initially shows Functional ID, Event Scenario ID, Event Scenario Description, Time for (risk) Calculation (year), Initiating Event ID, and Initiating Event Frequency (1 yr). The fields in the grid labeled Event Probability, (event) Dose Point Estimate, and Mean Dose, Min(imum) Dose, 5- 50- 95 percent Dose, and Max(imum) Dose from probabilistic calculations, would be calculated by further operations.

The event probability for every event scenario would be evaluated using the Calculate Event Probability button located at the bottom of the form Risk Analysis form.

Double-clicking on each Event Scenario ID would bring up the dialog box Event Scenario Risk, as shown in Figure 8-6. The Event Scenario Risk form would display existing data on the event scenario: Event Scenario ID, Time for (risk) calculation and Initiating Event Frequency (1 year), and Event Probability. The Event Point Estimate Dose and Event Main Dose fields would be initially empty. The form would also display data associated with the event scenario in a grid showing Functional Area, Event Sequence ID and Event Sequence frequency, Type of Run, and Consequence Path, showing directory paths where the files from consequence analysis runs are stored from either point estimate or probabilistic runs. The Event Scenario Risk dialog box allows calculation of point estimate and probabilistic event dose using the Event Dose button. The Event Dose button would automatically create input data and execute a Fortran routine pcsa_ietccdf.exe in the background. At the end of the calculation, the Event Dose Point Estimate and Event Dose Mean field would be populated. The tool calculates point estimate or probabilistic event dose based on the type of run, D or P, specified in the Type of Run field in the grid. For probabilistic calculation, the tool would also create a file containing complementary cumulative distribution function data for event dose and assign a path for data storage. In this fashion, the user would select one event scenario at a time from the Risk

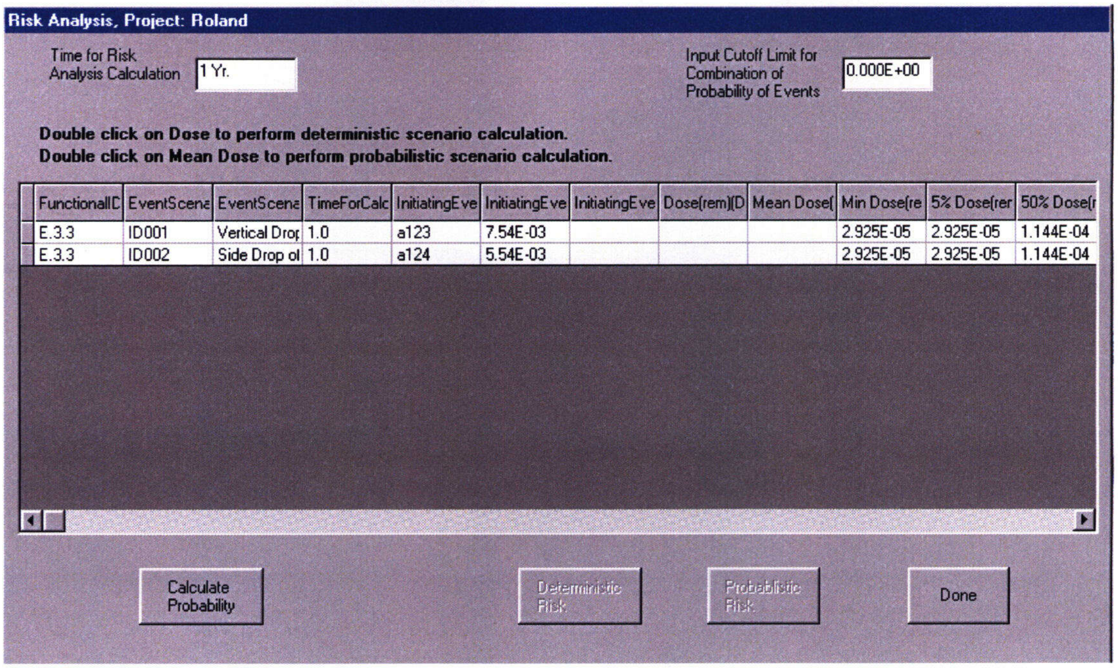


Figure 8-5. Output Screen Showing Event Scenario Risk Form

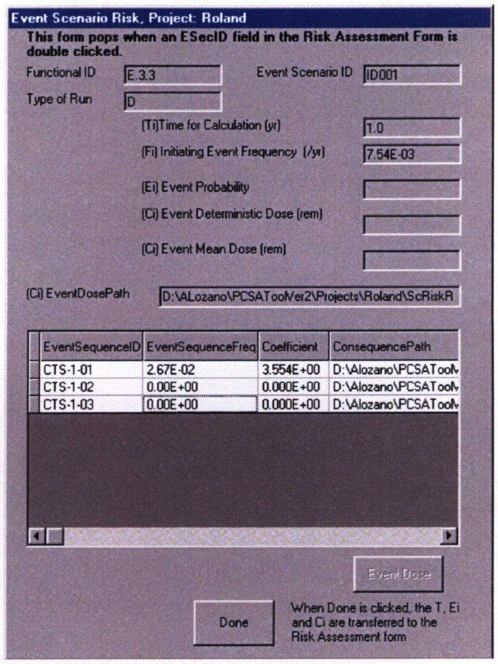
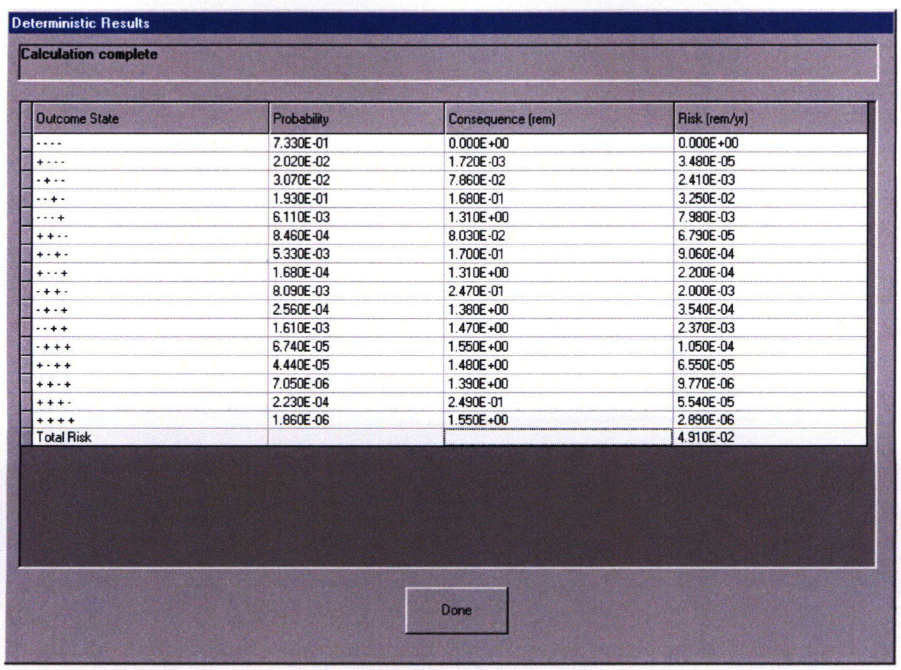


Figure 8-6. Output Screen Showing Risk Analysis Form

Analysis dialog box (Figure 8-5) and calculate the event dose and probability for each event scenario.

The user would then calculate total system risk by selecting the Deterministic Risk or Probabilistic Risk buttons as shown in Figure 8-5. The Deterministic Risk button would calculate risk using point estimates for the parameters and would display the Deterministic Results form (Figure 8-7) showing a grid with Outcome, Probability/yr, Consequence, and Risk fields. The Outcome field shows results of outcome analysis with each column representing an event. The + sign for a given event indicates that the event did occur and a - sign indicates that the event did not occur. The probability, consequence, and risk for each outcome will be shown in respective fields and at the end the total risk will be calculated. The probabilistic risk calculations are conducted by clicking on the Probabilistic Risk button. The Probabilistic Results form is displayed, which is shown in (Figure 8-8), the plot of the complementary cumulative distribution function of total risk and also shows the mean, Minimum, 5-, 50-, 95-percent, and maximum risk values at the top.



Outcome State	Probability	Consequence (rem)	Risk (rem/yr)
- - - -	7.330E-01	0.000E+00	0.000E+00
+ - - -	2.020E-02	1.720E-03	3.480E-05
- + - -	3.070E-02	7.860E-02	2.410E-03
- - + -	1.930E-01	1.680E-01	3.250E-02
- - - +	6.110E-03	1.310E+00	7.980E-03
+ + - -	8.460E-04	8.030E-02	6.790E-05
+ - + -	5.330E-03	1.700E-01	9.060E-04
+ - - +	1.680E-04	1.310E+00	2.200E-04
- + + -	8.090E-03	2.470E-01	2.000E-03
- + - +	2.560E-04	1.380E+00	3.540E-04
- - + +	1.610E-03	1.470E+00	2.370E-03
- + + +	6.740E-05	1.550E+00	1.050E-04
+ - + +	4.440E-05	1.480E+00	6.550E-05
+ + - +	7.050E-06	1.390E+00	9.770E-06
+ + + -	2.230E-04	2.490E-01	5.540E-05
+ + + +	1.860E-06	1.550E+00	2.890E-06
Total Risk			4.910E-02

Figure 8-7. Output Screen Showing Deterministic Results Form

Figure 8-8. Output Screen Showing Probabilistic Results Form

9 STRUCTURES, SYSTEMS, AND COMPONENTS IMPORTANT TO SAFETY

An important purpose of the tool is to review the U.S. Department of Energy (DOE) identification of structures, systems, and components important to safety for completeness and appropriateness for the proposed repository. The identification and classification of structures, systems, and components important to safety are necessary to assure the health and safety of the public and facility workers are adequately protected. As required in 10 CFR Part 63, the preclosure safety analysis must be used to identify structures, systems, and components important to safety and demonstrate compliance with the performance objectives contained in 10 CFR 63.111. Structures, systems, and components important to safety must be identified based on their capabilities to prevent or mitigate potential event sequences that have the potential to exceed the regulatory limits for normal operations, and Category 1 event sequences, and to prevent or mitigate the dose consequence of Category 2 event sequences. The acceptance criteria and review methods, addressed in Section 4.1.1.6 of the Yucca Mountain Review Plan NRC (2002a), are based on meeting the requirements of 10 CFR 63.112(e) related to the identifying structures, systems, and components important to safety and 10 CFR 63.142(c)(1) related to categorizing the structures, systems, and components. Consistent with the guidance provided in NRC (2002a), the staff would verify that analysis and identification of structures, systems, and components for the geologic repository operations area used the results of the iterative preclosure safety analysis (i.e., identification of hazards and initiating events; identification of event sequences; and consequence analyses). Additionally, staff would confirm that the DOE analyses include all structures, systems, and components and controls that should be functional to meet the performance objectives. Further the staff would confirm that structures, systems, and components are classified as important to safety according to the definition specified in 10 CFR 63.2. The tool module associated with this activity is in the development stage and will be modified based on the staff review and suggestions.

9.1 Concept

The capability for review of structures, systems, and components important to safety has been introduced in the current version of the PCSA Tool at a conceptual level. This feature will be improved when the DOE identification process and staff position on the review methodology are finalized.

During preclosure operations, the repository depends on active components whose failure could lead to the postulated top event and eventual release of radiological dose to the public and workers. For those structures, systems, and components that can be described as binary (i.e., it either functions, or it does not), the tool can calculate importance measures that are typically used in nuclear power reactor evaluation such as Fussell-Vasley, Risk Reduction Worth, and Birnbaum. Since preclosure operations consist of many independent stages corresponding to different radiological source terms, frequency-based importance measures for nuclear power reactors will not be applicable. In light of this fact, and consistent with the risk-informed performance-based regulation in 10 CFR Part 63, the tool has been designed to investigate dose-based importance measures.

The identification of structures, systems, and components important to safety is accomplished by an importance analysis. The importance of a structure, system, or component is assessed by considering that the probability of an event associated with the failure of a structure, system, or component is equal to 1.0 and then reevaluating the consequence for the modified Category 1 or Category 2 event sequences. The modified event sequence (i.e., event tree and fault tree models) is reanalyzed and event sequence frequencies may change as a result. Performance of the facility is reassessed with the modified results using the annualized dose approach for Category 1 event sequences or the event dose for Category 2 event sequences. If the dose exceeds the performance requirements (specified by 10 CFR 63.111) with the structure, system, or component not functional, then the structure, system, or component is considered to be important to safety. The DOE presented an approach to identification and quality assurance categorization of structures, systems, and components important to safety (Bechtel SAIC Company, LLC, 2002). The DOE methodology for identification and categorization of structures, systems, and components is under staff review.

9.2 PCSA Tool Function to Identify Structures, Systems, and Components Important to Safety

The analysis for identification of structures, systems, and components important to safety is executed through the tool by first selecting the Safety Assessment submenu accessed from the Project submenu located under the Performance menu in the main menu bar. The Safety Assessment menu launches a dialog box that shows a table containing the results of those event scenarios and event sequences from all the functional areas that have been selected. The data are displayed in the form view entitled Results Table–Project View Base Case. It is assumed that the performance objectives are met with all planned structures, systems, and components operating as designed.

The importance analysis is performed by the user reevaluating the event scenario by assigning the probability for the event associated with the structure, system, or component equal to 1.0 and reanalyzing event tree and fault tree models. The event sequence frequencies will be modified with respect to the basecase analysis, and the number of event sequences in the event scenario may be reduced. A new dose calculation including the failed structure, system, or component may also be required. At the bottom of the Results Table dialog box there is an SSCIS button (see Figure 9-1) that launches another dialog box, the Results Table-Project View SSCIS Case that looks similar to the basecase table. The table under SSCIS shows all the results from the basecase table except that it has some additional columns with headers SSC and Enable PA Code. In this table, columns under Event Frequency, Dose, SSC, and Enable PA Code can be edited. The fields in the Enable PA code column have the option of Yes or No (the default setting for this column is Yes). This feature allows the user to disable any event sequence from the safety assessment calculation and may be particularly helpful for analyzing Category 1 event sequences. The new values for the frequency and dose can be entered in the Results Table Project View Structure, SSCIS Case table, only for the event sequences affected by the failure of a particular structure, system, or component.

The identification of a structure, system, or component important to safety is made using an annualized dose approach for Category 1 event sequences where the resulting annualized dose is compared with the performance measures. The event dose for each Category 1 and 2 event sequence is compared with the annual and event dose limits, respectively. If the performance without the structure, system, or component functioning exceeds the regulatory limits, the structure, system, or component is considered to be important to safety.

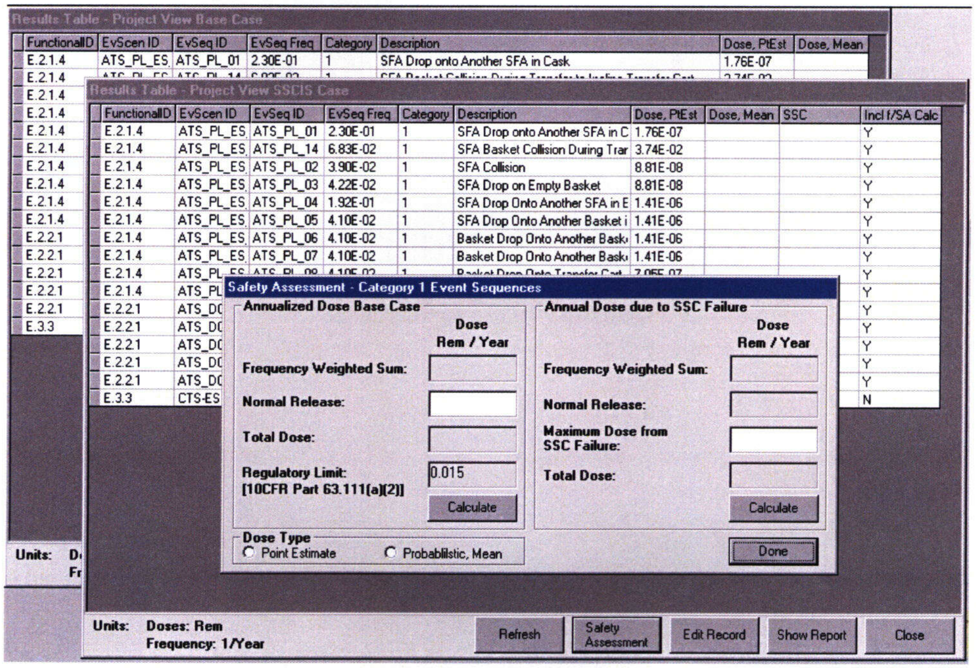


Figure 9-1. Example of Importance Analysis for Structures, Systems, and Components Important to Safety

10 EXAMPLE ANALYSIS USING THE PCSA TOOL

10.1 Introduction

In this chapter, preliminary example analyses are described on a portion of the assembly transfer system using the PCSA Tool. The objective is to demonstrate, through a series of examples, how independent analyses may be performed on selected portions of the U.S. Department of Energy (DOE) preclosure safety analysis to identify areas of vulnerability, check the DOE calculations for worker and public dose, or identify structures, systems, and components important to safety. A step-by-step approach is used to accomplish the example analyses to fully demonstrate the various sections of the tool.

The PCSA Tool consists of several modules designed to conduct qualitative as well as quantitative analysis. The modules are discussed in detail in Chapter 3. The aim is to demonstrate the various modules of the PCSA Tool by performing a full range of qualitative and quantitative analyses. A main window and menu bar are used to navigate through the various programs, forms, tables, and reports needed to perform the analyses according to the methodology discussed in Chapter 3.

The assembly transfer system moves spent nuclear fuel assemblies from transportation casks into disposal containers for emplacement into the repository. The process begins with receipt of loaded transportation casks from the carrier/cask handling system and receipt of empty disposal containers from the Disposal Container Handling System (DOE, 2001b). The casks are prepared for unloading by sampling the gas in the cask cavity, followed by venting and cool-down of the cask. These operations are performed in the Cask Preparation and Handling Area. The casks are next transferred to the Cask Unloading Pool for removal underwater of the contained spent nuclear fuel assemblies and transfer to the Dry Assembly Transfer Cell where the casks are dried and loaded into disposal containers. The disposal containers are temporarily filled with inert gas, sealed, and sent to the Disposal Container Handling System (see Figure 10-1). To meet the thermal loading criteria for the disposal containers, spent nuclear fuel assemblies may be stored and blended in the Fuel Blending and Storage Pools before transfer to the Dry Assembly Handling Transfer Cell for loading into the disposal containers. Nonstandard fuel assemblies are repackaged to meet waste package criteria (see Figure 10-2) (DOE, 2001b).

The assembly transfer system can be divided into four functional subareas: (i) cask unloading area, (ii) disposal container loading area, (iii) fuel blending and storage pools, and (iv) nonstandard fuel handling area (CRWMS M&O, 2000h). The example analyses in this chapter focus on the Cask Preparation and Decontamination Room 1, which is located within the first subarea (cask unloading area), and demonstrate the working of the PCSA Tool and its capabilities.

DOE published design information consisting of system description, process flow diagrams, mechanical flow diagrams, conceptual description of operations, and frequency and consequence calculations, is used as inputs in developing the various analyses. Because the

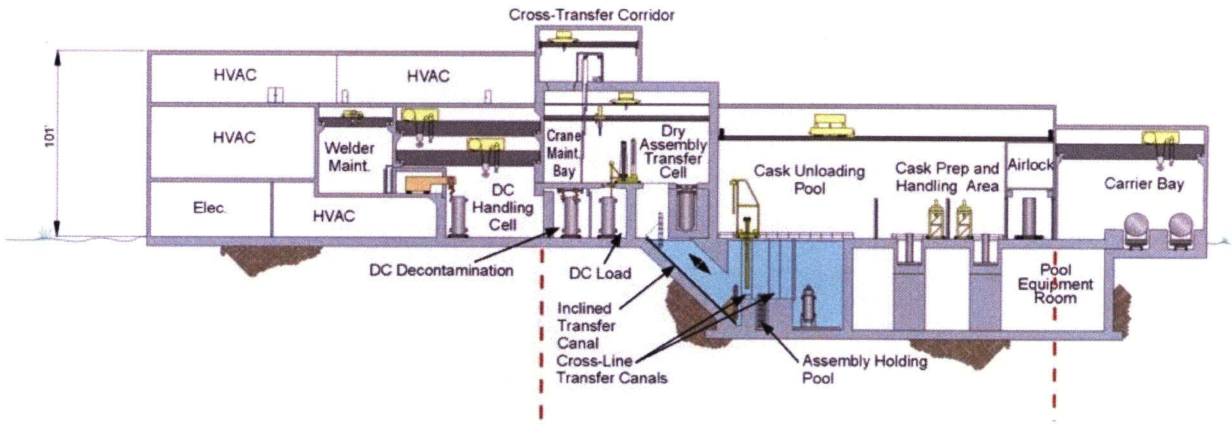


Figure 10-1. Assembly Transfer System in the Waste Handling Building (DOE, 2001b)

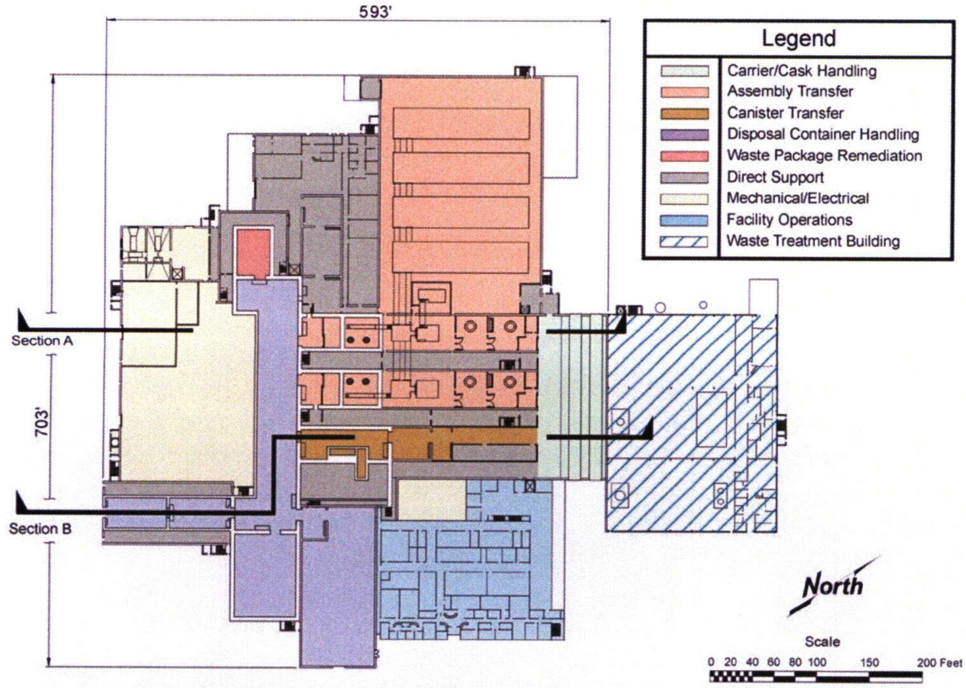


Figure 10-2. Waste Handling Building Layout Showing Assembly Transfer System (DOE, 2001b)

DOE design is preliminary at this stage, assumptions have been made in developing the analyses. These have been stated in the analyses.

10.2 Functional Area

A hierarchal approach is employed to divide the facility and operations of the geologic repository operations area into functional areas by specific function, physical area of the facility, or process. As discussed in Chapter 3, the functional area defines the boundary of the safety analysis. Design information consisting of system description, process flow diagrams, mechanical flow diagrams, and conceptual descriptions of operations is used as input in developing the hierarchal scheme.

The first step in performing the example analyses in the assembly transfer system area of the facility is to click on the Functions button in the PCSA Tool main menu and generate a hierarchal scheme for dividing the geologic repository operations area into functional areas. The hierarchal scheme generated for the example analysis is given in Table 10-1, in the Project Tree dialogue box (Appendix D, page D–2), and in the PCSA Project Tree Report (Appendix D, page D–3). In this scheme (see Table 10-1), the Waste Handling Building has been assigned the Functional Identification E; the assembly transfer system, which is located in the Waste Handling Building, is assigned the Functional Identification E.2; the Cask Unloading Area, which is a part of the assembly transfer system, is assigned the Functional Identification E.2.1; and finally, the Cask Preparation and Decontamination Room 1, which is part of the Cask Unloading Area, is assigned the Functional Identification E.2.1.2. As previously stated, the Cask Preparation and Decontamination Room 1 is the functional area chosen for the example analysis (Functional Identification No. E.2.1.2 in The PCSA Initial Information Report in Appendix D, page D–3).

10.3 Identification of Human-Induced Internal Events

Hazards from the operations in the subfunctional areas in the assembly transfer system are identified in this section.

10.3.1 System Description

Once the functional area for the subsystem or location being considered has been identified and a hierarchal scheme constructed, the next step is to click on the System menu in the PCSA Tool main menu bar, and then click on Sysdesc in the submenu. System description information for the operations occurring in the subsystem or location being considered is then entered onto the System Description Form and is displayed in the System Description Report in the PCSA Tool. Information to be entered includes a description of the functions of the system being analyzed, detailed step-by-step sequence of operations and human interactions, equipment used, remarks, and DOE references used.

For the Cask Preparation and Decontamination Room 1, the main operations occurring are (see Figure 5-7, Chapter 5): receipt of rail and truck transportation casks with impact limiters removed, transfer of the cask to the cask preparation pit, gas sampling of the cask or contained dual-purpose canister cavity, venting and cool down of the cask or dual-purpose canister, cask

Table 10-1. Example of Hierarchal Scheme for Dividing the Geologic Repository Operations Area into Functional Areas	
Functional Identification	**Description**
E	Waste Handling Building
E.2	Assembly Transfer System
E.2.1	Cask Unloading Area
E.2.2	Disposal Container Loading Area
E.2.3	Fuel Blending and Storage Pools
E.2.4	Nonstandard Fuel Handling Area
E.2.1.1	Airlock in Cask Unloading Area
E.2.1.2	**Cask Preparation and Decontamination Room 1**
E.2.1.3	Cask Preparation and Decontamination Room 2
E.2.1.4	Cask Unloading and Staging Pool

lid removal and unbolting of the shield plug, and transfer of the open cask to the unloading pool for removal of its contents. The main equipment used to accomplished these operations includes cask transfer carts, a bridge crane, cask or dual-purpose canister lifting yoke and fixtures, access platforms for the pit area, and the cask preparation manipulator (for remote operations in the pit area) (CRWMS M&O, 2000h).

The information entered onto the System Description Form for the Cask Preparation and Decontamination Room 1 (see Appendix D, page D–4) is displayed in the System Description Report (Appendix D, page D–5). This information includes a set of 17 sequential operations that will be performed at this location, a list of equipment to be used in performing the operations, and a list of references to DOE documents giving information on the proposed mode of operations. Because the DOE design is preliminary at this stage, assumptions have been made in developing the operations sequence. These assumptions appear with accompanying question marks in the report. For example, it is not known at present whether hooking the cask lifting yoke onto the cask will be performed remotely or manually. This has been indicated in the Operations Sequence Step 3 in the System Description Report (Appendix D, page D–5) by the statement in brackets as follows: "No gantry mounted manipulator available to assist operations in this location. Assume this is done manually using the bridge crane ?."

Finally, clicking on the submenu item Inventory (under the main menu item System) will display information on the various types of canisters, maximum annual throughput, transportation casks data, and disposal containers to be used at the repository. This information will be useful in proceeding with the hazard analysis.

10.3.2 Hazard Analysis

After completion of the System Description as described in the preceding section, the next step is to perform an Internal Hazard Analysis using Energy Analysis, Failure Modes and Effects Analysis, or What-If Analysis. Energy Analysis identifies hazards associated with each operation by considering the energy associated with each operational step in the process. What-If Analysis focuses on facility hazard and human error analysis, and failure modes and effects analysis focuses on the hardware and equipment failures that may result in radiological consequences. Depending on the functional area of interest, one may choose perform any or all of the analyses. These analyses are best performed by a team of persons with expertise in different aspects of the process/equipment design and operations. The results of the analysis are dependent to a great extent on the experience and skill of the team members involved.

A failure modes and effects analysis is performed for the operations occurring in the Cask Preparation and Decontamination Room 1 (Functional Area E.2.1.2). This analysis is accomplished by first clicking on the Internal Hazard Analysis button in the main menu, then clicking on the failure modes and effects analysis option in the submenu, and finally clicking on the Failure Modes and Effects Analysis form. The various fields in the Failure Modes and Effects Analysis form are then filled out to produce the PCSA Failure Modes and Effects Analysis Report.

The failure modes and effects analysis builds on the Operations Sequence identified in the System Description Report described in the previous section. For each of the 17 sequential operational steps identified in the System Description Report, the failure modes of the associated equipment and the effects of each failure are examined and recorded-onto the Failure Modes and Effects Analysis form. Based on the consequence and frequency of failure, each item is further categorized qualitatively as being a severe event or not. The category of the item is entered in the remarks section of the Failure Modes and Effects Analysis form (Appendix D, page D–7). The results of the analysis are displayed in the PCSA Failure Modes and Effects Analysis Report (Appendix D, pages D–8 through D–16).

For example, Operations Sequence step #16 in the System Description Report (Appendix D, page D–5) deals with the attachment of the yoke to the cask in preparation for lifting and transferring the cask over the cell partition walls and into the cask unloading pool, using the bridge crane. A failure modes and effects analysis is conducted on the equipment to be used in Operations Sequence step #16 (i.e., the cask lifting yoke), and the results are displayed as Item No. 0025.00 in the PCSA Failure Modes and Effects Analysis Report (Appendix D, page D–16). The failure modes and effects analysis is conducted for the yoke by filling out the fields of the Failure Modes and Effects Analysis form (see Appendix D, page D–7), as follows. The causes of failure for the yoke are identified as structural failure of the yoke and improper attachment of the yoke to the cask. The effect of the failure is the drop of the cask/dual-purpose canister. The recommended safeguards and controls are administrative control and proper attachment design. Safeguards identified by the DOE in its reports are also identified in the form, and provide a ready comparison with the list of recommended safeguards from the failure modes and effects analysis. In the case of this item, there are no safeguards identified by the DOE in its reports. Finally, this item is categorized as a "Severe" event on the form because the effect of the yoke failure will be a drop of the cask from a height ~7.6 m [~25 ft] (i.e., the lift height needed for the cask to clear the cell partition walls) (CRWMS M&O, 2000h). Because this drop height exceeds the design basis drop height for a cask without impact limiters (CRWMS M&O, 1998a), the cask is expected to rupture, causing a radiological release from the spilled spent nuclear fuel assemblies. In addition, because the cask lid will be removed and the shield plug unbolted prior to this lift (CRWMS M&O, 2000h), even a tip-over of the cask can result in spilling the contained spent nuclear fuel assemblies, causing a radiological release within the cell. Lastly, because human error could be involved in the cask drop (i.e., attachment of the yoke would involve operator action), the estimated frequency for this event may be relatively high. This item, therefore, is designated as being a "Severe" item in the PCSA Failure Modes and Effects Analysis Report. The reasons for considering this to be a "Severe" event are documented under the remarks column for this item (Item No. 0025, Appendix D, page D–14).

All "Severe" events identified in the PCSA Failure Modes and Effects Analysis Report are compiled in the PCSA Event Analysis Report (see Appendix D, page D–17 through D–20). In the case of the example of the Cask Preparation and Decontamination Room 1 described in the preceding text, 26 severe events are identified. Some of these items have been conservatively classified as severe events; further information is needed to better determine if these are indeed severe events. In such cases, the phrase "Need more information on system" has been included in the Remarks column of the report.

10.3.3 Failure Checklist

A failure checklist database library is used to assist in hazard analysis. The database library contains the modes of equipment failure and list of possible internal events.

For example, the checklist may be used to determine the various failure modes of a crane. This is accomplished by first clicking on the Checklist button in the main menu, then typing crane in the search box, followed by clicking the Search button. The various failure modes for cranes will be displayed on the screen (see Failure Modes and Effects Analysis Component Failure Mode Checklist in Appendix D, page D–21).

10.3.4 Failure Rate Database

The failure rate database is a comprehensive database library of failure rates of equipment from actuarial data. The failure rates are used to determine the probability of failure of the structures, systems, and components during the postulated 100-year operation before permanent closure, and are most commonly used as inputs for construction of event trees and fault trees for conducting frequency analysis, as explained in the next section (see Section 10.4). For example, failure-rate data for the components of a crane may be needed to construct a fault tree for determining the probability of a cask drop. These data are obtained from the failure rate database in the tool by first clicking on the Failure Rate in the main menu, then clicking on Search Database in the submenu and typing crane in the submenu form to obtain a list of crane related data. Finally, one selects the data that most closely match the needs of the fault tree being developed. In this case, the component failure data for bridge cranes, given under the reference Reliability Techniques Used in the Assessment of Cranes (Duke, 1985), (i.e., reference U in the database display) may be used (see Figure 6-3, Chapter 6).

Alternatively, the taxonomy tree may be used to locate the same data in the database. This is achieved by clicking on the View Taxonomy option in the submenu, and then scrolling down the tree structure to Crane Systems. A submenu with several crane related options is displayed. Clicking on Crane will display the same list of crane related data from which the crane component failure data given under the reference Reliability Techniques Used in the Assessment of Cranes (Duke, 1985) may be chosen as before.

10.4 Frequency Analysis

Severe Events identified in the Hazard Analysis module are used as input for Frequency Analysis for development of Category 1 and Category 2 design basis event sequences. Input information for conducting fault tree and event tree analysis is first compiled in the Event Tree Analysis form (see Appendix D, page D–22) and displayed in the PCSA Event Scenario Report (see Appendix D, page D–23). Based on this information, fault tree and event tree analyses are subsequently performed using SAPHIRE code under the SAPHIRE menu item. Two examples of frequency analyses performed on "Severe" events identified in the previous section are given in the text that follows. These examples illustrate how the PCSA Tool may be used to check for potential deficiencies and vulnerabilities in the DOE design.

Radiological Release Due to Breach of Cask Containing Bare Spent Nuclear Fuel Assemblies

This example illustrates how an independent event tree analysis can be performed using the PCSA Tool. The analysis is performed on a selected event sequence scenario using DOE-generated failure rates and probabilities to uncover a Category 1 internal design basis event sequence that has been inappropriately classified as two Category 2 event sequences in the DOE preclosure safety analysis.

The event scenario involves the drop of a cask containing bare spent nuclear fuel assemblies from a height exceeding the design basis height, so that the drop results in a breach in the cask and a radiological release within the cell from the spilled spent nuclear fuel assemblies. The sequence of events to be considered in the event tree analysis is (i) drop of cask, (ii) breach of cask and radiological release within the cell, and (iii) with and without functional high-efficiency particulate air filtration system. The scenario is developed in detail in the text that follows.

In the Cask Preparation and Decontamination Room 1, the bridge crane is employed for all lifts involving the cask. The probability of a load drop involving a bridge crane has been estimated at 1.4×10^{-5}/lift (CRWMS M&O, 1998a). Further, the design basis drop height for a cask without impact limiters is 2.1–2.7 m [7–9 ft] (CRWMS M&O, 1998a). In the Cask Preparation and Decontamination Room 1, this maximum drop height is expected to be exceeded during two crane operations: (i) lowering the cask into the cask preparation pit {the drop height to the bottom of the pit is about 4.6 m [15 ft]} and (ii) transferring the cask over the cell partition walls and into the cask unloading pool {the drop height is estimated to be approximately 7.6 m [25 ft]} (CRWMS M&O, 2000h). Transportation casks to be processed in the assembly transfer system will contain dual-purpose canisters or uncanistered spent nuclear fuel assemblies. The latter will be more likely to result in radiological release on breach of the cask. The annual number of vulnerable casks may be estimated from the DOE report (CRWMS M&O, 1999b). Per Table 2-2 in the referenced report, up to 551 casks will be processed annually, and the 551 casks will contain 22 dual-purpose canisters (CRWMS M&O, 1999b). If each cask is assumed to hold 1 dual-purpose canister (conservative assumption), there can be 529 casks holding uncanistered spent nuclear fuel assemblies that could result in radiological release on breach of the cask.

Number of cask lifts that exceeds 2.7 m [9 ft] = (529 casks/year) * (1 lift into pit/cask + 1 lift to pool/cask) = 1,058 lifts/year

Frequency of cask drops expected to result in radiological release = 1,058 lifts/year * 1.4×10^{-5} drops/lift = 1.48×10^{-2}/year

Information needed to conduct the frequency analysis for the noted event scenario is compiled using the Event Tree Analysis form in the PCSA Tool. This form is activated by clicking on the Freq. Analysis button in the main menu and then clicking on the Event Tree button. Clicking on the Frequency Calculation button within the Event Tree Analysis form will display a calculator. The frequency of the initiating event (i.e., the frequency of cask drop) is calculated within the form by typing 1.4×10^{-5} drops/lift and 1,058 lifts/year in the calculator fields. The description and probabilities of subsequent events are next entered in the appropriate fields in the form (see Event Tree Analysis form in Appendix D, page D–22). The DOE supplied value of 1.7×10^{-7} (CRWMS M&O, 1999i) is entered for the probability of high-efficiency particulate air filter failure in the form. The sources for the failure rate information used are entered in the remarks field of the form. The results are displayed in the PCSA Event Scenario Report (see Appendix D, page D–23).

An event tree is then modeled for the Cask Drop and Breach Initiating Event using the SAPHIRE code (see Appendix D, page D–24). Event sequence #2 of the event tree involves the cask drop and breach followed by radiological release within the cell with the high-efficiency particulate air filtration system functional. The sequence is found to have a frequency of 1.48×10^{-2}, and can, therefore, be classified as a Category 1 Design Basis Event Sequence.

It should be noted that this event sequence has not been included in the 14 Category 1 Internal Design Basis Event Sequences listed in the present DOE analysis (CRWMS M&O 2000e, Table 5-5). Instead, this event sequence has been classified by the DOE as two separate Category II sequences, Events #2-11 and #2-12 in the table entitled Design Basis Event Frequency Calculations (CRWMS M&O 2000f, page VII-5). Because a single bridge crane will be used in the operation, and the event scenario of interest involves the radiological release from the drop and subsequent breach of a cask containing bare spent nuclear fuel assemblies, the two event sequences should be combined into one event sequence in the DOE analysis.

This example illustrates the value of the PCSA Tool in ensuring that potential Category 1 event sequences are not downgraded to Category 2 event sequences in the DOE preclosure safety analysis.

Radiological Release Due to Yoke Drop on a Cask with Lid Removed

This example illustrates how an independent fault tree analysis can be performed using the PCSA Tool. The analysis is performed on a selected initiating event in a sequence, and shows how two Category 2 event sequences in the DOE preclosure safety analysis may be reclassified as a more severe Category 1 event sequence when data from the failure rate database in the tool are used in the analysis.

The selected top event for the fault tree analysis is the Probability of Yoke Drop. DOE constructed a fault tree for the Probability of Yoke Drop (CRWMS M&O, 2000f, page VI-5) in which the top event is postulated to occur from either a human-induced event sequence or an electrical or mechanical failure. An equivalent fault tree is constructed using SAPHIRE software in the PCSA Tool. The human-induced event sequence portion of the fault tree is left unaltered from the DOE fault tree. In addition, the preclosure safety analysis fault tree maintains the same overall logic for the probability of electrical or mechanical failure. Failure-rate data from Duke (1985), obtained from the failure rate database in the tool, are used in this portion of the fault tree, however. Because the data available in this referenced source are more detailed, the preclosure safety analysis generated fault tree uses two subfault trees to generate the composite failure probabilities for mechanical and electrical components of the system (see Appendix D, pages D–26 and D–27).

The probabilities used in developing the fault tree are given in Table 10-2. Probabilities for the human-induced event sequence portion of the fault tree are copied from the DOE report (CRWMS M&O, 2000f, page VI-5). The balance of the probabilities are obtained from the failure rate database in the tool as described in the preceding section.

The frequency of the yoke drop calculated using the PCSA Tool generated fault tree is 1.9×10^{-6} (see Fault Tree on Yoke Drop in Appendix D, page D–25). This frequency is significantly more than the DOE calculated frequency of 1.83×10^{-7} (CRWMS M&O, 2000f, page VI-5). Further, because DOE uses this number for Design Basis Event Sequence Frequency calculations (CRWMS M&O, 2000f, page VII-5), the use of the new number obtained from PCSA Tool fault tree analysis will result in Events #2-05 and #2-06 being reclassified as the more severe Category 1 event sequence. Here again, this example illustrates how the tool may be used to draw out potential deficiencies in the DOE preclosure safety analysis.

10.5 Consequence Analysis

This section carries forward with a dose calculation to the public from the cask drop scenario presented in the first example in the preceding section.

An example dose calculation is performed for an off-site member of the public from the radiological release resulting from a cask drop in the Cask Preparation and Decommissioning Room 1 area with operational high-efficiency particulate air filtration. Based on the DOE documentation (CRWMS M&O, 2000f), the source term for this event sequence was determined to be 68 boiling water reactor fuel assemblies (Events #2-11 and #2-12 in Table 9 of the referenced report). The source term inputs for the RSAC deterministic dose calculation are shown in the three dialogue boxes: RSAC Input, BWR Fuel, and 1 Assembly Breached (Appendix D, pages D–28 through D–30, the values on page D–30 for fraction discharge from building ventilation should be 0.01 for crud and 0.002 for particulates). The remaining RSAC input parameters and their values are presented in Tables 10-3 to 10-7 for the meteorological, inhalation, ingestion, ground surface, and submersion inputs, respectively.

The RSAC Output display box titled Summary Results (Appendix D page, D–31) displays the four pathway doses and a total effective dose equivalent of 20.4 μSv [2.04 mrem] which is well below the 250-μSv [25-mrem] and 0.05-Sv [5-rem] total effective dose equivalent limits specified in 10 CFR Part 63 for Category 1 and Category 2 event sequences, respectively. The

Table 10-2. Fault Tree Inputs			
Name of Fault Tree	**Event Label**	**Event Probability**	**Reference**
Probability of Yoke Drop	FWPDM	1.0×10^{-2}	*
	CFDE-DM	1.0×10^{-1}	*
	CFD-EM	1.0×10^{-1}	*
	RCF	1.7×10^{-5}	†
	CCF-ME	1.0×10^{-4}	*
	OP-ER	1.0×10^{-3}	*
	CCF-REMC		†
Mechanical Failure of Components			
	HK	2.0×10^{-9}	†
	RD	4.0×10^{-8}	†
	RDP	4.0×10^{-8}	†
	DGS	2.0×10^{-7}	†
	DGC	8.0×10^{-7}	†
	BRAKE	1.0×10^{-5}	†
	RSF	4.0×10^{-6}	†
	GEARBOX	1.0×10^{-6}	†
	GBS	2.0×10^{-7}	†
	GBC	8.0×10^{-7}	†
Electrical Failure			
	BMS	2.0×10^{-7}	†
	BMC	8.0×10^{-7}	†
	HM	6.0×10^{-5}	†
	CL	1.0×10^{-5}	†
	CC	4.0×10^{-6}	†
	DMH	2.5×10^{-4}	†
	EMSPB	2.5×10^{-4}	†
	CMC	6.2×10^{-4}	†

*CRWMS M&O. "Design Basis Event Frequency and Dose Calculation for Site Recommendation." CAL–WHS–SE–000001. Revision 01. Las Vegas, Nevada: CRWMS M&O. 2000.
†Duke, A.J. "Reliability Techniques Used in the Assessment of Cranes." NCSR/GR/64. Warington, United Kingdom: National Center of Systems Reliability, United Kingdom Atomic Energy Authority. 1985.

Table 10-3. Meteorological Data Input		
Input Parameter	**Input Value**	**Remarks**
Average wind velocity	3 m/s [7 mi/hr]	Most-probable velocity (site-specific estimate)
Stack release height	40 m [130 ft]	Estimation of stack height
Mixing depth	1,420 m [4,660 ft]	Average mixing height based data from Desert Rock, Nevada
Air density	1.29×10^3 g/m^3 [80.5 16 ft^3]	Site-specific mean value*
Wet deposition scavenging coefficient	0 1/s	No plume depletion by wet deposition, radiological safety analysis computer program default value
Plume depletion by dry deposition	1	Yes
Deposition velocity for solids	0.001 m/s [0.003 ft/s]	RSAC code default value
Deposition velocity for halogens	0.01 m/s [0.03 ft/s]	RSAC code default value
Deposition velocity for noble gases	0.0 m/s [0.0 ft/s]	RSAC code default value
Deposition velocity for cesium	0.001 m/s [0.003 ft/s]	RSAC code default value
Deposition velocity for ruthenium	0.001 m/s [0.003 ft/s]	RSAC code default value
Downwind distance	11,000 m [6.8 mi]	Site-specific approximation†
Linear constant in decay function	1 1/s	RSAC code default value for instantaneous release
Exponential constant in decay function	0.0 1/s	RSAC code default value for instantaneous release
Crosswind distances to be entered	No	Assuming critical group is directly downwind
Diffusion definition	2	Program calculates standard deviations
Type of sigma (standard deviation) set	1	Hilsmeier-Gifford for <15-minute releases at desert sites

Table 10-3. Meteorological Data Input (continued)		
Input Parameter	**Input Value**	**Remarks**
Building width	0 m [0 ft]	RSAC code default value, option only if stack height in 0 m
Building height	0 m [0 ft]	RSAC code default value, option only if stack height is 0 m
Building wake coefficient	0	If zero, radiological safety analysis computer program default value of 1 is used
Weather class	6	6 relates to Class F, the most-probable class (site-specific estimate)
Plume rise indicator	0	No plume rise

*Weast, R.C. *CRC Handbook of Chemistry and Physics*. Cleveland, Ohio: CRC Press. 1976.
†CRWMS M&O. "Design Basis Event Frequency and Dose Calculation for Site Recommendation." CAL–WHS–SE–000001. Revision 01. Las Vegas, Nevada: CRWMS M&O: 2000.

Table 10-4. Inhalation Dose Input		
Input Parameter	**Input Value**	**Remarks**
Type of dose calculation	1	International Commission on Radiological Protection-30 inhalation with user-specified parameters
Output control for dose	−2	Only dose summaries
Dose unit	1	Output in rem
Elements for calculation	0	All elements
Organ choice	1	All organs
For inhalation, breathing rate	3.33×10^{-4} m^3/s [1.18×10^{-2} ft^3/s]	RSAC code default value, average daily breathing rate
Decay time for exponential decay function	0.0 1/s	RSAC code default value for instantaneous release
Activity mean aerodynamic diameter	1 μm [4×10^{-5} in]	RSAC code default value
Clearance classes	1	RSAC code default classes

Table 10-5. Ingestion Dose Input		
Input Parameter	**Input Value**	**Remarks**
Type of dose calculation	3	Ingestion with user-specified parameters
Output control for dose	-2	Only dose summaries
Dose unit	1	Output in rem
Elements for calculation	0	All elements
Organ choice	1	All organs
Decay time for exponential decay function	0 1/s	RSAC code default value for instantaneous release
Plant midpoint of operating life	1 yr	Dose during year of intake for acute releases
Ingestion transfer parameter control	0	RSAC code default transfer parameters used
Ingestion parameter control	2	User-specified ingestion parameters
Time crops are exposed to contamination during growing season	7 day	Times <60 day are interpreted as acute releases
Harvest duration following acute release	7 day	RSAC code default value
Stored (other) vegetable consumption rate includes fruits and grains	23.8 wet kg/yr [52.5 wet lb/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents*
Fresh (leafy) vegetable consumption rate	15 wet kg/yr [33.1 wet lb/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents*
Meat consumption rate includes beef and poultry	3.7 kg/yr [8.2 lb/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents*

Table 10-5. Ingestion Dose Input (continued)		
Input Parameter	**Input Value**	**Remarks**
Milk consumption rate	4.1 L/yr [1.1 U.S. gal/yr]	Mean consumption of locally produced food from survey of Amargosa Valley residents* assuming a milk density of 1 kg/L
Fraction of stored vegetables from garden	0.76	RSAC code default value
Fraction of fresh vegetables from garden	1	RSAC code default value
Retention factor for activity on forage	0.57	RSAC code default value
Retention factor for activity on vegetables	0.2	RSAC code default value
Retention factor for iodines on forage	1	RSAC code default value
Removal rate constant for crops	0.0021 1/hr	RSAC code default value
Vegetable exposure time for chronic releases	7 day	Set equal to time crops are exposed to contamination during growing season
Forage exposure time for chronic releases	7 day	Set equal to time crops are exposed to contamination during growing season
Tritiated water, removal half-time	1 day	RSAC code default value
Effective surface density for soil	225 (kg/m^3) [14.0 lb/ft^3]	RSAC code default value
Stored vegetable holdup time after harvest	14 day	Site-specific value*
Fresh vegetable holdup time after harvest	1 day	Site-specific value*
Animals daily forage feed	16 dry kg/day [35 dry/lb/day]	RSAC code default value

Table 10-5. Ingestion Dose Input (continued)		
Input Parameter	**Input Value**	**Remarks**
Feed-milk receptor transfer time	2 day	RSAC code default value
Slaughter to consumption time	20 day	Site-specific value*
Fraction of year that animals graze	0.4	RSAC code default value
Fraction of feed that is pasture when grazing	0.43	RSAC code default value
Stored feed holdup time	14 day	Set equal to stored vegetable holdup time (day)
Vegetable vegetation yield	3.0 wet kg/m^2 [0.61 wet lb/ft^2]	Average of leafy vegetable (2.0), other vegetable (4.0), and fruit (3.0) yields*
Forage vegetation yield	1.23 dry kg/m^2 [0.252 wet lb/ft^2]	Site-specific value*
Absolute humidity	4.9 g/m^3 [0.31 lb/ft^3]	RSAC code default value
Fraction of annual stored vegetables that are contaminated by acute release	0.5	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
Fraction of annual fresh vegetables that are contaminated by acute release	0.33	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
Fraction of annual stored forage that is contaminated by acute release	0.5	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
Fraction of annual fresh forage that is contaminated by acute release	0.33	RSAC code default value for crops exposed to contamination between 1 hour and <30 days
*LaPlante, P.A. and K. Poor. "Information and Analysis to Support Selection of Critical Groups and Reference Biosphere for Yucca Mountain Exposure Scenarios." CNWRA 97-009. San Antonio, Texas: CNWRA. 1997.		

Table 10-6. Ground Surface Dose Input		
Input Parameter	**Input Value**	**Remarks**
Type of dose calculation	4	Ground surface dose calculation
Output control for dose	-2	Only dose summaries
Dose unit	1	Output in rem
Elements for calculation	0	All elements
Organ choice	1	All organs
Decay time for exponential calculations	0 s	RSAC code default value for instantaneous release
Ground surface exposure time	1 yr	Dose is calculated for 1 year after the event
Building shielding factor (dimensionless)	0.7	RSAC code default value

Table 10-7. Submersion Dose Input		
Input Parameter	**Input Value**	**Remarks**
Gamma cloud model selection	0	All calculations are made using a finite model
Decay time for exponential decay function	0 s	RSAC default value for instantaneous release
Type of dose calculation	2	Calculate external effective dose equivalent

results of the organ dose calculations are shown in the last three RSAC Output display screens (Appendix D, pages D–32 through D–34) for the inhalation, ingestion, and ground surface pathways, respectively. Assuming uniform whole-body irradiation from submersion, the total organ doses were calculated by adding the effective submersion dose to the sum of the organ doses from the inhalation, ingestion, and ground surface pathways. Of all the organs, the thyroid received the largest total organ dose of 0.471 mSv [47.1 mrem], which is substantially lower than the 0.5-Sv [50-rem] organ dose limit specified in 10 CFR Part 63 for Category 2 event sequences.

10.6 Conclusions

The example analyses conducted on the Cask Preparation and Decontamination Room 1 area of the assembly transfer system demonstrate the various modules of the PCSA Tool and its capabilities. The analyses also illustrate the value of the tool in uncovering potential deficiencies in the DOE preclosure safety analysis. Specifically, the analyses performed for the two examples in Section 10.4 indicated 3 sequences for possible addition to the list of 14 Category 1 design basis event sequences given in the present DOE analysis (CRWMS M&O, 2000f). These additional event sequences would be expected to increase the estimated dose to the public from Category 1 event sequences.

11 FUTURE WORK

During fiscal year 2002, the focus of PCSA Tool development was mainly on (i) acceptance testing of the functional behavior of the tool, testing of the consequence analysis module, and code fixes based on test results; (ii) modification of the tool to make it more efficient and user friendly; (iii) incorporation of the human reliability analysis; and (iv) incorporation of risk assessment methodologies. This chapter discusses future work on the tool development and the tasks to be accomplished in fiscal year 2003.

11.1 PCSA Tool Features

Testing of the PCSA Tool will continue in fiscal year 2003. A verification plan will be developed and verification tests will be conducted. Changes will be made in the tool based on the test results. Report capabilities for consequence analysis input and output data will be developed, and a graphical display of the output data for the consequence analysis will be added using Component Chart 7.0. The current Show Report, which uses an in-built feature in Visual Basic 6, will be replaced by Crystal Report Developer to improve flexibility in data display and transportability of the reports to WordPerfect documents.

11.2 Software Reliability

Further evaluation of various software reliability models may be warranted as more detail regarding the hardware, software, and operations of the proposed repository become available. With more details available, possibly including failure data on the specific software to be deployed at the repository, an evaluation could be made to determine the need for quantification of the software reliability and, if quantification is needed, what specific software reliability models would be most appropriate.

Methods for software design and reliability in the context of safety-critical systems appear to be extremely pertinent to preclosure repository safety (Eisenberg, 2001b). The literature, methods, and procedures for software reliability in the context of safety-critical systems will continue to be evaluated. Further investigation of these methods is directed at enhancing the U.S. Nuclear Regulatory Commission (NRC) and Center for Nuclear Waste Regulatory Analyses (CNWRA) review capability and providing tools for identifying vulnerabilities, in any, in U.S. Department of Energy (DOE) approaches and designs. Particular emphasis is being placed on the developments made by the National Aeronautics and Space Administration.

Software reliability approaches based on the development process are being explored further. A particular focus is the Capability Maturity Model, developed by the Software Engineering Institute, Carnegie-Mellon University.

Although it is premature to attempt to put a quantitative capability into the PCSA Tool, work is continuing on an approach to quantifying software reliability. Further evaluation of DOE documents related to software reliability and repository design and operations will be undertaken, as those documents become available.

11.3 Fire Hazard Analysis

The internal fire hazard for the surface and subsurface facilities requires special attention. Methods of performing fire analysis will rely on the internal fire probabilistic risk analysis for nuclear power plants. The procedures and guidelines for fire probabilistic risk assessment provided in NRC (1983) and other documents will be used to review the DOE fire hazard analysis. An approach will be developed, consistent with Section 4.1.1.3 of NRC (2002a), to document the review of the DOE fire hazard analysis in the PCSA Tool.

11.4 Assessment of Transportation Hazards

Existing documents and studies related to transportation of hazardous material will be reviewed and tool capabilities to identify hazards related to transportation from the site boundary to the repository surface facilities will be assessed.

11.5 Seismic Hazard Analysis

DOE presented its current conceptual approach to seismic design of structures, systems, and components important to safety and its relationship to the preclosure safety analysis in Bechtel SAIC Company, LLC (2002). To meet the regulatory requirements of 10 CFR Part 63, DOE proposed to use two different design basis earthquakes, as outlined in Seismic Topical Report 2 (DOE, 1996), for the seismic design of structures, systems, and components important to safety. The proposed DOE methodology is centered around seismic classification of each structure, system, and component to withstand either a frequency Category 1 or frequency Category 2 design basis earthquake as defined in DOE (1996) and tentatively approved by NRC.

In its seismic design methodology (Bechtel SAIC Company, LLC, 2002), the DOE would identify scenarios by which radionuclides could potentially be released by event sequences initiated by earthquakes. These potential scenarios would be analyzed using seismic event trees. Seismic designations of structures, systems, and components would be made based on compliance with the regulatory dose limits with and without the mitigation features of the structures, systems, and components in each event scenario. Staff, however, noted[1] that each design basis earthquake needs to be treated as an initiating event, and the probability of exceeding the dose requirements of 10 CFR Part 63 must be determined by considering the event sequences attributable to this initiating event. In other words, assessment of the event sequences should consider the probabilities of the initiating event (e.g., earthquakes) and the associated combinations of repository structure, system, and/or component failures.

The DOE also proposed using fragility and seismic margin analyses to demonstrate the probability of an unacceptable dose as a result of an earthquake initiating event will be less than 1 in 10,000 within the preclosure period. Bechtel SAIC Company, LLC (2002), however, does not clearly define the circumstances or conditions that govern the use of these analysis

---

[1]Schlueter, J.R. "Preclosure Agreement 6.02." Letter (August 5) to J.D. Ziegler, DOE. Washington, DC: NRC. 2002.

methodologies. Staff assessment of the DOE seismic design methodology will continue and a strategy will be developed to review the DOE safety case for seismic events.

PCSA Tool modules will be added, as needed, to facilitate review of DOE analyses. In addition, the tool will be used to conduct independent seismic analyses.

11.6 Other Hazards

Incorporation of analyses for other hazards (e.g., flood and tornado) in the tool will be explored.

11.7 Failure Rate Database

Development of a failure rate database will continue. As more details on repository design become available, additional equipment, controls, and instruments to be used in the surface and subsurface operations will be identified and incorporated into the database. Failure rate data will be further explored, and the database will be expanded.

11.8 Consequence Analysis

Development and testing of the consequence analysis module will continue. Graphical display of the output from the probabilistic consequence analysis will be developed. For example, the output data are planned to be augmented by presenting the contributions of individual radionuclides to the dose results. Report capabilities for consequence analysis input and output data will be developed. Improvements are planned for the transfer of information from RSAC code into the PCSA Tool interface to allow probabilistic calculations for the Advanced RSAC Input. In addition to the average boiling water reactor and pressurized water reactor characteristics for commercial spent nuclear fuel, bounding characteristics for other waste types may be added into the source term options. Upgrading the RSAC code to a more recent version is also planned. Finally, consideration for inclusion of the MACCS2 code into the PCSA Tool will continue. Documented in NRC (1998), the MACCS2 code would allow for comparisons with the RSAC code results.

11.9 Safety Assessment

Report capabilities for safety assessment will be developed, using Crystal Report. In addition to the annualized dose approach, the PCSA Tool currently uses a simplified approach to assess combinations of Category 1 event sequences that could occur in the same year for screening purposes. The approach will be revised to make it mathematically rigorous and a graphical user interface will be developed to display results.

11.10 Risk Assessment

Report capabilities for risk assessment will be developed, and a graphical display of the risk assessment output data will be added using Crystal Report and Component Chart 7.0, respectively.

11.11 Structures, Systems, and Components Important to Safety

The module in the tool dealing with identification of structures, systems, and components will be modified and may be redesigned if the NRC accepts the DOE approach outlined in Bechtel SAIC Company, LLC (2002).

12 CONCLUSIONS

The U.S. Department of Energy (DOE) will conduct a preclosure safety analysis of the proposed geologic repository operations area as a part of its license application for construction authorization. The purpose of the preclosure safety analysis is to ensure that (i) all relevant hazards with potential radiological consequences in excess of the regulatory limits have been evaluated and (ii) structures, systems, and components relied on for safety have been identified. This report includes the formulation of a risk-informed performance-based methodology, and documents the development of a computer code, PCSA Tool Version 2.0 Beta, that can be used by U.S. Nuclear Regulatory Commission (NRC) and Center for Nuclear Waste Regulatory Analyses (CNWRA) staffs to review the DOE preclosure safety analysis of the proposed geologic repository at Yucca Mountain. The PCSA Tool allows the user to conduct and document independent checks of the safety analyses for a part of or the entire repository system. Furthermore, the PCSA Tool has been designed to handle updated reviews of the DOE safety analysis throughout the licensing process (i.e., through the construction authorization, receipt and possession of waste, and permanent closure phases).

The preclosure safety analysis methodology used in the tool is based on the requirements for preclosure safety analysis of the geologic repository operations area in 10 CFR 63.112 and the preclosure performance objectives in 10 CFR 63.111. The tool has been structured to address the relevant acceptance criteria and review methods provided in the preclosure safety analysis (Section 4.1.1) of the Yucca Mountain Review Plan (NRC 2002a). The activities presented in this report include development of (i) a database consisting of appropriate information and data for site-specific, naturally occurring, and human-induced events from the review of referenced sources; (ii) a hazards analysis capability for surface and subsurface facility operations using standard qualitative methodology, including human reliability; (iii) an event sequence analysis capability based on quantitative methods; (iv) a capability for determining radiological consequences to the public with either deterministic or probabilistic solutions and to workers with a deterministic calculation; (v) a safety assessment capability based on the frequency and dose limits in 10 CFR Part 63; (vi) a capability to evaluate total aggregate risk developed as an additional option to gain risk insight, though not required to comply with the regulation; (vii) a capability to identify structures, systems, or components important to safety based on available information; and (viii) a failure rate, failure mode, and checklist database from available literature for the equipment/systems for operational hazard analysis. Additionally, the application of the tool has been demonstrated by conducting preliminary analyses of a selected area of the assembly transfer system in the Waste Handling Building.

The PCSA Tool serves two purposes: (i) store data and results in a database and (ii) conduct model analyses. The PCSA Tool uses Visual Basic as the primary programming environment to develop a graphical user interface to project and probability databases in Microsoft Access and to other preexisting software packages. Specifically, the tool uses (i) SAPHIRE code for event sequence analyses and quantitative frequency evaluations using event tree and fault tree models, (ii) RSAC code to calculate the radiological consequences to a member of the public from an atmospheric release of radioactive material using deterministic and probabilistic approaches, and (iii) MELCOR code to estimate building discharge fractions. The project database allows segmenting the repository into several functional areas for the creation of input data for and storage of output data from model analyses using acquired software, displaying graphical results, and generating reports for each functional area. The failure rate database, which is a controlled database, contains the component failure rates obtained from actuarial and other information, such as literature citation, for source of the data.

Future work on the tool will involve modifications based on the validation and verification tests and suggestions by the users of the tool. The feasibility of incorporating software reliability analyses will be considered. Capability to review DOE analysis of seismic events will be incorporated. Fire hazards, transportation hazards and other external hazards (e.g., flood and tornado) will be assessed for incorporation in this tool. The failure rate database will be enhanced as more repository design details become available to include design-specific equipment, controls, and instruments. Improvements in the consequence analysis will focus on the transfer of information from the RSAC code into the PCSA Tool interface to allow probabilistic calculations for the Advanced RSAC Input. Consideration also will be given to incorporating the MACCS2 code into the PCSA Tool to allow comparisons with the RSAC results. Additionally, the report capabilities in the tool will be enhanced and the graphical display of the output from probabilistic consequence analysis will be developed.

13 REFERENCES

American Institute of Chemical Engineers. *Guidelines for Hazard Evaluation Procedures.* 2nd Edition with Worked Examples. New York City, New York: Center for Chemical Process Safety. 1992.

———. *Guidelines for Process Equipment Reliability Data.* New York City, New York: Center for Chemical Process Safety. 1989.

American National Standards Institute, Inc./American Nuclear Society. "American National Standards Guidelines for the Verification and Validation of Scientific and Engineering Programs for the Nuclear Industry." ANSI/ANS–10.4. New York City, New York: American National Standards Institute. 1987.

Anderson, B.C., R.W. Carlson, and L.E. Fischer. NUREG/CR–6487, "Containment Analysis for Type B Packages Used to Transport Various Contents." Livermore, California: Lawrence Livermore National Laboratory. November 1996.

Bechtel SAIC Company, LLC. "Preclosure Safety Analysis Guide." TDR–MGR–RL–000002. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 2002.

Benke, R., B. Dasgupta, B. Sagar, and A. Chowdhury. "A Methodology for Preclosure Risk Assessment for a Geologic Nuclear Waste Repository." Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management. June 23–28, 2002. San Juan, Puerto Rico. The International Association for Probabilistic Safety Assessment and Management. 2002.

CRWMS M&O. "Repository Safety Strategy: Plan to Prepare the Safety Case to Support Yucca Mountain Site Recommendation and Licensing Considerations." TDR–WIS–RL–000001. Rev. 04 ICN 01. Las Vegas, Nevada: CRWMS M&O. 2000a.

———. "Waste Emplacement/Retrieval System Description Document." SDD–WES–SE–000001. Rev. 01. Las Vegas, Nevada: CRWMS M&O. 2000b.

———. "Subsurface Ventilation System Description Document." SDD–SVS–SE–000001. Rev. 01. Las Vegas, Nevada: CRWMS M&O. 2000c.

———. "Ground Control System Description Document." SDD–GCS–SE–000001. Rev. 01. Las Vegas, Nevada: CRWMS M&O. 2000d.

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

———. "Design Basis Event Frequency and Dose Calculation for Site Recommendation." CAL–WHS–SE–000001. Rev. 01. Las Vegas, Nevada: CRWMS M&O. 2000f.

———. "Subsurface Facility System Description Document." SDD–SFS–SE–000001. Rev. 01. Las Vegas, Nevada: CRWMS M&O. 2000g.

———. "WHB/WTB Space Program Analysis for Site Recommendation." ANL–WHS–AR–000001. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 2000h.

———. "Design Basis Events Related to Waste Packages." ANL–MGR–MD–000012. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 2000i.

———. "Monitored Geologic Repository Internal Hazards Analysis." ANL–MGR–SE–000003. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999a.

———. "Repository Surface Design Engineering Files Report." BCB000000–01717–5705–00009. Rev. 03. Las Vegas, Nevada: CRWMS M&O. 1999b.

———. "Reference Design Description for Geologic Repository." B00000000–01717–5707–00002. Rev. 02. Las Vegas, Nevada: CRWMS M&O. 1999c.

———. "MGR External Events Hazards Analysis." ANL–MGR–SE–000004. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999d.

———. "Preliminary Selection of MRG Design Basis Events." ANL–WHS–SE–000003. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999e.

———. "Engineering File-Subsurface Repository." Rev. 02. BCA000000–01717–5705–00005. Las Vegas, Nevada: CRWMS M&O. 1999f.

———. "Level of Design Detail Necessary for the License Application for Construction Authorization." B00000000–01717–1710–00003. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999g.

———. "Commercial SNF Accident Release Fractions." ANL–WHS–SE–000001. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999h.

———. "MRG Design Aircraft Crash Frequency Analysis." ANL–WHS–SE–000003. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999i.

———. "Reliability Assessment of Waste Handling Building HVAC System." BCBD00000–01717–0210–00008. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1999j.

———. "Preliminary Preclosure Design Basis Event Calculations for the Monitored Geologic Repository." BC000000–01717–0210–00001. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1998a.

———. "Controlled Design Assumptions Document." B00000000–01717–4600–00032. Rev. 5. Las Vegas, Nevada: CRWMS M&O. 1998b.

———. "DBE/Scenario Analysis for Preclosure Repository Subsurface Facilities." BCA000000–01717–00017. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1997.

———. "Mined Geologic Disposal System Advanced Conceptual Design Report, Volume II." B00000000–01717–5705–00027. Rev. 00. Las Vegas, Nevada: CRWMS M&O. 1996.

———. "Light Water Characteristics Database. LWR Radiological Module, Version 1.1." CSCIA00000000–02268–1200–20002. Las Vegas, Nevada: CRWMS M&O. 1993.

Dasgupta, B., A. Ghosh, A. Chowdhury, B. Hill, J. Stamatakos, and M. Lasher. "Hazard Identification for Geologic Operations Area: A Progress Report." San Antonio, Texas: CNWRA. 2002.

Dasgupta, B., R. Benke, D. Daruwalla, A. Ghosh, R. Janetzke, and A.H. Chowdhury. "PCSA Tool Development Progress Report." San Antonio, Texas: CNWRA. 2001a.

Dasgupta, B., D. Daruwalla, R. Benke, and A.H. Chowdhury. "Methodology for Assessment of Preclosure Safety for Yucca Mountain Project." Proceedings of the 9 Ninth International Conference on High-Level Radioactive Waste Management. Las Vegas, Nevada, April 29–May 3, 2001. La Grange Park, Illinois: American Nuclear Society. 2001b.

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

DOE. "Preliminary Preclosure Safety Assessment for Monitored Geologic Repository Site Recommendation." TDR–MGR–SE–000009. Rev. 00 ICN 03. Las Vegas, Nevada: DOE. 2001a.

———. "Yucca Mountain Science and Engineering Report Technical Information Site Recommendation Consideration." DOE/RW–0539. Las Vegas, Nevada: DOE. 2001b.

———. "Draft Environmental Impact Statement for a Geological Repository for the Disposal of Spent Nuclear Fuel and High-Level Radioactive Waste at Yucca Mountain, Nye County, Nevada." Vol. II. DOE/EIS–0250D. Las Vegas, Nevada: DOE. 1999.

———. "Viability Assessment of a Repository at Yucca Mountain. Vol. 1: Introduction and Site Characteristics and Vol. 2: Preliminary Design Concept fo the Repository and Waste Package." DOE/RW–0508-V1 and V2. Las Vegas, Nevada: DOE, Office of Civilian Radioactive Waste Management. 1998.

———. "Preclosure Seismic Design Methodology for a Geologic Repository at Yucca Mountain." Topical Report YMP/TR–003–NP. Rev. 1. Las Vegas, Nevada: DOE. Office of Civilian Radioactive Waste Management. 1996

———. "DOE Handbook—Airborne Release Fractions/Rates and Respirable Fractions for Nonnuclear Facilities." DOE–HDBK–3010–94. Washington, DC: DOE. 1994.

Dexter, A.H. and C.W. Perkins. "Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant." Aiken, South Carolina: E.I. Du Pont de Nemours & Co. Savannah River Laboratory. 1982.

Duke, A.J. “Reliability Techniques Used in the Assessment of Cranes.” NCSR/GR/64. Warington, United Kingdom: National Center of Systems Reliability, United Kingdom Atomic Energy Authority. 1985.

Eisenberg, N. “Human Reliability Analysis and Repository Preclosure Safety—An Initial Evaluation.” San Antonio, Texas: CNWRA. 2001a.

———. “Software Reliability Analysis and Repository Preclosure Safety—An Initial Survey.” San Antonio, Texas: CNWRA. 2001b.

EPA. “External Exposure to Radionuclides in Air, Water, and Soil.” Federal Guidance Report No. 12, EPA 402–R–93–081. Washington, DC: EPA. 1993.

———. “Limiting Values of Radionuclide Intake and Air Concentration and Dose Conversion Factors for Inhalation, Submersion, and Ingestion.” Federal Guidance Report No. 11, EPA 520/1–88–020. Washington, DC: EPA, Office of Radiation Programs. 1988.

Frank, M., M. Jarzemba, and J. Weldy. “A Survey of Risk Assessment Methods from the Nuclear, Chemical, and Aerospace Industries for Applicability to the Privatized Vitrification of Hanford Tank Wastes.” San Antonio, Texas: CNWRA. 1998.

Gauntt, R.O., R.K. Cole, C.M. Erickson, R.G. Gido, R.D. Gasser, S.B. Rodriguez, M.F. Young, S. Ashbaugh, M. Leonard, and A. Hill. NUREG/CR–6119, “MELCOR Computer Code Manuals.” Rev. 2. Washington, DC. NRC. October 2000.

Hickman, J.W., et al. NUREG/CR–2300, “PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Final Report. Vols. 1 and 2.” Washington, DC: NRC. January 1983.

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

Hossain, Q.A., A.H. Chowdhury, M.P. Hardy, K.S. Mark, J.E. O’Rourke, W.J. Silva, J.C. Stepp, and F.H. Swan, III. “Seismic and Dynamic Analysis and Design Considerations for High-Level Nuclear Waste Repositories.” J.C. Stepp, ed. New York City, New York: American Society of Civil Engineers. 1997.

Idaho National Engineering Laboratory. “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 6.0, Saphire Reference Manual.” Idaho Falls, Idaho: Idaho National Engineering Laboratory. 1998.

Iman, R.L. and M.J. Shortencarier. NUREG/CR–3624, “A FORTRAN77 Program and User’s Guide for the Generation of Latin Hypercube and Random Samples for Use with Computer Models.” Washington, DC: NRC. 1984.

International Commission on Radiological Protection (ICRP). “Limits for Intakes of Radionuclides by Workers.” ICRP30. Annals of the ICRP. Oxford, United Kingdom: Pergamon Press. 1979.

Kaplan, S. and B.J. Garrick. "On the Quantitative Definition of Risk." Risk Analysis. Vol. 1, No.1. pp. 11–27. 1981.

LaPlante, P.A. and K. Poor. "Information and Analysis to Support Selection of Critical Groups and Reference Biosphere for Yucca Mountain Exposure Scenarios." CNWRA 97-009. San Antonio, Texas: CNWRA. 1997.

Miller, C.F., W.H. Hubble, M. Trojovsky, and S.R. Brown. NUREG/CR–1363, "Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants." Washington, DC: NRC. October 1982.

NRC. NUREG–1804, "Yucca Mountain Review Plan—Draft Report for Comment." Rev. 2. Washington, DC: NRC. March 2002a.

———. NUREG–1762, "Integrated Issue Resolution Status Report." Washington, DC: NRC. July 2002b.

———. NUREG–1513, "Integrated Safety Analysis Guidance Document." Washington, DC: NRC. May 2001.

———. NUREG–1567, "Standard Review Plan for Spent Fuel Storage Facilities." Washington, DC: NRC. March 2000a.

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

———. NUREG–6613, "Code Manual for MACCS2: Users Guide." Washington, DC: NRC. May 1998.

———. NUREG–1536, "Standard Review Plan for Dry Cask Storage Systems." Washington, DC: NRC. January 1997.

———. 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. March 1994.

———. NUREG–0492, "Fault Tree Handbook." Washington, DC: NRC. March 1981.

Nuclear Energy Agency. "Critical Operator Actions: Human Reliability Modeling and Data Issues." Principal Working Group No. 5, Task 94–1. Final Task Report, prepared by a Group of Experts of the NEA Committee on the Safety of Nuclear Installations NEA/CSNI/R(98). Paris, France: Nuclear Energy Agency. 1998.

Oak Ridge National Laboratory. "Design, Construction, and Testing of High-Efficiency Air Cleaning Systems for Nuclear Applications." Nuclear Air Cleaning Handbook. ERDA76–21. Oak Ridge, Tennessee: Oak Ridge National Laboratory. 1976.

Rossi, M.J. “Nonelectronic Parts Reliability Data.” NPRD–3. Grifis Air Force Base, New York: Reliability Analysis Center, Rome Air Development Center. 1985.

Russel, K.D., C.L. Atwood, W.J. Galyean, M.B. Sattison, and D.M. Rasmuson. NUREG/CR–6616, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0, Technical Reference Manual.” Idaho Falls, Idaho: Idaho National Engineering Laboratory. 1993.

Shonka Research Associates, Inc. “Software Verification and Validation Report for WINCO RSAC–5 Code.” Marietta, Georgia: Shonka Research Associates, Inc. 1993.

Slade, D.H., ed. “Meteorology and Atomic Energy.” AEC/TID–24190. Silver Spring, Maryland: U.S. Atomic Energy Commission. 1968.

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

Southwest Research Institute. NUREG/CR–1635, “Nuclear Plant Reliability Data System 1979 Annual Reports of Cumulative System and Component Reliability.” Washington, DC: September 1980.

Swain, A.D. and H.E. Guttman. NUREG/CR–1278, “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.” Final Report. Washington, DC: NRC. August 1983.

System Safety Society. *System Safety Analysis Handbook—A Source Book for Safety Practitioners.* 2nd Edition. Albuquerque, New Mexico: System Safety Society. 1997.

Weast, R.C. *CRC Handbook of Chemistry and Physics.* Cleveland, Ohio: CRC Press. 1976.

Wenzel, D.R. “The Radiological Safety Analysis Computer Program (RSAC–5) User’s Manual, WINCO–1123.” Rev. 1. Idaho Falls, Idaho: Idaho National Engineering Laboratory. 1994.

APPENDIX A

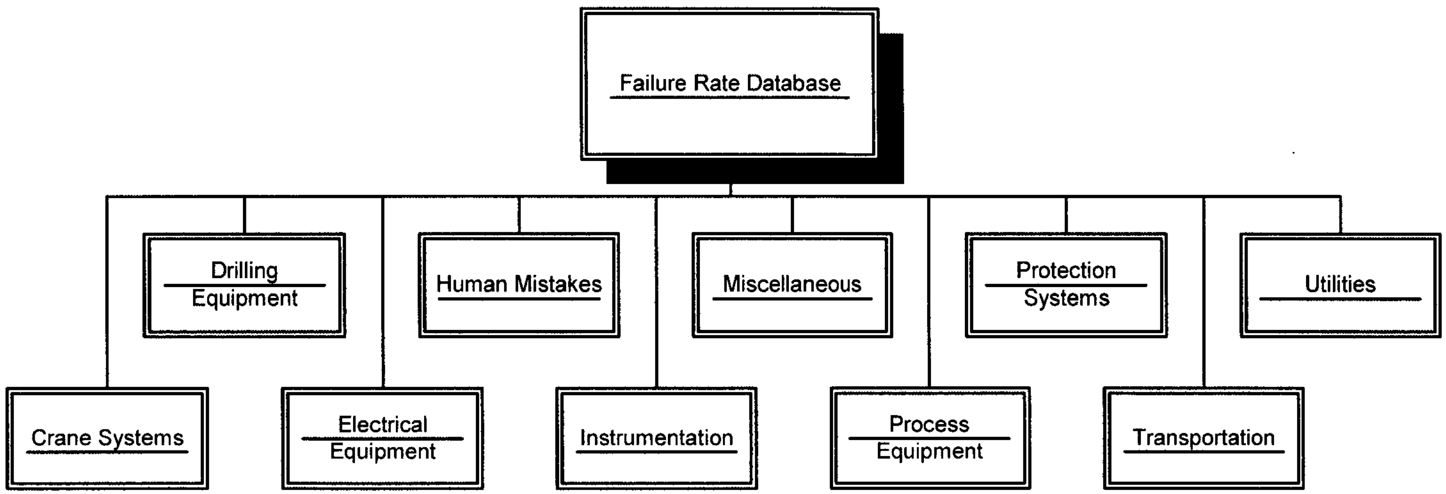
PRECLOSURE SAFETY ANALYSIS PROBABILITY DATA TAXONOMY

The taxonomy, or system of classification (ordering) used for the database has been modeled after the taxonomy scheme used by the Center for Chemical Process Safety of the American Institute of Chemical Engineers (1989) for their Process Equipment Reliability Data. The taxonomy levels for the Equipment and Systems Failure Rate Database are graphically presented in this appendix.

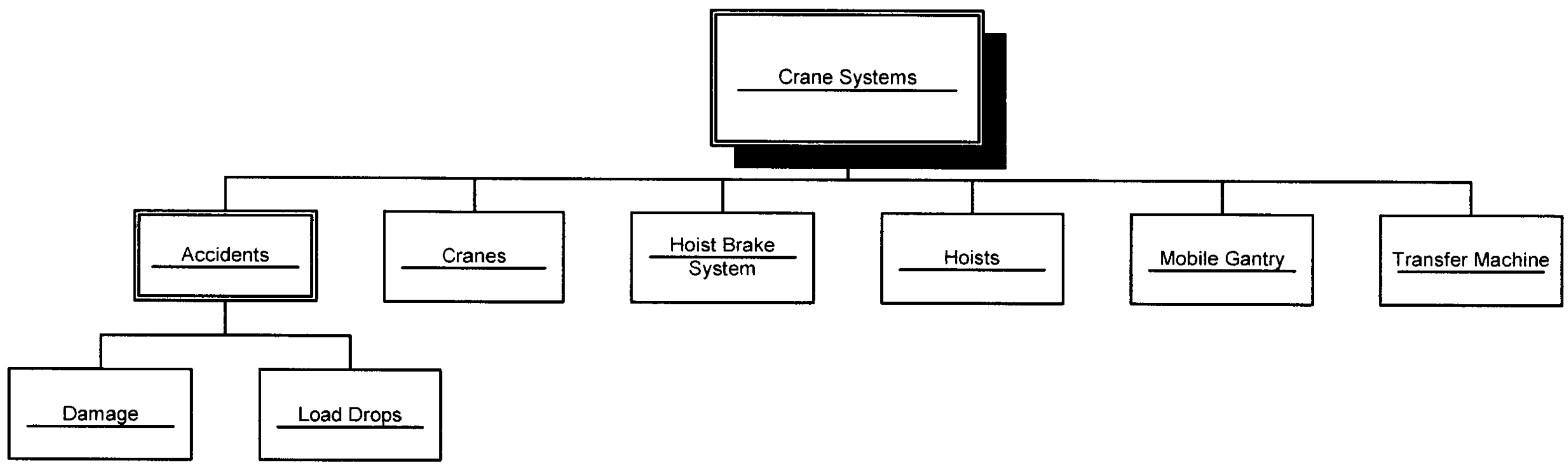
REFERENCES

American Institute of Chemical Engineers. *Guidelines for Process Equipment Reliability Data.* New York, New York: Center for Chemical Process Safety. American Institute of Chemical Engineers. 1989.

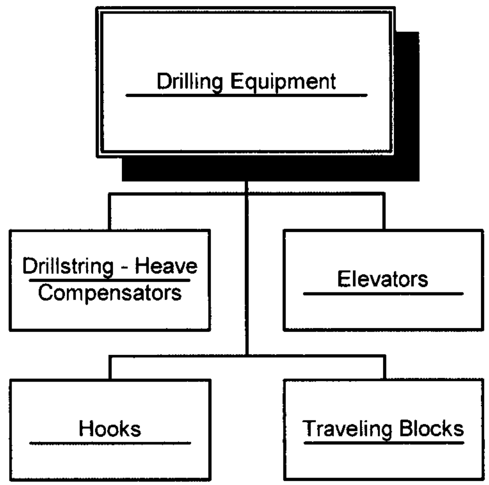
PCSA PROBABILITY DATA TAXONOMY



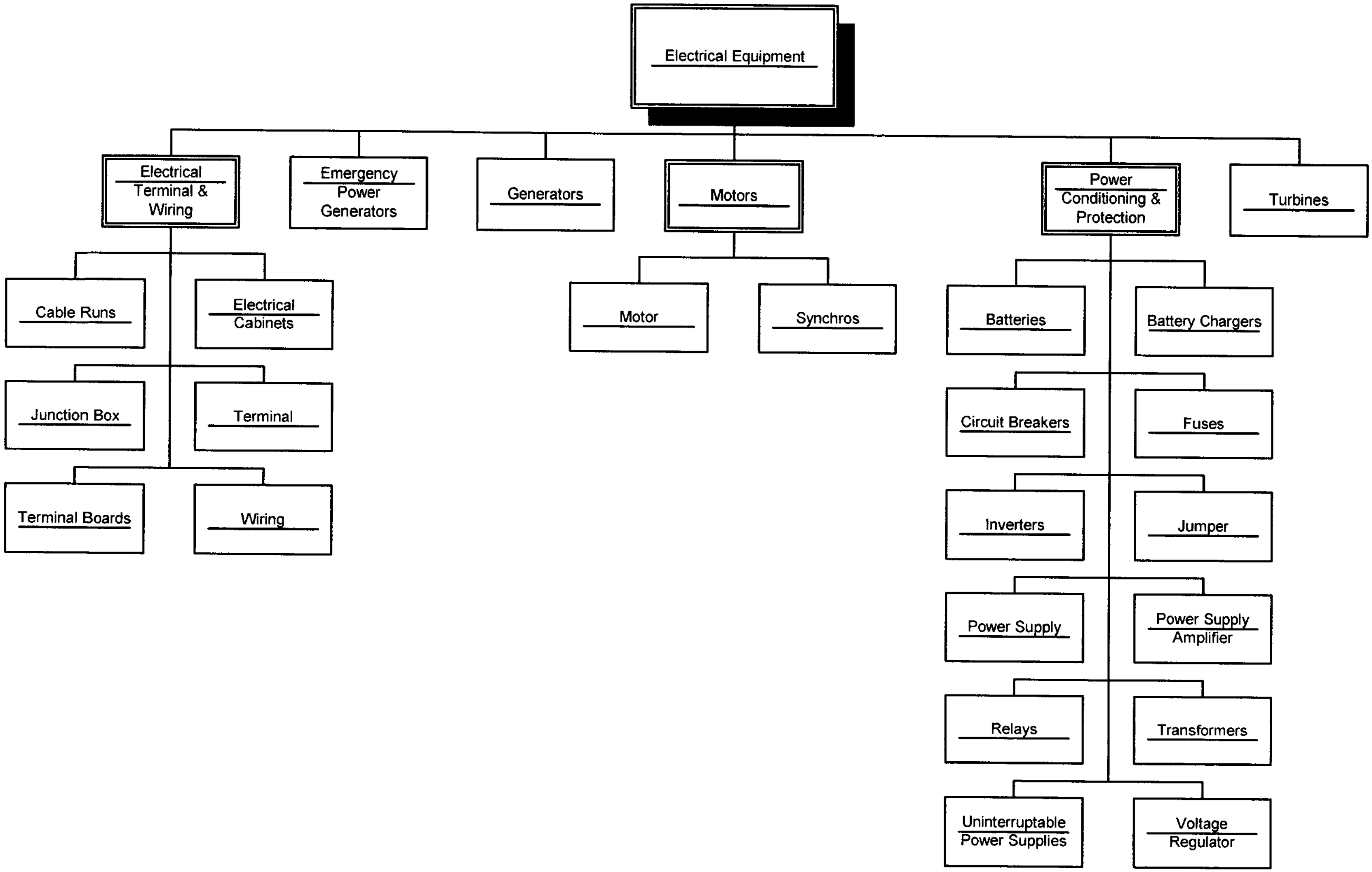
PCSA PROBABILITY DATA TAXONOMY (continued)



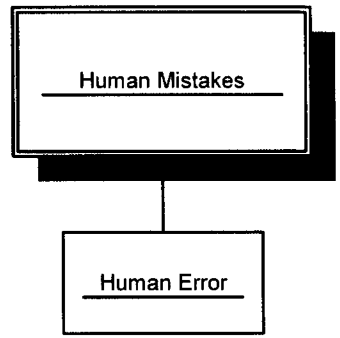
PCSA PROBABILITY DATA TAXONOMY (continued)



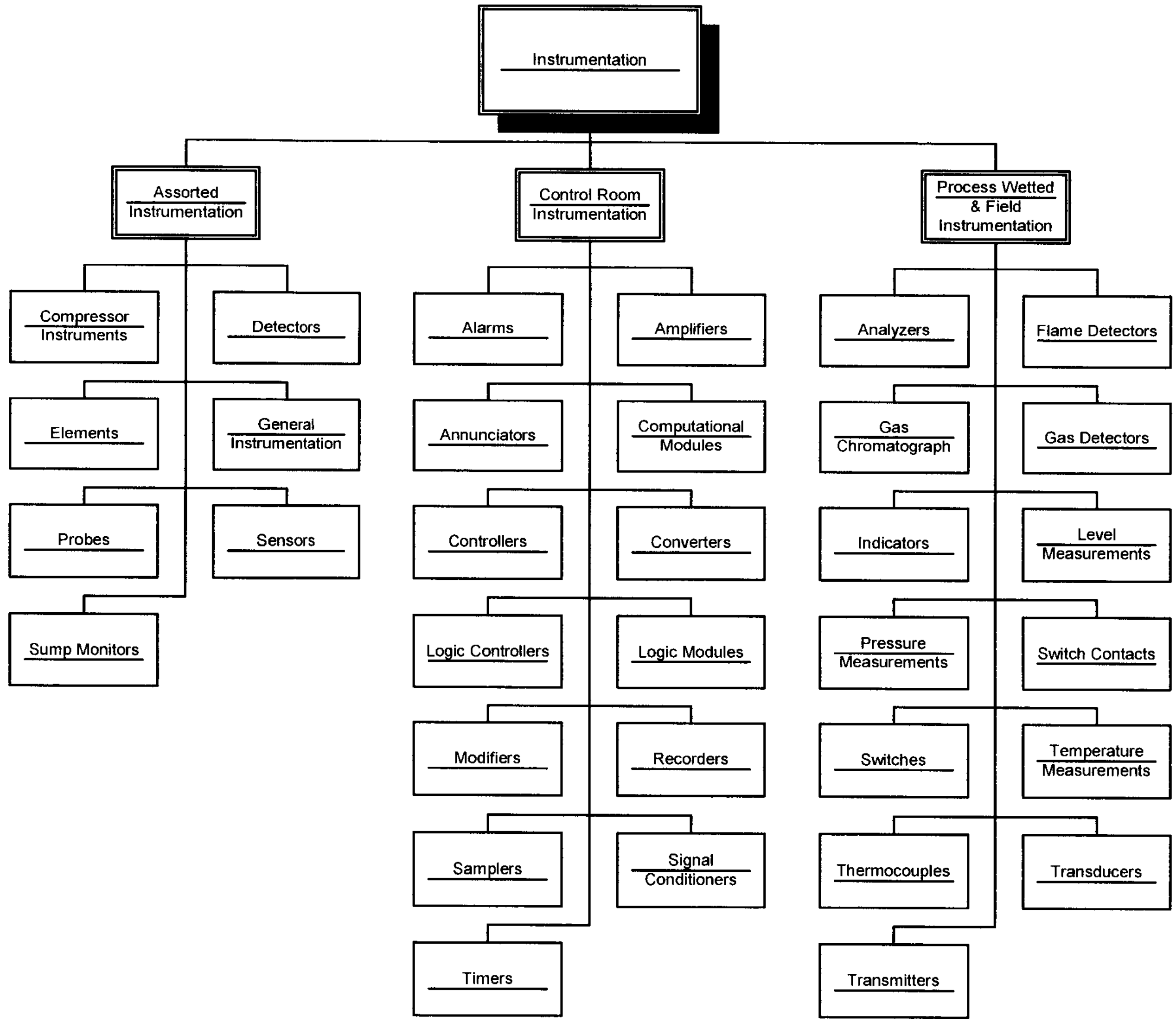
PCSA PROBABILITY DATA TAXONOMY (continued)



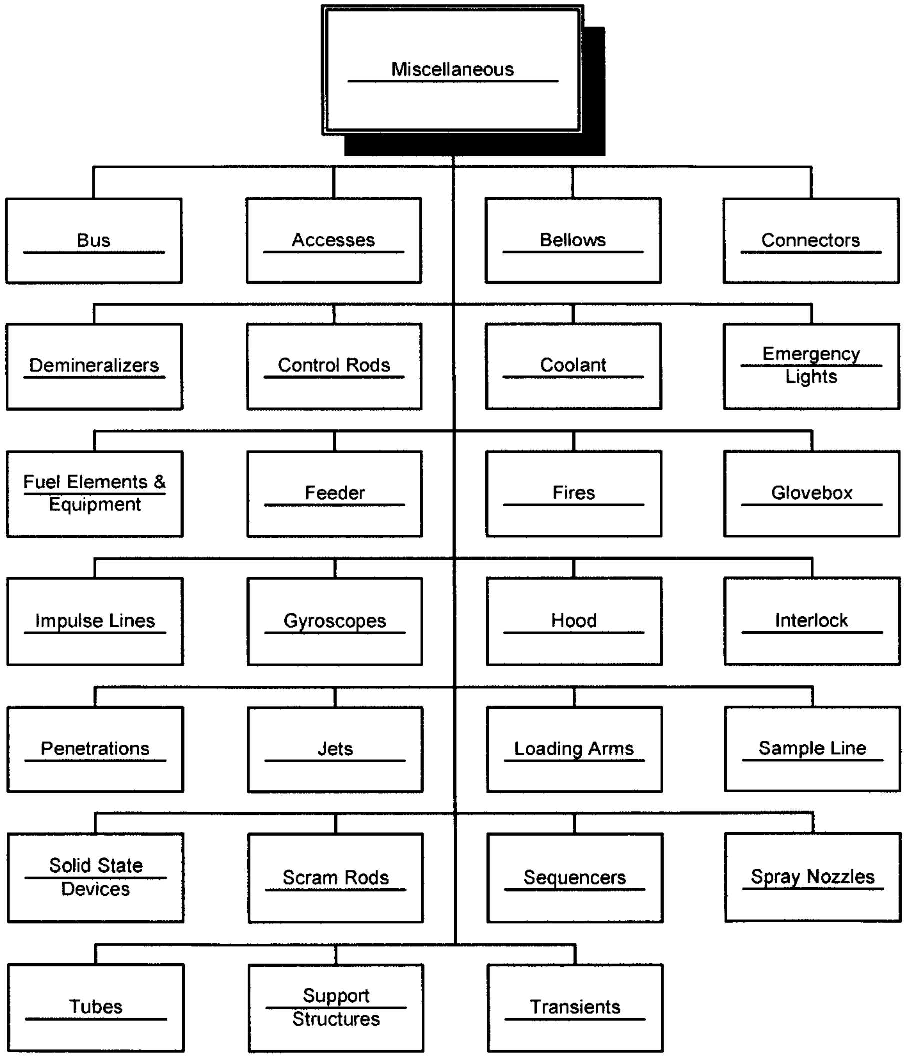
PCSA PROBABILITY DATA TAXONOMY (continued)



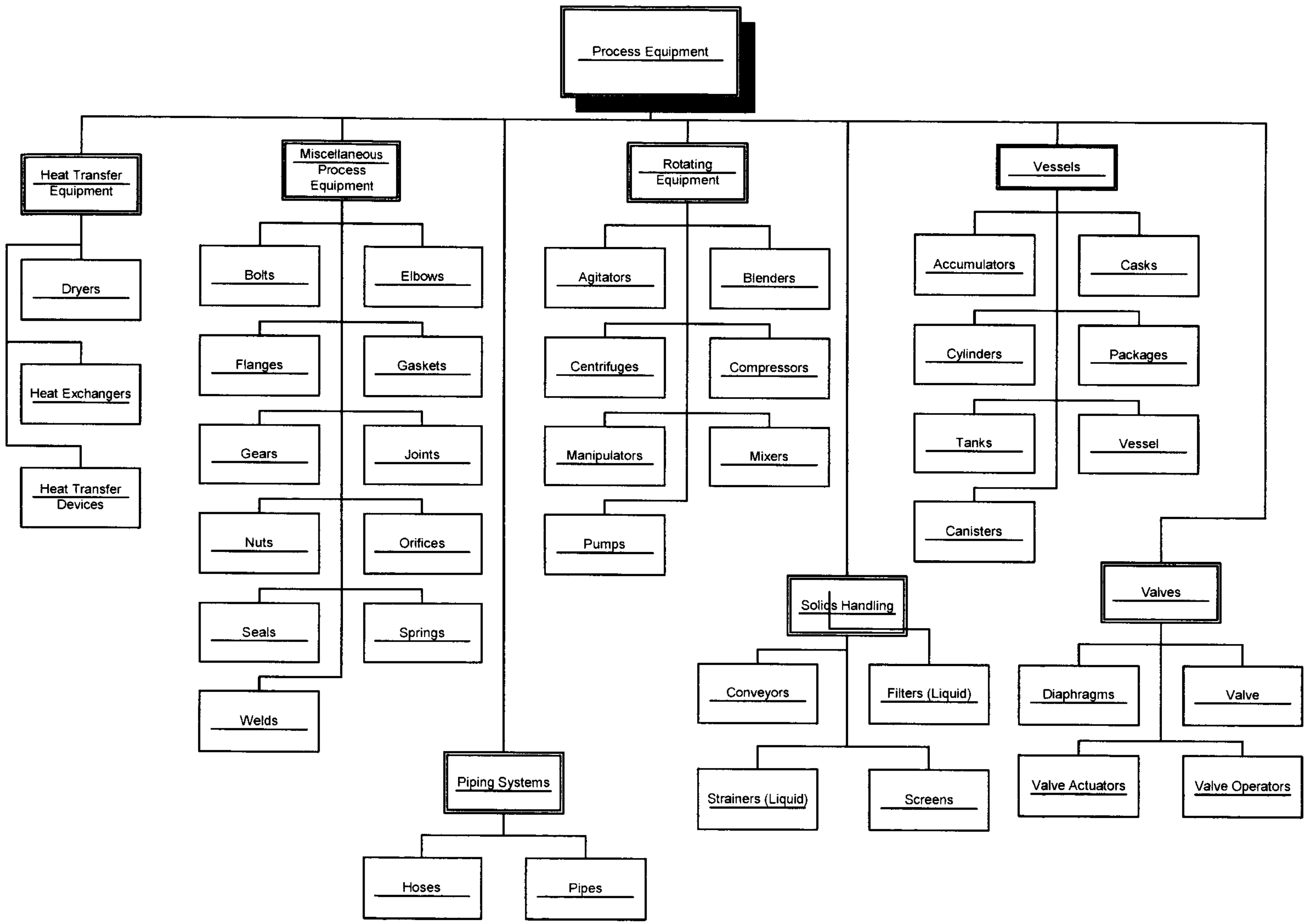
PCSA PROBABILITY DATA TAXONOMY (continued)



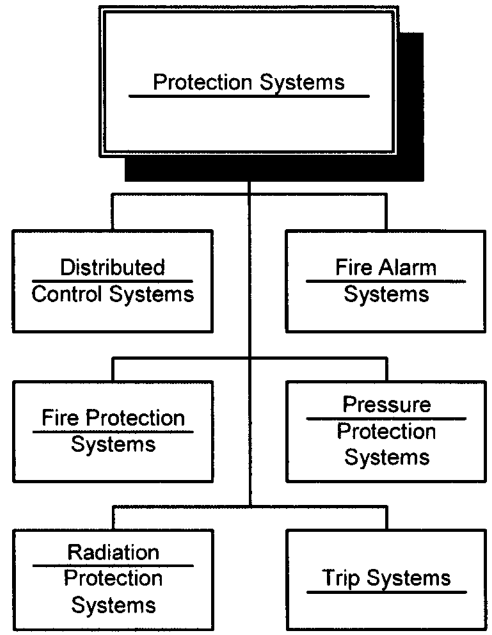
PCSA PROBABILITY DATA TAXONOMY (continued)



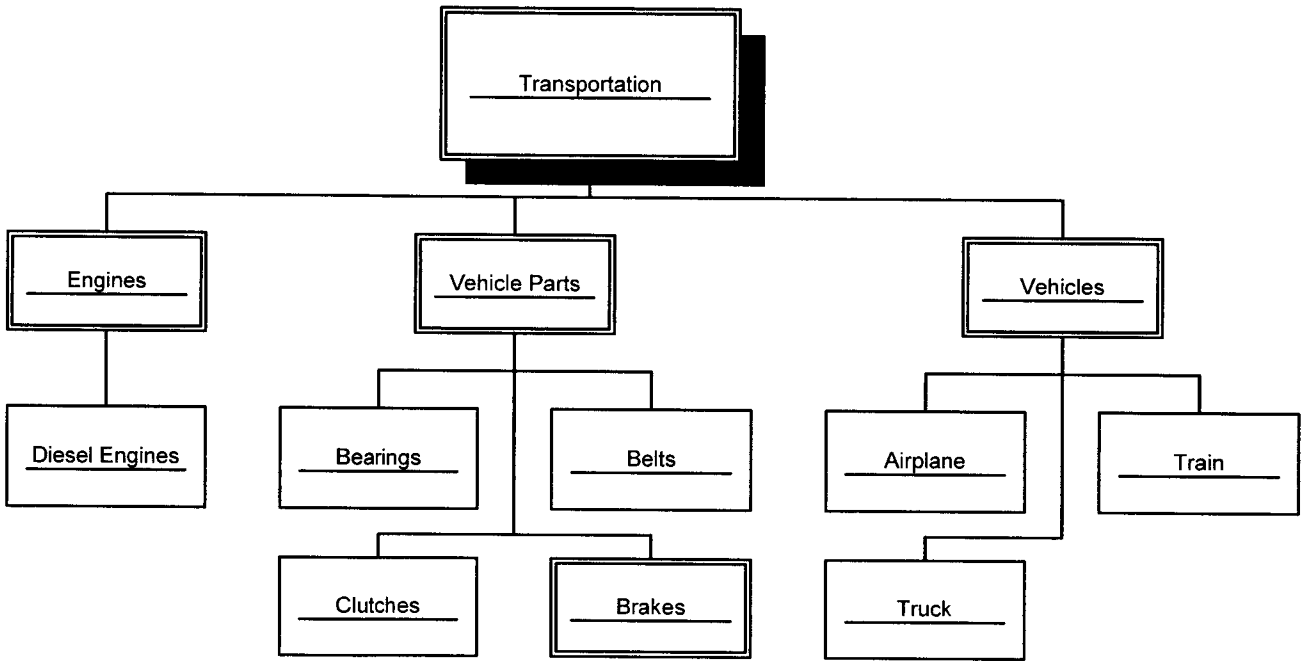
PCSA PROBABILITY DATA TAXONOMY (continued)



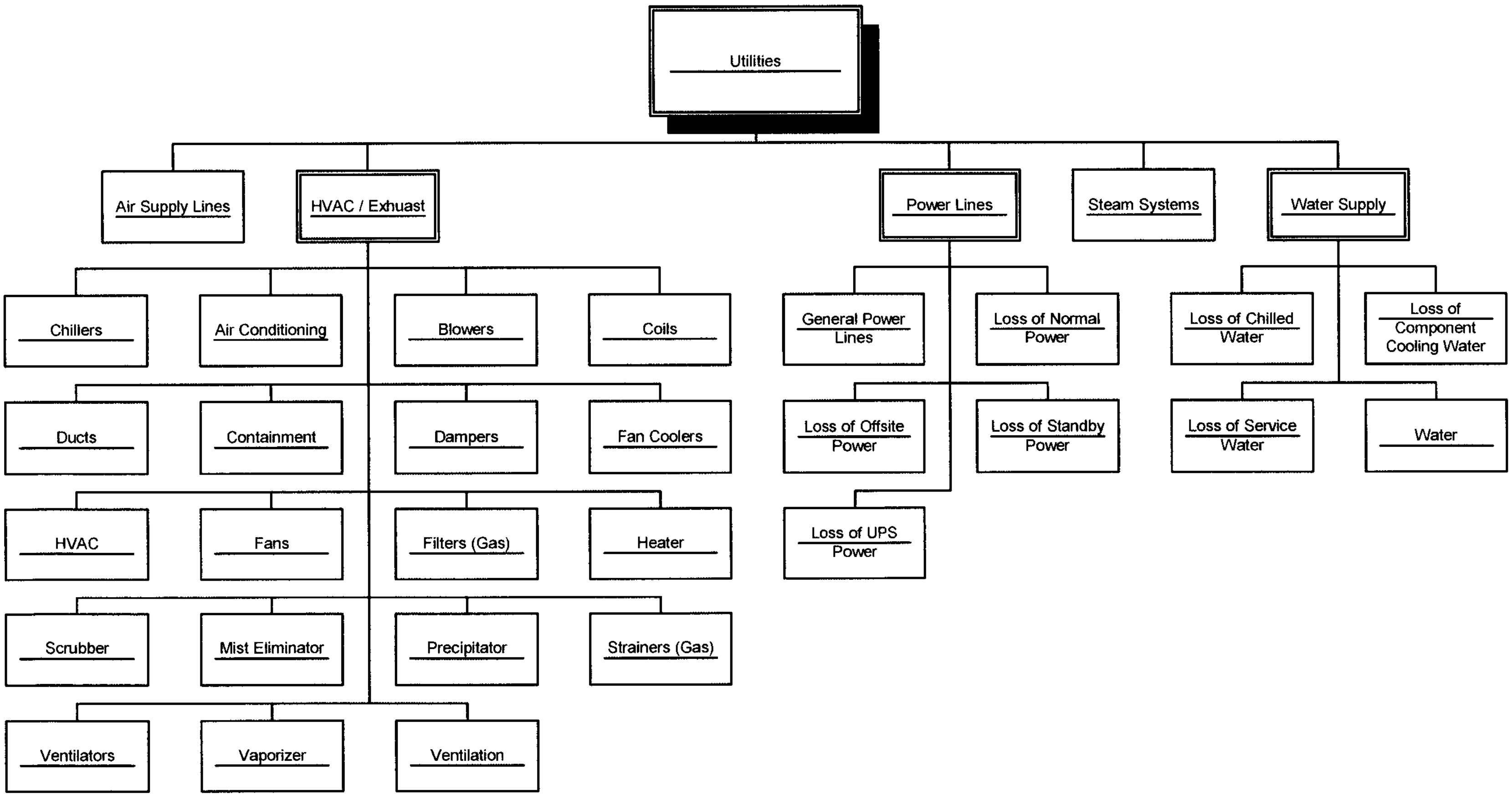
PCSA PROBABILITY DATA TAXONOMY (continued)



PCSA PROBABILITY DATA TAXONOMY (continued)



PCSA PROBABILITY DATA TAXONOMY (continued)



APPENDIX B

FAILURE RATE DATABASE REFERENCES LIST

The sources are divided into primary and secondary references. References from which data have been extracted for inclusion into the database are termed primary references. In most cases, each primary reference document has obtained its data inputs from several other references (secondary references). Letters denote primary references, while numbers have been used to represent secondary references. The list of references used in the database currently contains 37 primary references (denoted by alphabetical letters) and 108 secondary references (listed by numbers), for a total of 145 documents. The references, as they appear in this appendix, correspond with information in the PCSA Tool. Some documents may be listed as both primary and secondary references if they were utilized as a primary reference and were also listed as a secondary reference in another primary document. It should also be noted that gaps in the numbering system of the secondary references do not imply missing information. Rather, the database was organized in such a way that these gaps were a byproduct of its structure. The number assigned to each reference has no meaning other than as a simple tag to identify it.

Table B-1. Rate Database Reference List		
Letter ID	**Number ID**	**Book**
A		A.H. Dexter and W.C. Perkins. Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant. E.I. Du Pont de Nemours & Co., Savannah River Laboratory, Aiken, SC. (July, 1982)
B		Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area, A Pilot Study—A Report to the Rijnmond Public Authority. (Data obtained from part 2 of the report: an analysis of six industrial installations, prepared by Cremer and Warner Ltd.)
C		Offshore Reliability Data Handbook. 1st Edition. OREDA, Norway, (1984).
D		Guidelines for Process Equipment Reliability Data with Data Tables. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York (1989).
E		C.W. Ma, R.C. Sit, S.J. Zavoshy, L.J. Jardine. Preclosure Radiological Safety Analysis for Accident Conditions of the Potential Yucca Mountain Repository: Underground Facilities. Bechtel National, Inc. San Francisco for Sandia National Laboratories (1992).
F		Military Handbook – Reliability Prediction of Electronic Equipment, MIL-HDBK–217E.
G		R.J. Borkowski, J.P. Drago, J.R. Fragola, J.W. Johnson. The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report—the Pump Component. NUREG/CR–2886. ORNL/TM–8465, Oak Ridge National Laboratory (1982).
H		D.D. Orvis, C. Johnson, R. Jones. Review of Proposed Dry-Storage Concepts Using Probabilistic Risk Assessment. NP–3365, NUS Corporation, San Diego (1984).
I		R.J. Borkowski, J.P. Drago, J.R. Fragola, J.W. Johnson. The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report—the Valve Component. NUREG/CR–3154. ORNL/TM–8647, Oak Ridge National Laboratory (1983).
J		C.L. Atwood, D.L. Kelly, F.M. Marshall, D.A. Prawdzik, J.W. Stetkar. Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980-1996. NUREG/CR–5496. INEEL/EXT–97–00887, Idaho National Engineering and Environmental Laboratory (1998).
K		A.S. McClymont, B.W. Poehlman. Loss of Offsite Power at Nuclear Power Plants: Data and Analysis. NP–2301, Science Applications, Inc. Palo Alto (1982).

Table B-1. Rate Database Reference List (continued)

Letter ID	Number ID	Book
L		A.D. Swain, H.E. Guttmann. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications—Final Report. NUREG/CR–1278. SAND80–0200, Sandia National Laboratories (1983).
M		D. Jackson, T. Eaton, G. Hubbard. Draft Final Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants. Nuclear Regulatory Commission (2000).
N		C.F. Miller, W.H. Hubble, M. Trojovsky, S.R. Brown. Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants (Jan. 1, 1976 to Dec. 31, 1980). NUREG/CR–1363. EGG–EA–5816, EG&G Idaho, Inc. (1982).
O		D.W. Sams, M. Trojovsky. Data Summaries of Licensee Event Reports of Primary Containment Penetrations at U.S. Commercial Nuclear Power Plants (Jan. 1, 1972 to Dec. 31, 1978). NUREG/CR-1730. EGG-EA-5188, EG&G Idaho, Inc. (1980) Southwest Research Institute (1980).
P		Nuclear Plant Reliability Data System 1979 Annual Reports of Cumulative System and Component Reliability. NUREG/CR–1635. Southwest Research Institute (1980).
Q		J.P. Poloski, W.H. Sullivan. Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants (Jan. 1, 1976 to Dec. 31, 1978). NUREG/CR–1362. EGG–EA–5092, EG&G Idaho, Inc. (1980).
R		M. Trojovsky. Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants (Jan. 1, 1972 to Sep. 30, 1980). NUREG/CR–1205. EGG–EA–5524, EG&G Idaho, Inc. (1982).
S		G.L. Boner, H.W. Hanners. Enhancement of On-Site Emergency Diesel Generator Reliability. NUREG/CR–0660. UDR–TR–79–07, University of Dayton Research Institute (1979).
T		Nonelectronic Parts Reliability Data. NPRD–3, Reliability Analysis Center, Rome Air-Development Center, Grifis AFB, NY (Prepared by Michael J. Rossi, IIT Research Institute) (1985).
U		A.J. Duke. Reliability Techniques Used in the Assessment of Cranes. NCSR/GR/64. National Centre of Systems Reliability, United Kingdom Atomic Energy Authority. March, 1985.
V		Fire Risk Scoping Study: Investigation of Nuclear Power Plan Fire Risk, Including Previously Unaddressed Issues, NUREG/CR-5088, US Nuclear Regulatory Commission, January 1989.
W		"Generic component reliability data for research reactor PSA". International Atomic Energy Agency. IAEA-TECDOC-930, February 1997.

Table B-1. Rate Database Reference List (continued)		
Letter ID	Number ID	Book
X		Blanton, C.H. and Eide, S.A. "Savannah River Site Generic Data Base Development (U)". Westinghouse Savannah River Company, Savannah River Site - Aiken , S.C. WSRC-TR-93-262 (June 30, 1993).
Y		Houston Lighting and Power Co. "Level 2 Probabilistic Safety Assessment and Individual Plant Examination." South Texas Project Electric Generating Station, August 1992.
Z		Lees, Frank P. "Loss Prevention in the Process Industries; Hazard Identification, Assessment and Control". Second Edition.
AA		Lox, C.R., Cramer, D.S., Wellmaker, K.A. and Salaymeh, S.R. "Savannah River Site Hazard Analysis Generic Initiator Database". WSRC-RP-95-915, Rev. 0. Westinghouse Savannah River Company, Savannah River Site. Aiken, SC. October, 1995.
BB		Component Reliability Data for Use in Probabilistic Safety Assessment". IAEA-TECDOC-478. Issued by the International Atomic Energy Agency, Vienna, 1988.
CC		Pickard, Lowe and Garrick, Inc. "Salem Nuclear Generating Station Reliability and Safety Management Program - Baselin Safety Assessment" PLG-0493. Prepared for Public Service Electric and Gas Company, New Jersey. July 1986.
DD		"Analysis of Mechanisms for Early Waste Package Failure". ANL-EBS-MD-000023 REV 00.
EE		"Database for Probabilistic Risk Assessment of Light Water Nuclear Power Plants". Pickard, Lowe and Garrick, Inc. July, 1989.
FF		"DBE/Scenario Analysis for Preclosure Repository Subsurface Facilities". BCA000000-01717-0200-00017 REV 00, Attachment XIV.
GG		T.G. Alber, R.C. Hunt, S.P. Fogarty, J.R. Wilson. "Idaho Chemical Processing Plant Failure Rate Database". Idaho National Engineering Laboratory, Lockheed Idaho Technologies Company, Idaho Falls, Idaho. INEL-95/0422, August 1995.
HH		Geffen, C.A. et. al. "An Assessment of the Risk of Transporting Propane by Truck and Train", Pacific Northwest Laboratory. Richland, Washington dated March 1980.
II		US Nuclear Regulatory Commission "Reactor Safety Study - an Assessment of Accident Risks in the U.S. Commercial Nuclear Power Plants"; WASH-1400, October 1975, Appendix III "Failure Data" (and references therein).
JJ		Greenfield, Moses and Sargent, Thomas. Probability of Failure of the Waste Hoist Brake System at the Waste Isolation Pilot Plant (WIPP). Environmental Evaluation Group, New Mexico, January 1998.
KK		NOT USED

Rate Database Reference List (continued)		
Letter ID	Number ID	Book
LL		IEEE (Institute of Electrical and Electronic Engineers, Inc.), 1984. Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, ANSI/IEEE Std 500 (NNA.9004003.0396).
	1	U.S. Nuclear Regulatory Commission, "Control of Heavy Loads at Nuclear Power Plants, Resolution of Generic Technical Activity A-36," NUREG–0612, July 1980.
	2	NRC (US Nuclear Regulatory Commission), 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, (NUREG-75/014), U.S. Nuclear Regulatory Commission, Washington, DC (NNA.901130.0005-.0012).
	3	IEEE (Institute of Electrical and Electronic Engineers, Inc.), 1984. Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, ANSI/IEEE Std 500 (NNA.9004003.0396).
	4	Green, A.E. and Bourne, A.J. "Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors - Part 3." UKAEA AMSB(S) R117 - 1976.
	5	Lawley, H.G. and Kletz T.A. Chemical Engineering, 12th May 1975.
	6	US Atomic Energy Commission Reactor Safety Study—An Assessment of Accident Risks in the U.S. Commercial Nuclear Power Plants; WASH–1400, October 1975, Appendix III "Failure Data" (and references therein).
	7	Fragola, Joseph. Science Applications International Corp. Proprietary Data Set. SAIC, New York.
	8	The In-Plant Reliability Data Base for Nuclear Power Plant Components. USNRC-RES (1984), Obtain reports from the NTIS.
	9	IEEE Standard 500. IEEE Service Center, Piscataway, NJ (1984).
	10	Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Programming Guide (NREP). USNRC-RES, Obtain reports from EG&G Idaho, Inc. Idaho Falls, ID.
	11	Big Rock Point Probabilistic Risk Assessment. Consumers Power Co. (1979).
	12	Indian Point Units 2 and 3 Probabilistic Risk Assessment. Consolidated Edison and New York Power Authority (December 1979).
	13	Interim Reliability Evaluation Program: Analysis of the Millstone Point 1 Nuclear Power Plant Assessment. Northeast Utilities (1985).

	Table B-1. Rate Database Reference List (continued)	
Letter ID	Number ID	Book
	14	Yankee Nuclear Power Station Probabilistic Safety Study. Yankee Atomic Electric Co. (1983).
	15	Zion Probabilistic Safety Study. Commonwealth Edison Co. (1981).
	17	NUREG/CR–0942, Nuclear Plant Reliability Data System 1978 Annual Reports of Cumulative System and Component Reliability, Southwest Research Institute, San Antonio, Texas (Sept. 1979).
	18	A.E. Green and A. J. Bourne. Reliability Technology, John Wiley, New York (1972).
	19	Nonelectronic Parts Reliability Data. NPPD-1, Reliability Analysis Center, Rome Air-Development Center, Grifis AFB, NY (Prepared by Donald W. Fulton, IIT Research Institute) (1978).
	20	B.J. Garrick, W.C. Gekler, L. Goldfisher, R.H. Karcher, B. Shimizu, and J.H. Wilson. HN-190, Reliability Analysis of Nuclear Power Plant Protective Systems. Holmes and Narver, Inc., Nuclear Division, Los Angeles, CA. (Also refer to references23 and 24) (May 1967).
	21	A. A. Schmudde. "Engine Generator Sets Meet Strict Reliability Limits." Power (April 1967).
	22	E. R. Snaith. Nuclear Engineering and Design. 13, 216 (1970).
	23	D.R. Earles. Reliability Application and Analysis Guide. MI–60–54 (Rev. 1), The Martin Co. (July 1961).
	24	"Reliability Stress and Failure Rate Data for Electronic Equipment." Military Standardization Handbook, MIL–HDBK–217A, Department of Defense, (Dec. 1965).
	25	"Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, WASH-1400 (NUREG-75/014). Appendix III and IV (October 1975).
	26	NRC (US Nuclear Regulatory Commission), 1985. Evaluation of Station Blackout Accidents at Nuclear Power Plants, NUREG-1032, U.S. Nuclear Regulatory Commission, Washington, DC (NNA.890906.0189)
	38	RADC NonElectronic Reliability Notebook. Rome Air Development Center, Griffiss AFB, NY (1985). NTIS Report No: AD/A163 900.
	41	Reliability Data Book for Components in Swedish Nuclear Power Plants. Swedish State Power Board. Nuclear Safety Board of the Swedish Utilities, Stockholm.
	45	Offshore Reliabiity Data Handbook (OREDA). OREDA Committee, Norway (1984).
	46	Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants (WASH-1400). USNRC (1974) Obtain reports from NTIS.

Table B-1. Rate Database Reference List (continued)		
Letter ID	Number ID	Book
	53	Oconee-3 PRA: A Probabilistic Risk Assessment of Oconee Unit 3. Electric Power Research Institute and Duke Power, Research Reports Center, Palo Alto, CA. Report No: NSAC-60, Volumes 1–5, (June 1984).
	59	Reliability Prediction of Electronic Equipment (Military Handbook 217E). Rome Air Development Center, Griffiss AFB, NY.
	86	Data Summaries of Licensee Event Reports at U.S. Commercial Nuclear Power Plants (Various Components). USNRC–RES, (1983). Obtain reports from NTIS.
	92	S.N. Anyakora, G.F.M. Engel and F.P. Lees. "Some Data on the Reliability of Instruments in the Chemical Plant Environment." The Chemical Engineer (November 1971).
	95	S.B. Gibson. "The Design of New Chemical Plants Using Hazard Analysis." Institution of Chemical Engineers Symposium Series No. 41 (1976).
	96	Lees, F.P. Chemistry and Industry (March 6, 1976).
	97	Lees, F.P. "A Review of Instrument Failure Data." I.Chem. Eng. Symposium No. 47, 1976 (and references therein).
	98	Skala, V. "Improving Instrument Service Factors" Instrumentation Technology, November 1974.
	103	A.E. Green and A.J. Bourne. Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors. U. K. Atomic Energy Authority Health and Safety Branch, Rep. AHSB(s) R117, Part 3, Risley, Lancashire (1966).
	106	Development of an Improved Liquefied Natural Gas Plant Failure Rate Data Base. Gas Research Institute (June 1981). NTIS Report No. PB 82–153503.
	132	Science Applications, Inc. LNG Terminal Risk Assessment Study for Los Angeles, California, Report prepared for Western LNG Terminal Company, December 1975.
	137	"Technology for Commercial Radioactive Waste Management," U.S. department of Energy, DOE/ET. 0028, May 1979, Table 5.6.68.
	138	Dennis, A.W., J.T. Foley, Jr., W.F. Hartman, and D.W. Larson, 1978. Severities of Transportation Accidents Involving Large Packages, SAND77–0001, Sandia National Laboratories, Albuquerque, NM (NNA.900417.0026).

Table B-1. Rate Database Reference List (continued)		
Letter ID	Number ID	Book
	155	Reliability Stress and Failure Rate Data for Electronic Equipment. Military Standardization Handbook, MIL–HDBK–217A, Department of Defense, (Dec. 1965).
	156	Probabilistic Risk Assessment: Big Rock Point Plant Table VI.27, Consumers Power Company, 1981.
	161	EPRI NP-1128. Status Report on the EPRI Fuel Cycle Accident Risk Assessment (July 1979).
	163	Probabilistic Risk Assessment, Limerick Generating Station, Philadelphia Electric Co., March, 1981.
	168	Welker, J.R. et al, "Fire Safety Aboard LNG Vessels," NTIS AD/A–030 619, January 1976.
	186	Probabilistic Risk Assessment: Big Rock Point Plant Table III-4C, Consumers Power Company, 1981.
	187	Zion Probabilistic Safety Study, Table II 4-7, Commonwealth Edison Company, 1981.
	195	R.J. Campana, et al, "A Methodology for Operational Risk Assessment of a Spent Unreprocessed Fuel, Bedded Slat Repository," Sandia National Laboratory, NUREG/CR-1931, July, 1981.
	196	N.C. Finley, et al, ""Transportation of Radionuclides in Urban Environs: Draft Environmental Assessment," Sandia National Laboratories, NUREG/CR-0743, July, 1970.
	199	Jacobs, R.M. "Minimizing Hazards in Design," Quality Progress, October 1971.
	200	Hazardous Waste Tank Failure. US EPA, NTIS Report No.: PB86–192945 (1985).
	204	Safety of Interstate Natural Gas Pipelines. A report prepared for the use of the U.S. Senate Committee on Commerce by the Federal Power Commission, U.S. Government Printing Office, Washington, DC (1966).
	206	SRS Data Bank
	207	Smith, T.A. and Warwick, R.G. "The Second Survey of Defects in Pressure Vessels Built to High Standards of Construction and its Relevance to Nucelar Primary Circuits," Safety and Reliability Directorate, SRD R30, 1974.
	208	Phillips C.A.G. and Warwick, R.G. A Survey of Defects in Pressure Vessels Built to High Standards of Construction and its Relevance to Nuclear Primary Circuits." UKAEA AHSB(S) R162 1969.
	209	An Analysis of Reportable Incidents for Natural Gas Transmission and Gathering Lines - 1970 through June 1984. American Gas Association, Order Processing Depart., Arlington, VA (1984).
	212	"Zion Probabilistic Safety Study", Commonwealth Edison Company, 1981.

Table B-1. Rate Database Reference List (continued)		
Letter ID	Number ID	Book
	218	W. M. Coltharp, R. D. Delleney, C. E. Riese, and T.I. Strange. Determining Availability of Steam Supply Systems. Loss Prevention, 12, 53 (1978).
	220	D.J. Sherwin. "Failure and Maintenance Data Analysis at a Petrochemical Plant." Reliability Engineering, C98 Vol. 5 (1983).
	229	R. Deuschle and J. Goldberg. Instruments and Control Systems, 47, 67 (March 1974).
	241	Data Summaries of Licensee Event Reports at U.S. Commercial Nuclear Power Plants (Various Components). USNRC-RES, (1983). Obtain reports from NTIS.
	245	Plant 1
	246	Plant 2
	247	Plant 3
	248	Plant 4
	287	C. A. G. Phillips and R.G. Warwick. Nuclear Engineering and Design. 13, 227 (1970).
	294	Marsall, W. et al, "An Assessment of the Integrity of PWR Prsssure Vessels," UKAEA Report (October 1976).
	295	Bush, S.H. "Pressure Vessel Reliability," Trans. Of ASME–Journal of Pressure Vessel Technology, February 1975.
	301	J.R. Engel. "Pressure Vessel Failure Statistics and Probabilities". Nuclear Safety, Vol. 15, No.4, (July-August 1974).
	302	M. J. Miller. "Reliability of Fire Protection Systems." Chem. Eng. Prog. 70, 62 (1974).
	314	Kletz T.A. "Specifying and Designing Protective Systems" A.I. Chem. Eng. Loss Prevention Vol.6, 1972.
	316	Nonelectronic Parts Reliability Data. NPRD–3, Reliability Analysis Center, Rome Air-Development Center, Grifis AFB, NY (Prepared by Michael J. Rossi, IIT Research Institute) (1985).
	317	Pickard, Lowe and Garrick, Inc., "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants," PLG-0209, June 1981.
	318	Dexter, A.H., and Perkins, W.C. "Component Failure Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant". E.I. du Pont de Nemours and Company, Savannah River Laboratory, July 1982.
	319	"Evaluations of Accident Risks in the Transportation of Hazards Material by Truck and Rail at the Savannah River Site" (U). WSRC-RP-89-715, Revision 1, Westinghouse Savannah River Company, Aiken, SC. September 1992.
	320	Cramer, D.S. "Database for Probabilistic Risk Assessment of the Uranium Solidification Facility" (U). SRT-DCA-93002, Westinghouse Savannah River Company, Aiken, SC, November 1993.

Table B-1. Rate Database Reference List (continued)		
Letter ID	Number ID	Book
	321	Brandyberry, M.D., Cramer, D.S., et.al. 'SRS PRA of Reactor Operation – Level 1, Internal Events". Westinghouse Savannah River Company, Aiken, SC, June 1990.
	322	Blanton, C.H. and Eide, S.A. (LATA). "Savannah River Site Generic Data Base Development" (U). WSRC-TR-93-262, Westinghouse Savannah River Company, Aiken, SC, June 1993.
	323	Cramer, D.S. to PRA File, "Reactor Risk Analysis Group. Failure Modes and Rates for Automatic Transfer Switches". SRL-PRA-910276, E.I. du Pont de Nemours and Company, Savannah River Laboratory, Aiken, SC, August 1991.
	324	Cramer, D.S. "Data Base Development and Equipment Reliability for Phase 1 of the Probabilistic Risk Analysis". DPST-87-642, E.I. du Pont de Nemours and Company, Savannah River Laboratory, Aiken, SC, October 1987.
	325	OREDA, "Offshore Reliability Data Handbook". 1st Edition, OREDA, Hovik, Norway, 1984.
	326	"IEEE Guide to the Collection and presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations". IEEE, Std 500-1984, The Institute for Electrical and Electronics Engineers, Inc., New York, New York, December 1993.
	327	Tinnes, S.P. "Probabilistic Risk Assessment of SRS Reactor Scram Channel Wiring Failures" (U). WSRC-RP-90-1308, Westinghouse Savannah River Company, Aiken, SC, November 1990.
	328	Cramer, D.S. "Fires Plus Explosions in Oil Filled Electrical Transformers" (U). Calc-Note Q-CLC-G-00008, Rev. 0, Westinghouse Savannah River Company, Aiken, SC, November 1994.
	329	"IWP Methodology Manual for IWP Implementation". (Draft to be issued October 1995).
	330	Jansen, J.M. and Mason, C.L. "Frequency of Deflagration in the In-Tank Precipitation Process Tanks Due to Loss of Nitrogen Purge System" (U). WSRC-TR-93-169, Rev. 2, Westinghouse Savannah River Company, Aiken, SC, January 1994.
	332	Lee, M.W., and Prout, W.E. "Statistical Analysis of Sand Filter Efficiency". DPST-79-506, E.I. du Pont de Nemours and Company, Savannah River Laboratory, Aiken, SC. September 1979.
	333	Benhardt, H.C., Eide, S.A., Held, J.E., Olsen, L.M., and Vail, R.E. "Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities" (U). WSRC-TR-93-581, Westinghouse Savannah River Company, Aiken, SC, February 1994.
	334	Brandyberry, M.D., Cramer, D.S., and Logan, V.E. "Analysis of the Frequency of Loss of Control Rod or Fuel Assembly Cooling Due to Plugging" (ILCR/LOFA) (U). WSRC-RP-91-956,Westinghouse Savannah River Company, Aiken, SC, October 1991.

Table B-1. Rate Database Reference List (continued)

Letter ID	Number ID	Book
	335	J. R. Wilson, JRW-2-91, to N.C. Olson, "Transmittal of TS/S Violation Report," dated March 5, 1991.
	336	J. R. Wilson, JRW-5-93, to L.H. Frauenholz, "ICPP Power Outage Study," dated May 21, 1993.
	337	J. R. Wilson, JRW-2-87, to R.D. Bradley, "Transmittal of Report on Chemical Makeup Errors (R&D) Project," dated January 6, 1987.
	338	J. R. Wilson, JRW-22-86, to R.D. Bradley, "State of Maintenance Error Controversy (R&D) Project," dated December 31, 1986.
	339	B.J. Harwood, BJH-01-88, to J.R. Wilson, "CPP-601 Volume Measurement Error (R and D Project)," dated March 23, 1988.
	340	J. R. Wilson, JRW-23-85, to R. D. Bradley, "Transmittal of Data Analysis Study of Inadvertent Transfers (R and D Project)," dated December 31, 1986.
	341	J. N. Wilkinson, JNW-3-89, to J. R. Wilson, "Update of Frequency of Plugging Various Instrument and Equipment Items," dated June 8, 1989.
	342	J. R. Wilson, JRW-9-87, to R. D. Bradley, "Transmittal of Human Factors Report on Sampling and Analytical Processes (R & D Project)," dated February 10, 1987.
	343	T. G. Alber, TGA-03-94, to J. R. Wilson, "Study of Crane Related Failures at the Idaho Chemical Processing Plant," dated September 20, 1994.
	344	M. J. Miller, "Reliability of Fire Protection Systems", Chemical Engineering Progress, Vol. 70, No. 4, dated April 1974.
	345	W. C. Perkins, Frequency Probability Evaluation of 200-Area Process Laboratory Errors, DPST-84-543, Savannah River Laboratory, dated October 16, 1984.
	346	W. C. Perkins, et. al., "Failure Rates for Liquid Level Detectors in F-Canyon Sumps", DPST-83-820, Savannah River Laboratory, dated September 8, 1983.
	347	A.D. Swain, and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application", NUREG/CR-1278, USNRC, dated August 1983.
	348	Systems Anlysis-200 Area, Savannah River Plant, H-Canyon Operations, DPSTSY-200-1H, Savannah River Laboratory. Based on MTBF of 6 days for 160 probes. Evaporators No. 1 contributor, dissolvers/ion exchange next, and waste neutralization average.

Table B-1. Rate Database Reference List (continued)		
Letter ID	Number ID	Book
	349	Eide, S.A., and M.B. Calley. Generic Component Failure Database, Proceedings Probabilistic Safety Assessment and Management, PSA '93, American Nuclear Society, Clearwater Beach Florida, Jan. 1993; based on Nuclear Computerized Library for Assessing Reactor Probability, (NUCLARR), US NRC, NUREG/CR-4639, June 1989.
	350	Ref 5.3Waste Handling Systems Configuration Analysis, BCBBD0000-01717-0200-00001 REV 00, CRWMS.
	351	Swain, A.D. Accident Sequence Evaluation Program Human Reliability Analysis Procedure, US NRC, NUREG/CR-4772, February 1987.

APPENDIX C

CRANE FAILURE DATA

The failure rate data for cranes is presented in this appendix as an example of the type of data available in the database.

Table C-1. Crane Failure Rates

Equipment Type	Group	Description	Field 1	Field 2	Field 3	Ref	Unit	Failure Rate	High Value	Low Value	Remark	20% Lower	80% Upper
CRANE SYSTEMS		OVERHEAD CRANES				E2	/HR	5.00e-05					
CRANE SYSTEMS		OVERHEAD BRIDGE CRANES	10 TON			E3	/HR	1.10e-04					
CRANE SYSTEMS		BRIDGE CRANES	BASE RANGE OF FAILURE OF HANDLING SYSTEM			M1	/YR	5.40e-05	1.50e-04	1.00e-05			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FRACTION OF LOAD HANGUP EVENTS	(1990 NAVY DATA)	M1	N/A	1.40e-01	1.40e-01	1.40e-01			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FAILURE OF THE OVERLOAD DEVICE		M1	/DM	4.00e-03	1.00e-02	1.00e-03			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FRACTION OF COMPONENT FAILURE EVENTS	(1990 NAVY DATA)	M1	N/A	6.10e-01	6.10e-01	6.10e-01			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FRACTION OF TWO BLOCKING EVENTS	(1990 NAVY DATA)	M1	N/A	5.00e-02	5.00e-02	5.00e-02			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FAILURE OF LOWER LIMIT SWITCH		M1	/DM	4.00e-03	1.00e-02	1.00e-03			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FAILURE OF UPPER LIMIT SWITCH		M1	/DM	4.00e-02	1.00e-01	1.00e-02			

Table C-1. Crane Failure Rates (continued)														
Equipment Type	**Group**	**Description**	**Field 1**	**Field 2**	**Field 3**	**Ref**	**Unit**	**Failure Rate**	**High Value**	**Low Value**	**Remark**	**20% Lower**	**80% Upper**
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	FRACTION OF SINGLE COMPONENT FAILURE	(1990 NAVY DATA)	M1	N/A	1.00e-02	1.00e-02	1.00e-02			
CRANE SYSTEMS		BRIDGE CRANES	CRANE FAILURE	LIFTS PER YEAR LEADING TO DROP	(100 YEAR/ LIFTS, DROPS FROM	M1	NO.	3.00e+00	3.00e+00	3.00e+00			
CRANE SYSTEMS		BRIDGE CRANES	RIGGING FAILURE (BASED ON WIPP METHOD)	FRACTION OF IMPROPER RIGGING EVENTS	(1990 NAVY DATA)	M1	N/A	2.10e-01	2.10e-01	2.10e-01			
CRANE SYSTEMS		BRIDGE CRANES	RIGGING FAILURE (BASED ON WIPP METHOD)	FAILURE CAUSED BY IMPROPER RIGGING	(MEAN FROM WIPP STUDY)	M1	/YR	8.70e-07	8.70e-07	8.70e-07			
CRANE SYSTEMS		BRIDGE CRANES	FAILURE CAUSED BY IMPROPER RIGGING	LIFTS PER YEAR LEADING TO DROP	(100 LIFTS/ YEAR, DROPS FROM RIGGING	M1	NO.	6.00e+00	6.00e+00	6.00e+00			
CRANE SYSTEMS		BRIDGE CRANES	LOSS OF INVENTORY FOR A SINGLE-FAILURE-PROOF CRANE	FRACTION OF YEAR OVER WHICH A RELEASE MAY OCCUR		M1	N/A	1.00e+00	1.00e+00	1.00e+00			

Table C-1. Crane Failure Rates (continued)													
Equipment Type	Group	Description	Field 1	Field 2	Field 3	Ref	Unit	Failure Rate	High Value	Low Value	Remark	20% Lower	80% Upper
CRANE SYSTEMS		BRIDGE CRANES	LOSS OF INVENTORY FOR A SINGLE-FAILURE-PROOF CRANE	FRACTION OF PATH NEAR/OVER POOL		M1	N/A	1.30e-01	2.50e-01	5.00e-02			
CRANE SYSTEMS		BRIDGE CRANES	LOSS OF INVENTORY FOR A SINGLE-FAILURE-PROOF CRANE	FRACTION OF PATH CRITICAL FOR LOAD DROP		M1	N/A	1.60e-01	2.50e-01	1.00e-01			
CRANE SYSTEMS		BRIDGE CRANES	LOSS OF INVENTORY FOR A NONSINGLE-FAILURE-PROOF CRANE	TOTAL FAILURES LEADING TO A DROPPED LOAD		M1	NO.	2.10e-05	7.50e-05	1.00e-07			
CRANE SYSTEMS		BRIDGE CRANES	LOSS OF INVENTORY FOR A NONSINGLE-FAILURE PROOF CRANE	FRACTION OF YEAR OVER WHICH A RELEASE MAY OCCUR		M1	N/A	1.00e+00	1.00e+00	1.00e+00			
CRANE SYSTEMS		BRIDGE CRANES	HOOK	CATASTROPHIC FRACTURE		U	/YR	1.00e-06					
CRANE SYSTEMS		BRIDGE CRANES	HOOK	CATASTROPHIC FRACTURE		U	/DM	2.00e-09					
CRANE SYSTEMS		BRIDGE CRANES	ROPE SYSTEM	BREAK		U	/YR	2.00e-03					
CRANE SYSTEMS		BRIDGE CRANES	ROPE SYSTEM	BREAK		U	/DM	4.00e-06					

Table C-1. Crane Failure Rates (continued)													
Equipment Type	Group	Description	Field 1	Field 2	Field 3	Ref	Unit	Failure Rate	High Value	Low Value	Remark	20% Lower	80% Upper
CRANE SYSTEMS		BRIDGE CRANES	ROPE DRUM	CATASTROPHIC FRACTURE		U	/YR	2.00e-05					
CRANE SYSTEMS		BRIDGE CRANES	ROPE DRUM	CATASTROPHIC FRACTURE		U	/DM	4.00e-08					
CRANE SYSTEMS		BRIDGE CRANES	DRUM BEARING & PEDESTAL	COLLAPSE/ CATASTROPHIC FRACTURE		U	/YR	2.00e-05					
CRANE SYSTEMS		BRIDGE CRANES	DRUM BEARING & PEDESTAL	COLLAPSE/ CATASTROPHIC FRACTURE		U	/DM	4.00e-08					
CRANE SYSTEMS		BRIDGE CRANES	DRUM/GEAR BOX SHAFT	SHAFT SHEAR		U	/YR	1.00e-04					
CRANE SYSTEMS		BRIDGE CRANES	DRUM/GEAR BOX SHAFT	SHAFT SHEAR		U	/DM	2.00e-07					
CRANE SYSTEMS		BRIDGE CRANES	DRUM/GEAR BOX SHAFT AND COUPLING	COUPLING CATASTROPHIC FAILURE, KEY SHEAR, BOLT SHEAR		U	/YR	4.00e-04					
CRANE SYSTEMS		BRIDGE CRANES	DRUM/GEARB OX SHAFT AND COUPLING	COUPLING CATASTROPHIC FAILURE, KEY SHEAR, BOLT SHEAR		U	/DM	8.00e-07					
CRANE SYSTEMS		BRIDGE CRANES	GEARBOX	BROKEN TEETH, SHAFT FAILURE, KEY SHEAR		U	/YR	5.00e-04					
CRANE SYSTEMS		BRIDGE CRANES	GEARBOX	BROKEN TEETH, SHAFT FAILURE, KEY SHEAR		U	/DM	1.00e-06					
CRANE SYSTEMS		BRIDGE CRANES	GEARBOX/ BRAKE SHAFT	SHAFT SHEAR		U	/YR	1.00e-04					

Table C-1. Crane Failure Rates (continued)

Equipment Type	Group	Description	Field 1	Field 2	Field 3	Ref	Unit	Failure Rate	High Value	Low Value	Remark	20% Lower	80% Upper
CRANE SYSTEMS		BRIDGE CRANES	GEARBOX/ BRAKE SHAFT	SHAFT SHEAR		U	/DM	2.00e-07					
CRANE SYSTEMS		BRIDGE CRANES	GEARBOX/ BRAKE SHAFT AND COUPLING	COUPLING CATASTROPHIC FAILURE, KEY SHEAR, BOLT SHEAR		U	/YR	4.00e-04					
CRANE SYSTEMS		BRIDGE CRANES	GEARBOX/ BRAKE SHAFT AND COUPLING	COUPLING CATASTROPHIC FAILURE, KEY SHEAR, BOLT SHEAR		U	/DM	8.00e-07					
CRANE SYSTEMS		BRIDGE CRANES	BRAKE (THRUSTER TYPE)	SPRING FAILURE, JAMMING OF THE MECHANISM OFF, DRUM FAILURE, CONTAMINATION OF THE BRAKE LINING		U	/YR	5.00e-03					
CRANE SYSTEMS		BRIDGE CRANES	BRAKE (THRUSTER TYPE)	SPRING FAILURE, JAMMING OF THE MECHANISM OFF, DRUM FAILURE, CONTAMINATION OF THE BRAKE LINING		U	/DM	1.00e-05					
CRANE SYSTEMS		BRIDGE CRANES	BRAKE/ MOTOR SHAFT	SHAFT SHEAR		U	/YR	1.00e-04					
CRANE SYSTEMS		BRIDGE CRANES	BRAKE/ MOTOR SHAFT	SHAFT SHEAR		U	/DM	2.00e-07					

Table C-1. Crane Failure Rates (continued)

Equipment Type	Group	Description	Field 1	Field 2	Field 3	Ref	Unit	Failure Rate	High Value	Low Value	Remark	20% Lower	80% Upper
CRANE SYSTEMS		BRIDGE CRANES	BRAKE/ MOTOR SHAFT AND COUPLING	COUPLING CATASTROPHIC FAILURE, KEY SHEAR, BOLT SHEAR		U	/YR	4.00e-04					
CRANE SYSTEMS		BRIDGE CRANES	BRAKE/ MOTOR SHAFT AND COUPLING	COUPLING CATASTROPHIC FAILURE, KEY SHEAR, BOLT SHEAR		U	/DM	8.00e-07					
CRANE SYSTEMS		BRIDGE CRANES	MOTOR	FAILURE TO PRODUCE ADEQUATE TORQUE		U	/YR	3.00e-02					
CRANE SYSTEMS		BRIDGE CRANES	MOTOR	FAILURE TO PRODUCE ADEQUATE TORQUE		U	/DM	6.00e-05					
CRANE SYSTEMS		BRIDGE CRANES	CONTACTOR (L = Lower)	MECHANICAL JAMMING, CONTACTS WELD CLOSED		U	/YR	5.00e-03					
CRANE SYSTEMS		BRIDGE CRANES	CONTACTOR (L = Lower)	MECHANICAL JAMMING, CONTACTS WELD CLOSED		U	/DM	1.00e-05					
CRANE SYSTEMS		BRIDGE CRANES	CONTACTOR (MC= Main Contractor)	MECHANICAL JAMMING, CONTACTS WELD CLOSED		U	/YR	5.00e-03					

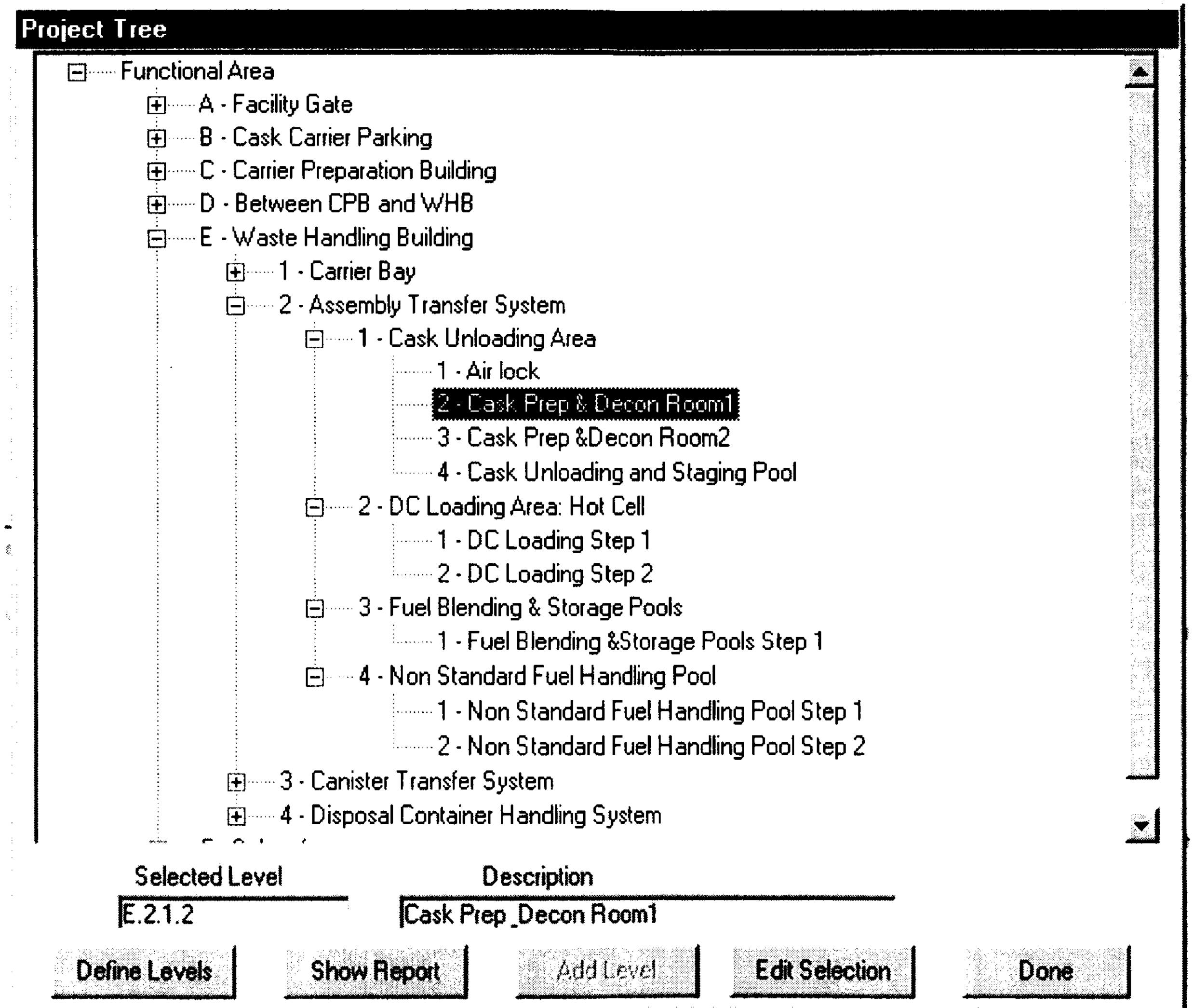
Table C-1. Crane Failure Rates (continued)

Equipment Type	Group	Description	Field 1	Field 2	Field 3	Ref	Unit	Failure Rate	High Value	Low Value	Remark	20% Lower	80% Upper
CRANE SYSTEMS		BRIDGE CRANES	CONTACTOR (MC= Main Contractor)	MECHANICAL JAMMING, CONTACTS WELD CLOSED		U	/DM	6.25e-04					
CRANE SYSTEMS		BRIDGE CRANES	EMERGENCY STOP (PB = Push Button)	DOES NOT ACTUATE MECHANICALLY, CONTACTS DO NOT OPEN		U	/YR	2.00e-03					
CRANE SYSTEMS		BRIDGE CRANES	EMERGENCY STOP (PB = Push Button)	DOES NOT ACTUATE MECHANICALLY, CONTACTS DO NOT OPEN		U	/DM	2.50e-04					
CRANE SYSTEMS		BRIDGE CRANES	DEAD MAN'S HANDLE	DOES NOT ACTUATE MECHANICALLY, CONTACTS DO NOT OPEN		U	/YR	2.00e-03					
CRANE SYSTEMS		BRIDGE CRANES	DEAD MAN'S HANDLE	DOES NOT ACTUATE MECHANICALLY, CONTACTS DO NOT OPEN		U	/DM	2.50e-04					
CRANE SYSTEMS		BRIDGE CRANES	CONTROLLER CONTACT 2	DOES NOT OPEN ON DEMAND		U	/YR	2.00e-03					
CRANE SYSTEMS		BRIDGE CRANES	CONTROLLER CONTACT 2	DOES NOT OPEN ON DEMAND		U	/DM	4.00e-06					
CRANE SYSTEMS		CRANES AND HOISTS	LOAD DROP FREQUENCIES		(1977 Navy Data)	KK	/DM	2.70e-05	3.06e-04	2.5e-05			

APPENDIX D

EXAMPLE ANALYSIS USING THE PCSA TOOL

PCSA Tool outputs such as dialogues boxes, forms, and reports are compiled in this Appendix. These outputs help illustrate the example analyses performed using the tool in Chapter 10 of the report.


Project Tree
Functional Area
A - Facility Gate
B - Cask Carrier Parking
C - Carrier Preparation Building
D - Between CPB and WHB
E - Waste Handling Building
1 - Carrier Bay
2 - Assembly Transfer System
1 - Cask Unloading Area
1 - Air lock
2 - Cask Prep & Decon Room1
3 - Cask Prep &Decon Room2
4 - Cask Unloading and Staging Pool
2 - DC Loading Area: Hot Cell
1 - DC Loading Step 1
2 - DC Loading Step 2
3 - Fuel Blending & Storage Pools
1 - Fuel Blending &Storage Pools Step 1
4 - Non Standard Fuel Handling Pool
1 - Non Standard Fuel Handling Pool Step 1
2 - Non Standard Fuel Handling Pool Step 2
3 - Canister Transfer System
4 - Disposal Container Handling System
Selected Level
E.2.1.2
Description
Cask Prep _Decon Room1
Define Levels
Show Report
Add Level
Edit Selection
Done

PCSA Project Tree Report

Project: YmpDr3New

Functional ID	1st Level	2nd Level	3rd Level	4th Level	Remarks
B.1.1	Transfer Carrier to On-Site Mover	Transporter	Between Site Gate and CPB		
C.1.1	Carrier Preparation Building	Carrier Prep. Material Handling System	Carrier Preparation		
E.2.1.1	Waste Handling Building	Assembly Transfer System	Cask Unloading Area	Air Lock	
E.2.1.2	Waste Handling Building	Assembly Transfer System	Cask Unloading Area	Cask Prep. & Decon Room 1	
E.2.1.3	Waste Handling Building	Assembly Transfer System	Cask Unloading Area	Cask Prep. & Decon Room 2	
E.2.1.4	Waste Handling Building	Assembly Transfer System	Cask Unloading Area	Cask Unloading & Staging Pool	
E.2.2.1	Waste Handling Building	Assembly Transfer System	DC Loading Area	DC Loading Step 1	
E.2.2.2	Waste Handling Building	Assembly Transfer System	DC Loading Area	DC Loading Step 2	
E.2.3.1	Waste Handling Building	Assembly Transfer System	Fuel Blending & Storage Pools	Fuel Blending & Storage Pools Step 1	
E.2.4.1	Waste Handling Building	Assembly Transfer System	Non Standard Fuel Handling Pool	Non Standard Fuel Handling Pool Step 1	
E.2.4.2	Waste Handling Building	Assembly Transfer System	Non Standard Fuel Handling Pool	Non Standard Fuel Handling Pool Step 2	
E.3.3.1	Waste Handling Building	Canister Transfer System	Canister Transfer System	Air Lock	
E.3.3.2	Waste Handling Building	Canister Transfer System	Canister Transfer System	Cask Prep. and Decontamination Area	
E.3.3.3	Waste Handling Building	Canister Transfer System	Canister Transfer System	Canister Transfer Cell	

System Description

Functional ID and Description

E.2.1.2	Waste Handling Building Assembly Transfer System Assembly Transfer System Cask Prep. & Decon Room 1

Functions:

Rail and truck transportation casks without impact limiters are received, sampled, cooled, and opened in the Cask Prep. & Decon Room 1. CSNF consisting of bare SNF assemblies, single element canisters, as well as DPC are unloaded from the transportation casks.

Detailed Operations Sequence:

13. For casks containing DPC:
- Attach remotely (per Ref 1, pg 25) DPC lifting fixture.

14. Move cask preparation manipulators and access platforms away from preparation pit. (Assume this is done manually ??)
15. Using bridge crane, lift yoke and bring to cask.
16. Using bridge crane, attach yoke to cask remotely. ?
17. Using bridge crane, lift cask and place in Cask Unloading Pool remotely

Equipment Used:

Bridge crane
Cask transfer carts (15 ft long, 11 ft wide, and 2 ft high)
Cask and DPC lifting yokes and fixtures

Source Terms:

Remarks:

Pit Dimensions: 13 ft dia., 13 ft to 15 ft depth ?

DOE References:

1. WHB/WTB Space Program Analysis for Site Recommendation. ANL-WHS-AR-000001 Rev 00. 5-22-00

Apply | Show Report | OK | Cancel

PCSA System Description Report

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Functions

Rail and truck transportation casks without impact limiters are received, sampled, cooled, and opened in the Cask Prep. & Decon Room 1. The transportation casks contain CSNF consisting of bare SNF assemblies, single element canisters, as well as DPCs.

Operations Sequence

1. Move cart with transport cask in Room 1 area, and secure.
2. Using bridge crane, lift yoke and bring to cask.
3. Hook cask lifting yoke onto cask
(No gantry mounted manipulator available to assist operations in this location. Assume this is done manually using the bridge crane ??)
4. Move cask preparation manipulators and access platforms away from preparation pit.
(Assume this is done manually ??)
5. Using bridge crane, lift cask off the cart, place, and secure in preparation pit.
6. Unhook cask yoke and store in preparation area.
7. Move access platforms and manipulator in place over cask
(Manipulator is called out as remote equipment (Ref. 1, pg 26))
8. For casks containing DPC:
- Perform remote (per Ref 1, pg 25) cask lid unbolting using manipulators and remote tools.
- Perform remote (per Ref 1, pg 25) cask lid removal, and lay-down using bridge crane ?
9. Perform remote (per Ref 1, pg 25) cask/DPC cavity sampling using manipulators and remote tools.
10. Perform remote (per Ref 1, pg 25) cask/DPC venting using manipulators and remote tools.
11. Perform remote (per Ref 1, pg 25) cask/DPC cool-down
12. For casks containing bare SNF assemblies:
- Perform remote (per Ref 1, pg 25) cask lid unbolting using manipulators and remote tools
- Perform remote (per Ref 1, pg 25) cask lid removal, and lay-down using bridge crane ?
- Perform remote (per Ref 1, pg 25) shield plug unbolting using manipulators and remote tools.
- Perform remote (per Ref 1, pg 25) shield plug lifting fixture attachment using manipulators and remote tools.
- Fill cask with water remotely
13. For casks containing DPC:
- Attach remotely (per Ref 1, pg 25) DPC lifting fixture.
14. Move cask preparation manipulators and access platforms away from preparation pit.
(Assume this is done manually ??)
15. Using bridge crane, lift yoke and bring to cask.
16. Using bridge crane, attach yoke to cask remotely. ?
17. Using bridge crane, lift cask and place in Cask Unloading Pool remotely
(It is assumed that this is done by lifting the cask over the two 24 ft high partition walls in the Cask Prep & Unloading Area - Fig I-17)

Equipment

Bridge crane
Cask transfer carts (15 ft long, 11 ft wide, and 2 ft high)
Cask and DPC lifting yokes and fixtures
Access platforms (in the pit area)
Cask preparation manipulator (remotely operated gantry-mounted) which straddles the pit and access platforms

Source Terms

Remarks

Pit Dimensions: 13 ft dia., 13 ft to 15 ft depth ?

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

DOE References	1. WHB/WTB Space Program Analysis for Site Recommendation. ANL-WHS-AR-000001 Rev 00.	5-22-00

FMEA Form, Project: YmpDr3New

Functional ID
E.2.1.2

Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No. 0025.00

Component Description Cask lifting yoke & fixtures

Failure Mode
Yoke Fails

Cause of Failure
Structural Failure.
Human Error (Yoke improperly attac

Effect of Failure
Drop of Cask /DPC

Recommended Safeguard and Controls
Administrative Control.
Proper Attachment Design.

DOE Failure Detection

Severe Events YES

Remarks
OSS 16.
Since cask has to clear the partition walls between Cask Prep.
& Decon Room 1 and the cask unloading pool, drop height for

Add Record | Delete Record | Cancel | Record: 33 | Show Report | FMEA Table | Close

PCSA FMEA Report

Project: YmpDr3New

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Functional ID: E.2.1.2

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
0001.00	Transportation Cask Transfer Cart	No Braking, Excessive Movement	Brake Failure. Operator Error.	Collision with Cask Unloading Area Partition Doors, Wall. Possible Tip-over of Cask.	Administrative Control. Design of Over-travel Limit Switch		NO	Operations Sequence Step (OSS) 1
0001.01	Bridge Crane	Loss of Control. (Lifting Yoke Crashes into Access Platforms, Gantry, Manipulator, or Cask mounted on Cart)	Failure of Controls Operator Error	Possible Tip-over of Cask Damage to Access Platforms, Gantry, Manipulator, or Remote Tools and Fixtures	Administrative Control Operator Training Use of NOG 1 Single Failure Proof Crane	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	NO	OSS 2. Cask tip-over height from cart is expected to be low
0001.02	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke	No Power	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	Fail-Safe Design of Crane Use of NOG 1 Single Failure Proof Crane	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 2. Drop height for yoke may be greater than ~30 ft
0001.03	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure.	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 2. Drop height for yoke may be greater than ~30 ft
0001.04	Bridge Crane	Crane Failure. (2 Block Failure involving Lifting Yoke)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides	Administrative Control. (Operator Training, Proper Maintenance of 2 block control	Use of crane with two of every active component necessary to support load, prevent a spurious	YES	OSS 2. Drop height for yoke may be greater than ~30 ft

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
				into cask unloading area.	mechanism) Use of NOG 1 Single Failure Proof Crane.	movement, or detect an operator error that could result in physical impact to vulnerable SNF.		
0002.00	Cask Lifting Yoke & Fixtures	Yoke Fails	Structural Failure. Human Error (Yoke improperly attached)	Drop of Cask /DPC	Administrative Control. Proper Attachment Design.		NO	OSS 3. Lift Height is expected to be low (~2 to 4 ft)
0003.00	Bridge Crane	Crane Failure (Normal Height Drop of Cask	No Power	Possible drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area.	Fail-Safe Design of Crane. Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 5. If Cask or DPC drops into the pit (~15 ft drop), the drop height will exceed the maximum drop height of cask without impact limiters. In all other cases the lift height is expected to be low (~2 to 4 ft)
0004.00	Bridge Crane	Crane Failure (Normal Height Drop of Cask	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area.	Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 5. If Cask or DPC drops into the pit (~15 ft drop), the drop height will exceed the maximum drop height of cask without impact limiters. In all other cases the lift height is expected to be low (~2 to 4 ft)
0005.00	Bridge Crane	Crane Failure. (2 Block Failure involving Cask)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area.	Administrative Control. (Operator Training, Proper Maintenance of 2 block control mechanism) Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 5. Drop from a height exceeding the maximum drop height of cask without impact limiters
0006.00	Bridge Crane	Loss of Control. (Cask Crashes into	Failure of Controls. Operator Error.	Possible Drop of Cask. Damage to Access	Administrative Control.	Use of crane with two of every active	NO	OSS 5. Cask lift height is

D-9

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
		Access Platforms, Gantry, or Manipulator)		Platforms, Gantry, Manipulator, or Remote Tools and Fixtures.	Operator Training. Use of NOG 1 Single Failure Proof Crane.	component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.		expected to be low (~2 to 4 ft)
0007.00	Cask and DPC Lifting Yoke & Fixtures	Yoke Fails to Detach from Cask	Operator Error (Yoke improperly connected)	Possible drop and rupture of Cask or DPC Release of radionuclides into cask unloading area	Administrative Control Proper Attachment Design Operator Training		YES	OSS 6. The drop height into the pit (~15 ft), can exceed the maximum drop height of cask without impact limiters.
0008.00	Cask and DPC Lifting Yoke & Fixtures	Yoke Fails to Detach from Crane Hook	Operator Error (Yoke improperly connected)	Yoke drop on floor cavity for storing yoke	Administrative Control Operator Training Proper Attachment Design		NO	OSS 6.
0009.00	Access Platforms, Gantry, or Manipulator	Loss of Control. (Access Platforms, Gantry, or Manipulator Crashes into Cask in Prep. Pit)	Failure of Controls Operator Error	Damage to Access Platforms, Gantry, or Manipulator	Administrative Control Operator Training		NO	OSS 7.
0009.01	Remote cask lid unbolting system	Improper unbolting of cask lid	Mechanical Malfunction of system. Human Error.	Possible lifting and tip-over of cask with DPC during lid removal operations. Possible release of radionuclides into cask unloading area.			YES	OSS 8. Need more information on this system.
0009.02	Bridge Crane	Crane Failure. (Normal Height Drop of Cask Lid)	No Power.	Possible Lid drop on cask containing DPC. Possible rupture of cask and DPC. Release of radionuclides into cask unloading area.	Fail-Safe Design of Crane. Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	NO	OSS 8. Even though the drop height for lid may be greater than ~ 50 ft., the DPC is shielded to some extent by the surrounding cask.
0009.03	Bridge Crane	Crane Failure. (Normal Height Drop of	1. Cable Failure. 2. Motor Failure.	Possible Lid drop on cask containing DPC.	Fail-Safe Design of Crane.	Use of crane with two of every active	NO	OSS 8. Even though the drop

D-10

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
		Lid)	3. Brake Failure. 4. Other Mechanical Failure.	Possible rupture of cask and DPC. Release of radionuclides into cask unloading area.	Use of NOG 1 Single Failure Proof Crane.	component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.		height for lid may be greater than ~ 50 ft., the DPC is shielded to some extent by the surrounding cask.
0009.04	Bridge Crane	Crane Failure. (2 Block Failure involving Lid)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control).	Possible Lid drop on cask containing DPC. Possible rupture of cask and DPC. Release of radionuclides into cask unloading area.	Fail-Safe Design of Crane. Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	NO	OSS 8. Even though the drop height for lid may be greater than ~ 50 ft., the DPC is shielded to some extent by the surrounding cask.
0010.00	Cask/DPC Cavity Sampler	Fails to give proper reading.	Human Error. Out of Calibration. Mechanical Failure.	Cask/DPC misdiagnosed as not containing radioactive gases from broken fuel rods. ?? Radioactive gases may be released in cell during subsequent venting and lid unbolting operations.	Administrative Control. Operator Training. Proper Calibration.		YES	OSS 9. Need more information on this system.
0011.00	Remote Cask/DPC Venting System	Fails to vent cask/DPC	Mechanical Malfunction of system. Human Error.	Cask/DPC remains Pressurized ???	Administrative Control. Operator Training. Proper Maintenance of system.		YES	OSS 10. Possible venting of pressure during remote lid unbolting operations. Need more information on this system.
0012.00	Cask/DPC Cool-down System						YES	OSS 11. Need more information on this system.
0013.00	Remote cask lid unbolting system	Improper unbolting of cask lid	Mechanical Malfunction of system. Human Error.	Possible lifting and tip-over of cask during lid removal operations. Release of radionuclides into cask unloading area			YES	OSS 12. Need more information on this system.

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
				or pool.				
0014.00	Bridge Crane	Crane Failure. (Normal Height Drop of Cask Lid)	No Power.	Possible Lid drop on cask. Possible rupture of cask. Release of radionuclides into cask unloading area.	Fail-Safe Design of Crane. Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 12. Drop height for lid may be greater than ~ 50 ft.
0015.00	Bridge Crane	Crane Failure. (Normal Height Drop of Lid)	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure.	Possible Lid drop on cask. Possible rupture of cask. Release of radionuclides into cask unloading area.	Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 12. Drop height for lid may be greater than ~ 50 ft.
0016.00	Bridge Crane	Crane Failure. (2 Block Failure involving Lid)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control).	Possible Lid drop on cask. Possible rupture of cask. Release of radionuclides into cask unloading area.	Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 12. Drop height for lid may be greater than ~ 50 ft.
0017.00	Remote cask shield plug unbolting system	Improper unbolting of cask shield plug	Mechanical Malfunction of system. Human Error.	Possible lifting and tip-over of cask during shield plug removal operations in unloading pool. Release of radionuclides into cask unloading pool.			YES	OSS 12. Need more information on this system.
0018.00	Cask shield plug lifting fixture	Cask shield plug lifting fixture fails.	Structural Failure. Human Error (Fixture improperly attached)	Drop of shield plug in unloading pool. Possible damage of SNF assemblies in unloading pool	Administrative Control Proper Attachment Design		YES	OSS 12. May require cask to be lifted out of unloading pool and returned to prep. and

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
								unloading area so that the lifting fixture can be reattached to shield plug.
0019.00	Fill cask with water ???	Cask overfilled with water	Mechanical Malfunction of system. Human Error.	Cask overflow water spilled in cask unloading area. Release of radionuclides into cask unloading area.			YES	OSS 12. Need more information on this system.
0020.00	DPC lifting fixture	DPC lifting fixture fails	Structural Failure. Human Error (Fixture improperly attached)	Drop of DPC in unloading pool. Possible damage of SNF assemblies in unloading pool	Administrative Control Proper Attachment Design		YES	OSS 13. May require cask to be lifted out of unloading pool and returned to Cask Prep. & Decon Room 1 so that the lifting fixture can be reattached to shield plug. Lift height needed to clear the partition walls will exceed maximum drop height for cask without impact limiters. Need more information on this system.
0021.00	Bridge Crane	Loss of Control. (Lifting Yoke Crashes into Access Platforms, Gantry, Manipulator, or Cask in pit)					NO	OSS 15. Even though cask lid is removed, cask is unlikely to tip-over as it is in the pit.
0022.00	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke)	No Powe	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.			YES	OSS 15. Drop height for yoke may be greater than ~30 ft. Cask is without lid
0023.00	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke)	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure.	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides			YES	OSS 15. Drop height for yoke may be greater than ~30 ft. Cask is without lid

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
				into cask unloading area.				
0024.00	Bridge Crane	Crane Failure. (2 Block Failure involving Lifting Yoke)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 15. Drop height for yoke may be greater than ~30 ft. Cask is without lid
0025.00	Cask lifting yoke & fixtures	Yoke Fails	Structural Failure. Human Error (Yoke improperly attac	Drop of Cask /DPC	Administrative Control. Proper Attachment Design.		YES	OSS 16. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this system.
0026.00	Bridge Crane	Crane Failure. (Normal Height Drop of Cask)	No Power	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool.	Fail-Safe Design of Crane. Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
0027.00	Bridge Crane	Crane Failure. (Normal Height Drop of Cask)	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool.	Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.
0028.00	Bridge Crane	Crane Failure. (2 Block Failure involving Cask)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool.	Administrative Control. (Operator Training, Proper Maintenance of 2 block control mechanism) Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.
0029.00	Bridge Crane	Loss of Control. (Cask Crashes into Prep. Area Partition Walls Access Platforms, Gantry, or Manipulator)	Failure of Controls. Operator Error.	Possible Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool. Damage to Partition Wall, Access Platforms, Gantry, Manipulator, or Remote Tools and Fixtures.	Administrative Control. Operator Training. Use of NOG 1 Single Failure Proof Crane.	Use of crane with two of every active component necessary to support load, prevent a spurious movement, or detect an operator error that could result in physical impact to vulnerable SNF.	YES	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Safeguard	DOE Failure Detection	Severe Events	Remarks
								maximum drop height for cask without impacters. Need more information on this operation.

D-16

PCSA Event Analysis Report

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Remarks
0001.02	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke	No Power	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	OSS 2. Drop height for yoke may be greater than ~30 ft
0001.03	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure.	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	OSS 2. Drop height for yoke may be greater than ~30 ft
0001.04	Bridge Crane	Crane Failure. (2 Block Failure involving Lifting Yoke)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	OSS 2. Drop height for yoke may be greater than ~30 ft
0003.00	Bridge Crane	Crane Failure (Normal Height Drop of Cask	No Power	Possible drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area.	OSS 5. If Cask or DPC drops into the pit (~15 ft drop), the drop height will exceed the maximum drop height of cask without impact limiters. In all other cases the lift height is expected to be low (~2 to 4 ft)
0004.00	Bridge Crane	Crane Failure (Normal Height Drop of Cask	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area.	OSS 5. If Cask or DPC drops into the pit (~15 ft drop), the drop height will exceed the maximum drop height of cask without impact limiters. In all other cases the lift height is expected to be low (~2 to 4 ft)
0005.00	Bridge Crane	Crane Failure. (2 Block Failure involving Cask)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area.	OSS 5. Drop from a height exceeding the maximum drop height of cask without impact limiters
0007.00	Cask and DPC Lifting Yoke & Fixtures	Yoke Fails to Detach from Cask	Operator Error (Yoke improperly connected)	Possible drop and rupture of Cask or DPC Release of radionuclides into cask unloading area	OSS 6. The drop height into the pit (~15 ft), can exceed the maximum drop height of cask without impact limiters.
0009.01	Remote cask lid unbolting system	Improper unbolting of cask lid	Mechanical Malfunction of system. Human Error.	Possible lifting and tip-over of cask with DPC during lid removal	OSS 8. Need more information on this

D-17

Project: YmpDr3New

Functional ID: E.2.1.2 **Description:** Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Remarks
				operations. Possible release of radionuclides into cask unloading area.	system.
0010.00	Cask/DPC Cavity Sampler	Fails to give proper reading.	Human Error. Out of Calibration. Mechanical Failure.	Cask/DPC misdiagnosed as not containing radioactive gases from broken fuel rods. ?? Radioactive gases may be released in cell during subsequent venting and lid unbolting operations.	OSS 9. Need more information on this system.
0011.00	Remote Cask/DPC Venting System	Fails to vent cask/DPC	Mechanical Malfunction of system. Human Error.	Cask/DPC remains Pressurized ???	OSS 10. Possible venting of pressure during remote lid unbolting operations. Need more information on this system.
0012.00	Cask/DPC Cool-down System				OSS 11. Need more information on this system.
0013.00	Remote cask lid unbolting system	Improper unbolting of cask lid	Mechanical Malfunction of system. Human Error.	Possible lifting and tip-over of cask during lid removal operations. Release of radionuclides into cask unloading area or pool.	OSS 12. Need more information on this system.
0014.00	Bridge Crane	Crane Failure. (Normal Height Drop of Cask Lid)	No Power.	Possible Lid drop on cask. Possible rupture of cask. Release of radionuclides into cask unloading area.	OSS 12. Drop height for lid may be greater than ~ 50 ft.
0015.00	Bridge Crane	Crane Failure. (Normal Height Drop of Lid)	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure.	Possible Lid drop on cask. Possible rupture of cask. Release of radionuclides into cask unloading area.	OSS 12. Drop height for lid may be greater than ~ 50 ft.
0016.00	Bridge Crane	Crane Failure. (2 Block Failure involving Lid)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control).	Possible Lid drop on cask. Possible rupture of cask. Release of radionuclides into cask unloading area.	OSS 12. Drop height for lid may be greater than ~ 50 ft.
0017.00	Remote cask shield plug unbolting system	Improper unbolting of cask shield plug	Mechanical Malfunction of system. Human Error.	Possible lifting and tip-over of cask during shield plug removal operations in unloading pool. Release of radionuclides into cask unloading pool.	OSS 12. Need more information on this system.

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Remarks
0018.00	Cask shield plug lifting fixture	Cask shield plug lifting fixture fails.	Structural Failure. Human Error (Fixture improperly attached)	Drop of shield plug in unloading pool. Possible damage of SNF assemblies in unloading pool	OSS 12. May require cask to be lifted out of unloading pool and returned to prep. and unloading area so that the lifting fixture can be reattached to shield plug.
0019.00	Fill cask with water ???	Cask overfilled with water	Mechanical Malfunction of system. Human Error.	Cask overflow water spilled in cask unloading area. Release of radionuclides into cask unloading area.	OSS 12. Need more information on this system.
0020.00	DPC lifting fixture	DPC lifting fixture fails	Structural Failure. Human Error (Fixture improperly attached)	Drop of DPC in unloading pool. Possible damage of SNF assemblies in unloading pool	OSS 13. May require cask to be lifted out of unloading pool and returned to Cask Prep. & Decon Room 1 so that the lifting fixture can be reattached to shield plug. Lift height needed to clear the partition walls will exceed maximum drop height for cask without impact limiters. Need more information on this system.
0022.00	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke)	No Powe	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	OSS 15. Drop height for yoke may be greater than ~30 ft. Cask is without lid
0023.00	Bridge Crane	Crane Failure. (Normal Height Drop of Lifting Yoke)	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure.	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	OSS 15. Drop height for yoke may be greater than ~30 ft. Cask is without lid
0024.00	Bridge Crane	Crane Failure. (2 Block Failure involving Lifting Yoke)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Possible Yoke drop on cask. Possible rupture of cask or DPC. Release of radionuclides into cask unloading area.	OSS 15. Drop height for yoke may be greater than ~30 ft. Cask is without lid
0025.00	Cask lifting yoke & fixtures	Yoke Fails	Structural Failure. Human Error (Yoke improperly attac	Drop of Cask /DPC	OSS 16. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this system.

Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

Item No	Component Description	Failure Mode	Cause of Failure	Effect of Failure	Remarks
0026.00	Bridge Crane	Crane Failure. (Normal Height Drop of Cask)	No Power	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool.	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.
0027.00	Bridge Crane	Crane Failure. (Normal Height Drop of Cask)	1. Cable Failure. 2. Motor Failure. 3. Brake Failure. 4. Other Mechanical Failure	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool.	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.
0028.00	Bridge Crane	Crane Failure. (2 Block Failure involving Cask)	Failure of Controls + Human Error. (Operator error + Failure of 2 block control)	Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool.	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.
0029.00	Bridge Crane	Loss of Control. (Cask Crashes into Prep. Area Partition Walls Access Platforms, Gantry, or Manipulator)	Failure of Controls. Operator Error.	Possible Drop and rupture of Cask or DPC. Release of radionuclides into cask unloading area or pool. Damage to Partition Wall, Access Platforms, Gantry, Manipulator, or Remote Tools and Fixtures.	OSS 17. Since cask has to clear the partition walls between Cask Prep. & Decon Room 1 and the cask unloading pool, drop height for cask/DPC will exceed ~25 ft. Cask is without lid, and the drop height exceeds the maximum drop height for cask without impacters. Need more information on this operation.

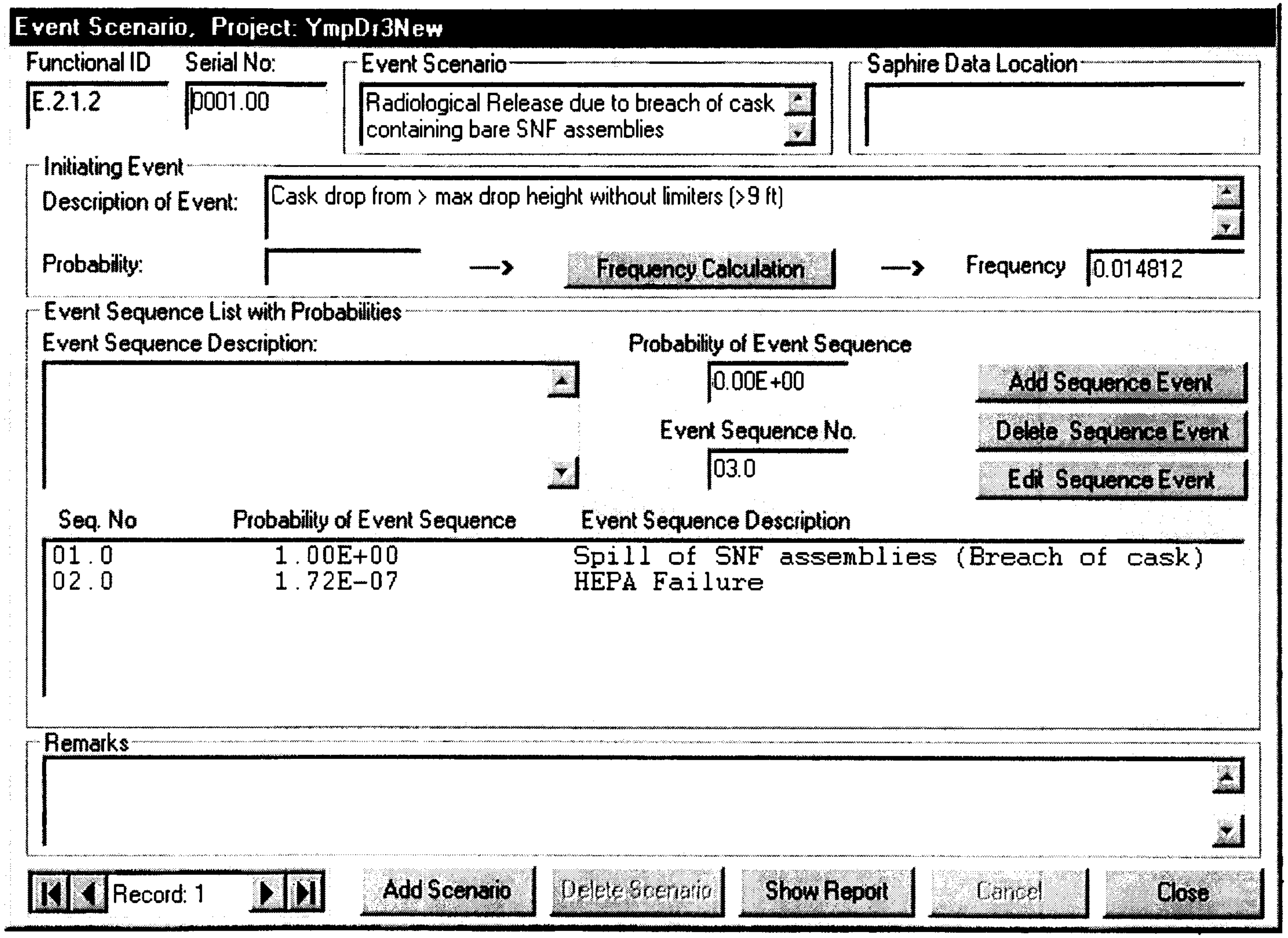
Component Failure Mode Checklist

Component: Crane

Search

Close

Component	Failure Mode
Cranes	Component Failure -Hook -Rope System -Rope drum -Drum bearing and pedestal -Drum/gearbox shaft and coupling -Gearbox -Gearbox/brake shaft and coupling -Brake (thruster type) -Brake/motor shaft and coupling -Motor -Contactor L -Contactor MC -Emergency stop PB -Dead man's handle -Controller Contact 2


Event Scenario, Project: YmpDr3New
Functional ID
E.2.1.2
Serial No:
0001.00
Event Scenario
Radiological Release due to breach of cask containing bare SNF assemblies
Saphire Data Location
Initiating Event
Description of Event:
Cask drop from > max drop height without limiters (>9 ft)
Probability:
Frequency Calculation
Frequency
0.014812
Event Sequence List with Probabilities
Event Sequence Description:
Probability of Event Sequence
0.00E+00
Add Sequence Event
Event Sequence No.
03.0
Delete Sequence Event
Edit Sequence Event
Seq. No
Probability of Event Sequence
Event Sequence Description
01.0
1.00E+00
Spill of SNF assemblies (Breach of cask)
02.0
1.72E-07
HEPA Failure
Remarks
Record: 1
Add Scenario
Delete Scenario
Show Report
Cancel
Close

PCSA Event Scenario Report

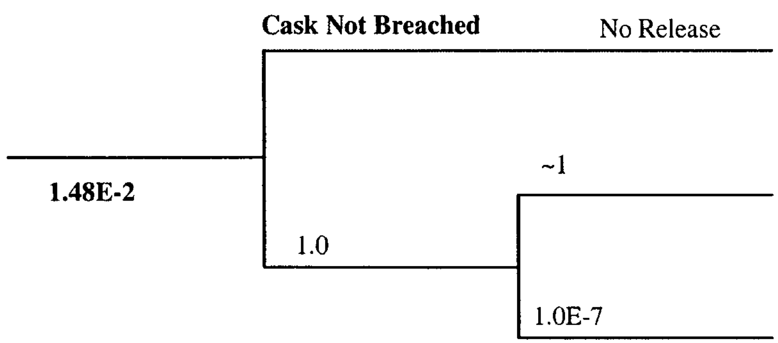
Project: YmpDr3New

Functional ID: E.2.1.2

Description: Waste Handling Building
Assembly Transfer System
Cask Unloading Area
Cask Prep. & Decon Room 1

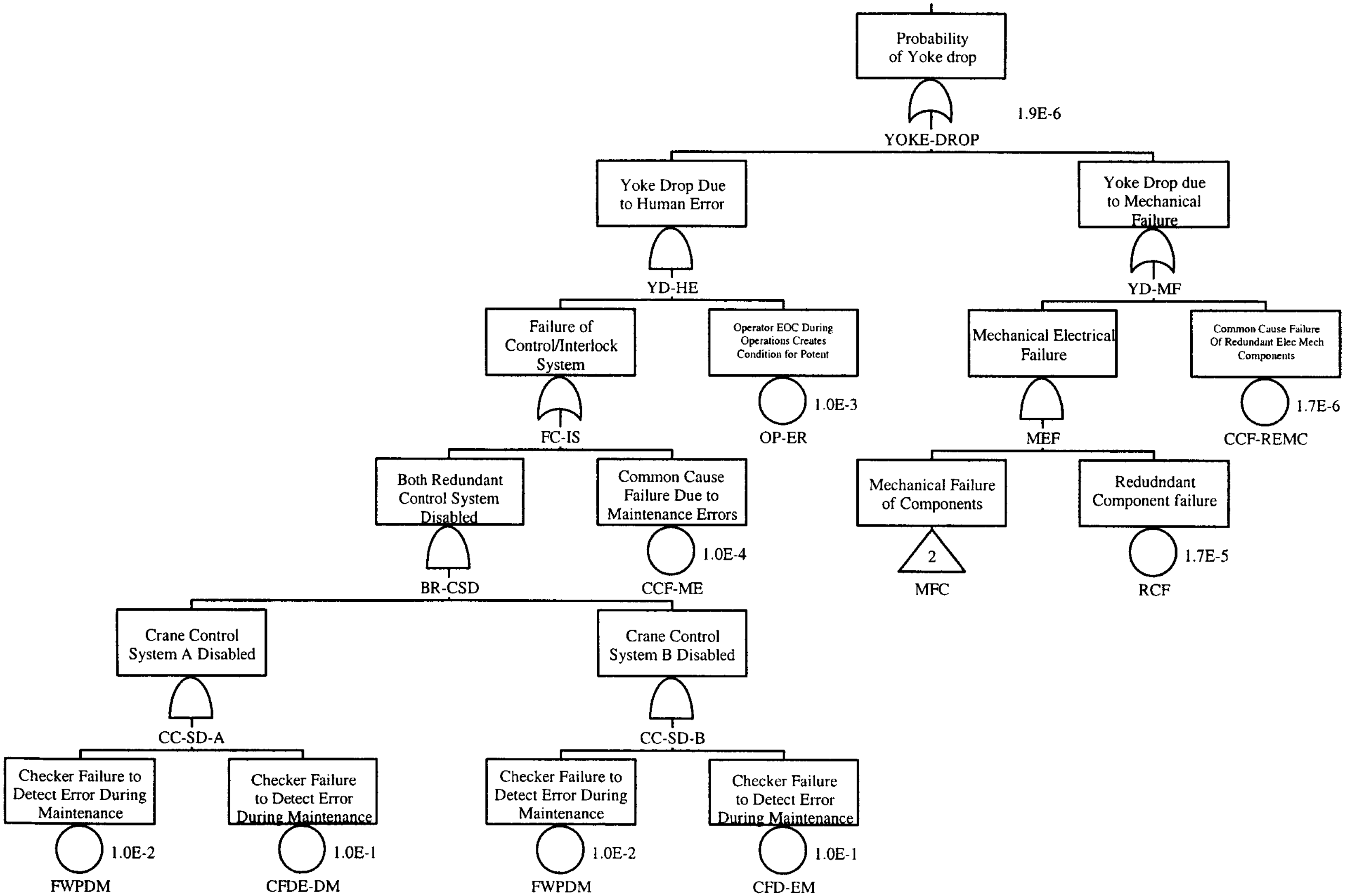
Serial No	Event Scenario	Initiating Event	Initiating Event Frequency	Event Seq. No.	Event Sequence	Probability of Event Sequence
0001.00	Radiological Release due to breach of cask containing bare SNF assemblies	Cask drop from > max drop height without limiters (>9 ft)	0.014812	**01.0**	Spill of SNF assemblies (Breach of cask)	1.00E+00
				02.0	HEPA Failure	1.72E-07

Cask Drop Initiating Event	Cask Breach	HEPA Filtration				
CD1_ATS	CB1_ATS	HEPA	#	EVN-SEQ-ID	END-STATE	FREQUENCY

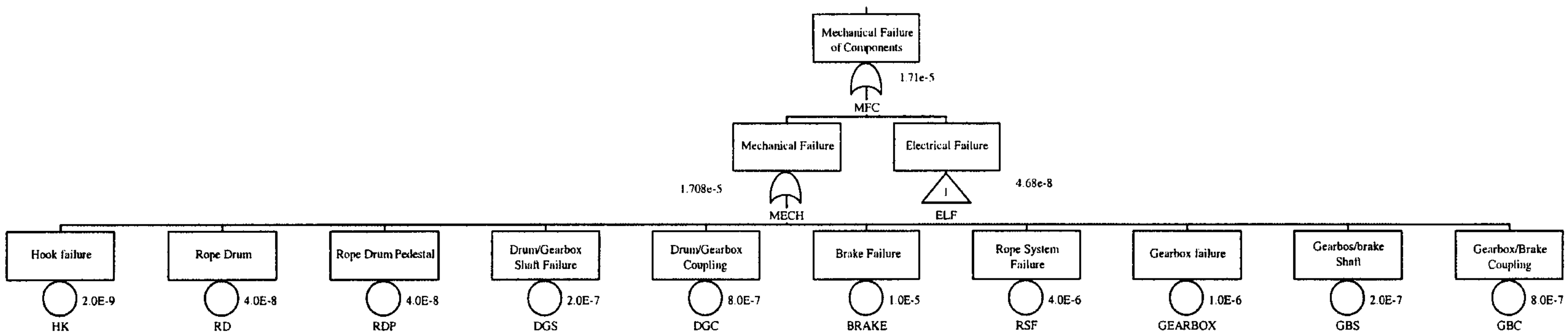


#	EVN-SEQ-ID	END-STATE	FREQUENCY
1	ATS-CD1	OK	
2	ATS-CD-2	SMALL-RELEASE	1.480E-002
3	ATS-CD-3	LARGE-RELEASE	1.480E-009

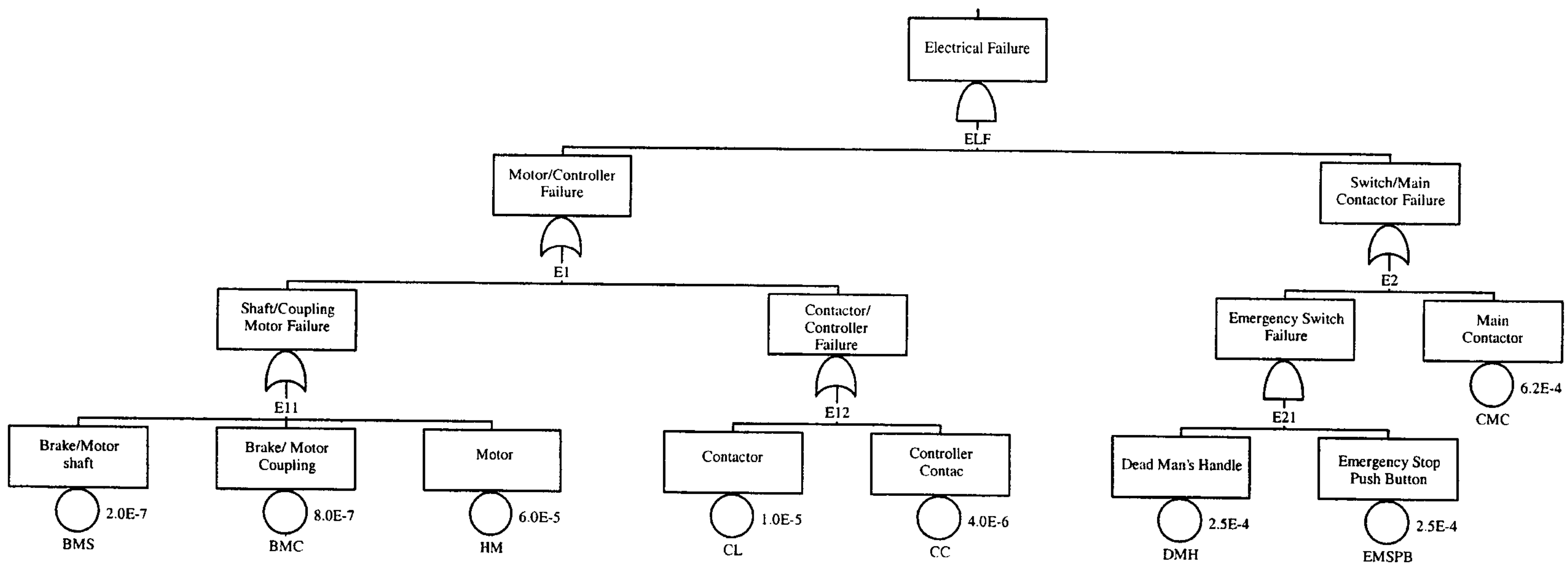
CASK-DROP-ATS-1 - 2001/08/09 Page 1

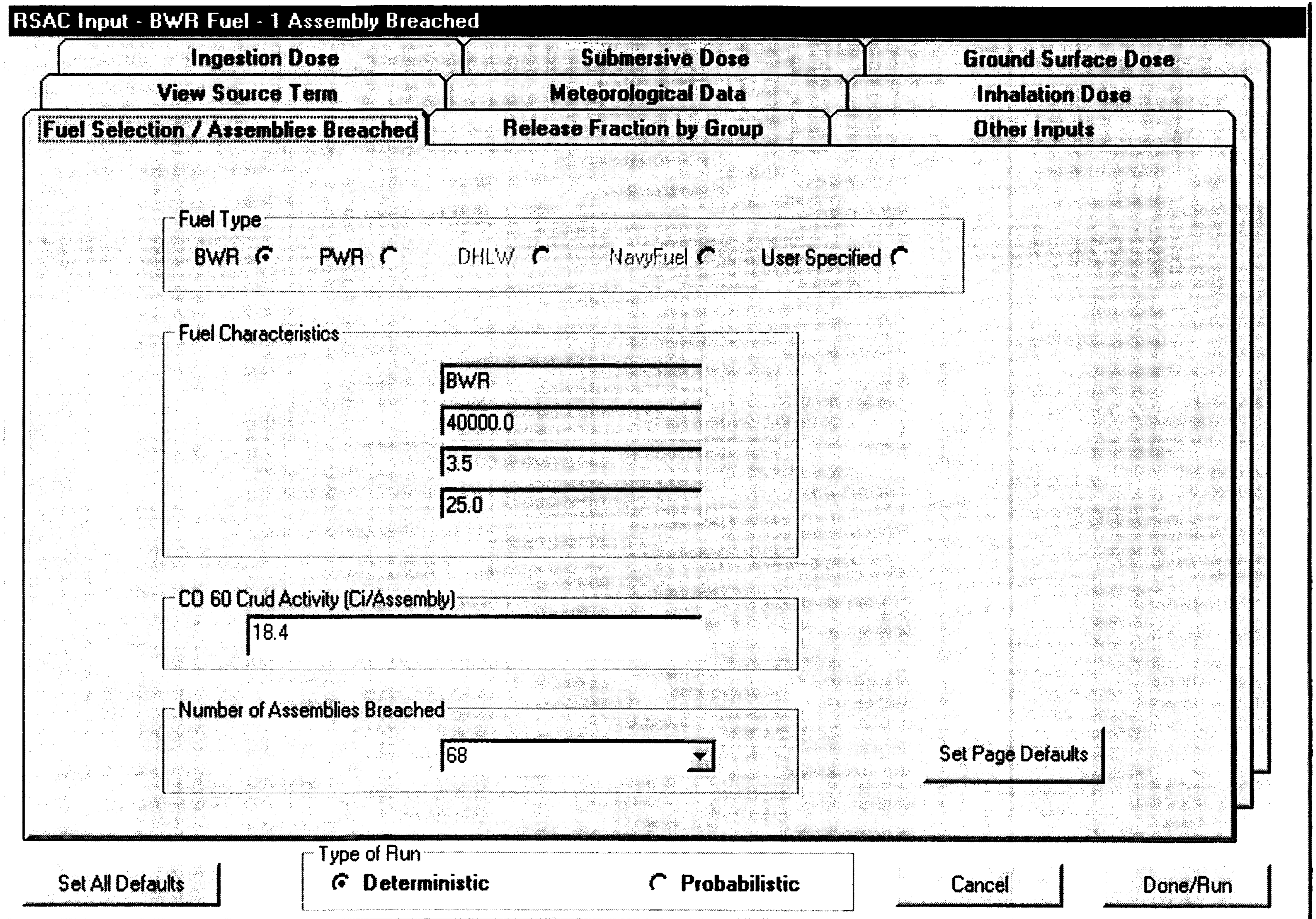


YOKE-DROP - Probability of Yoke drop 2001/07/21 Page 3



Mechanical Failure of Components
1.71e-5
MFC
Mechanical Failure
1.708e-5
MECH
Electrical Failure
1
4.68e-8
ELF
Hook failure
2.0E-9
HK
Rope Drum
4.0E-8
RD
Rope Drum Pedestal
4.0E-8
RDP
Drum/Gearbox Shaft Failure
2.0E-7
DGS
Drum/Gearbox Coupling
8.0E-7
DGC
Brake Failure
1.0E-5
BRAKE
Rope System Failure
4.0E-6
RSF
Gearbox failure
1.0E-6
GEARBOX
Gearbos/brake Shaft
2.0E-7
GBS
Gearbox/Brake Coupling
8.0E-7
GBC


Electrical Failure
ELF
Motor/Controller Failure
E1
Switch/Main Contactor Failure
E2
Shaft/Coupling Motor Failure
E11
Contactor/ Controller Failure
E12
Emergency Switch Failure
E21
Main Contactor
6.2E-4
CMC
Brake/Motor shaft
2.0E-7
BMS
Brake/ Motor Coupling
8.0E-7
BMC
Motor
6.0E-5
HM
Contactor
1.0E-5
CL
Controller Contac
4.0E-6
CC
Dead Man's Handle
2.5E-4
DMH
Emergency Stop Push Button
2.5E-4
EMSPB


RSAC Input - BWR Fuel - 1 Assembly Breached
Ingestion Dose
Submersive Dose
Ground Surface Dose
View Source Term
Meteorological Data
Inhalation Dose
Fuel Selection / Assemblies Breached
Release Fraction by Group
Other Inputs
Fuel Type
BWR
PWR
DHLW
NavyFuel
User Specified
Fuel Characteristics
BWR
40000.0
3.5
25.0
CO 60 Crud Activity (Ci/Assembly)
18.4
Number of Assemblies Breached
68
Set Page Defaults
Set All Defaults
Type of Run
Deterministic
Probabilistic
Cancel
Done/Run

RSAC Input - BWR Fuel - 1 Assembly Breached

Ingestion Dose | Submersion Dose | Ground Surface Dose

View Source Term | Meteorological Data | Inhalation Dose

Fuel Selection / Assemblies Breached | **Release Fraction by Group** | Hepa, Bldg. Discharge, _Others

KeyNumber	Group ID	Group Name	Release Fraction	Radionuclides In Group	Default Value
1	Group 1	H 3	3.00e-01	H 3	3.00e-01
2	Group 2	Ruthenium	1.50e-05	RU106	1.50e-05
3	Group 3	Iodine	1.00e-01	I129	1.00e-01
4	Group 4	Cesium + Strontium	2.30e-05	CS134, CS135, CS137, SR 90	2.30e-05
5	Group 5	noble gases	4.00e-01	AR 39, KR 85, RN219, RN220, RN222	4.00e-01
6	Group 8	CO 60 Crud	1.50e-01	CO 60 Crud	1.50e-01
7	Group 9	other particulates and fuel fines	2.00e-06	All others	2.00e-06

Release in

(•) Air ( ) Pool

Set Page Defaults

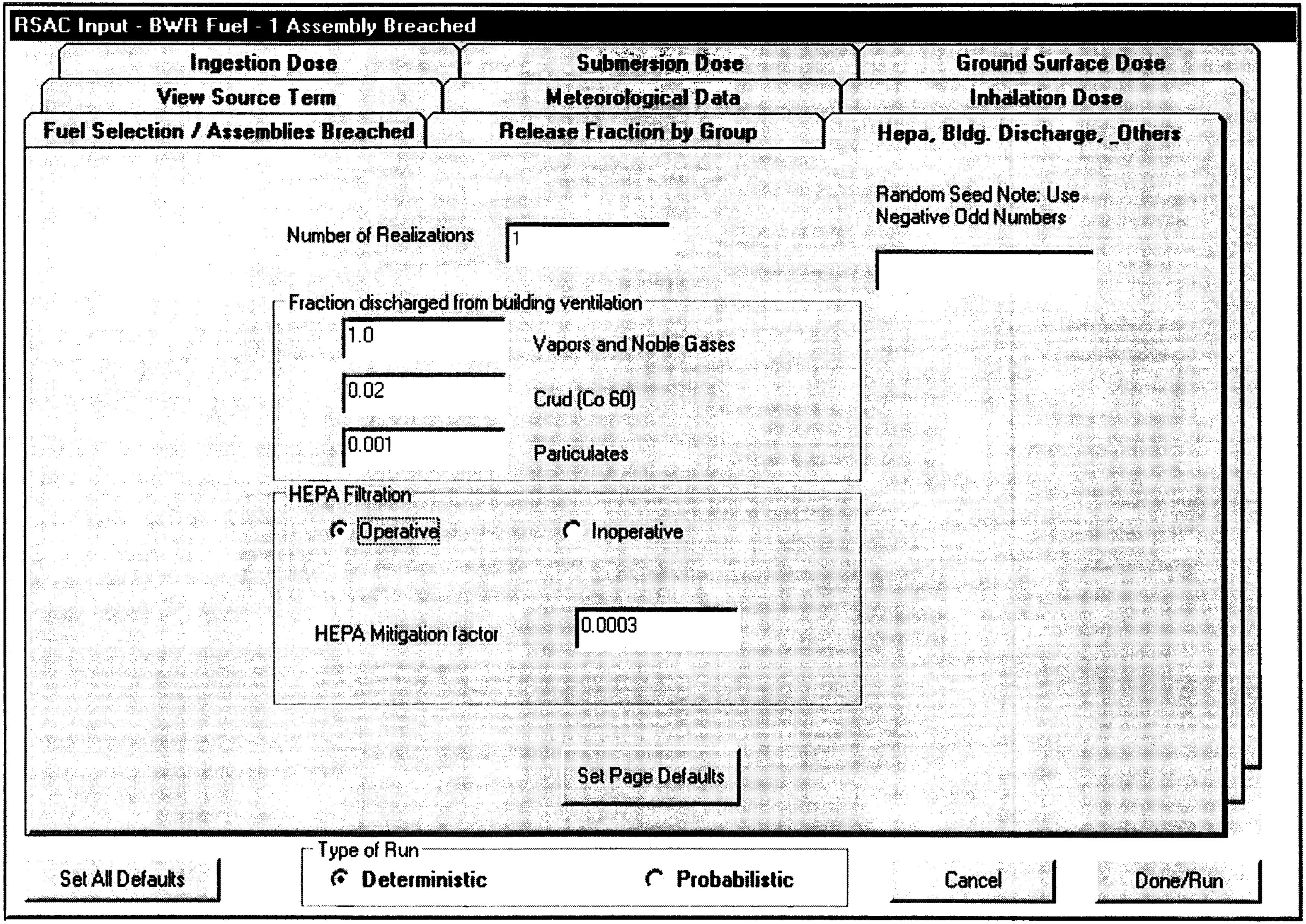
Set All Defaults

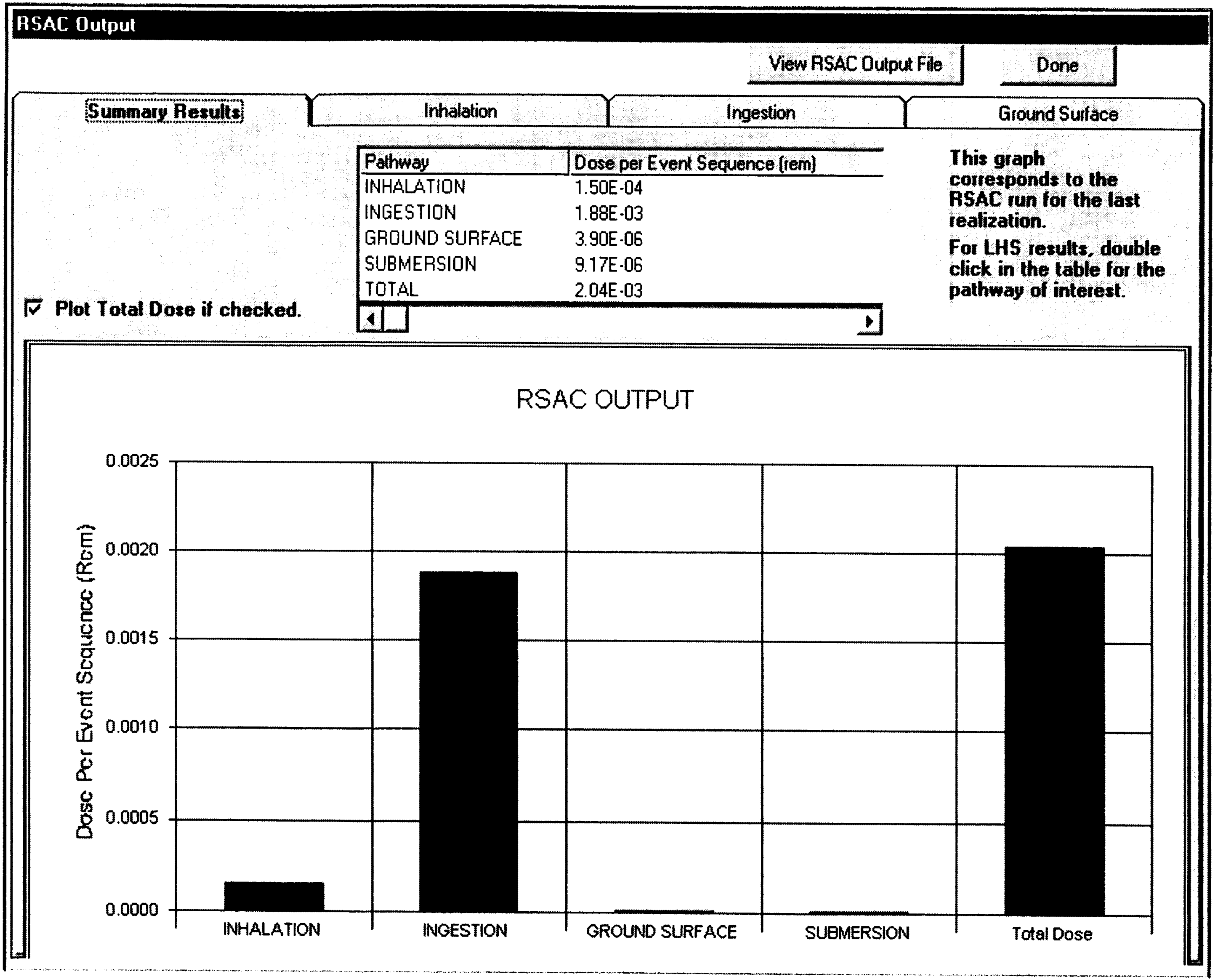
Type of Run

(•) Deterministic ( ) Probabilistic

Cancel

Done/Run


RSAC Input - BWR Fuel - 1 Assembly Breached
Ingestion Dose
Submersion Dose
Ground Surface Dose
View Source Term
Meteorological Data
Inhalation Dose
Fuel Selection / Assemblies Breached
Release Fraction by Group
Hepa, Bldg. Discharge, _Others
Random Seed Note: Use Negative Odd Numbers
Number of Realizations
1
Fraction discharged from building ventilation
1.0
Vapors and Noble Gases
0.02
Crud (Co 60)
0.001
Particulates
HEPA Filtration
Operative
Inoperative
HEPA Mitigation factor
0.0003
Set Page Defaults
Set All Defaults
Type of Run
Deterministic
Probabilistic
Cancel
Done/Run


RSAC Output
View RSAC Output File
Done
Summary Results
Inhalation
Ingestion
Ground Surface
Pathway
Dose per Event Sequence (rem)
INHALATION 1.50E-04
INGESTION 1.88E-03
GROUND SURFACE 3.90E-06
SUBMERSION 9.17E-06
TOTAL 2.04E-03
This graph corresponds to the RSAC run for the last realization.
For LHS results, double click in the table for the pathway of interest.
Plot Total Dose if checked.
RSAC OUTPUT
Dose Per Event Sequence (Rem)
0.0025
0.0020
0.0015
0.0010
0.0005
0.0000
INHALATION
INGESTION
GROUND SURFACE
SUBMERSION
Total Dose

RSAC Output

View RSAC Output File

Done

Summary Results | Inhalation | Ingestion | Ground Surface

For LHS results, double click in the table for the organ of interest.

Organs	Dose per Event Sequence (rem)
LUNGS	1.96E-06
S WALL	1.01E-15
SI WALL	6.95E-10
ULI WALL	6.99E-10
LLI WALL	7.56E-10
GONADS	1.38E-08
BREASTS	5.93E-10
BONE SUR	2.53E-06
R MARROW	2.20E-07
THYROID	4.94E-04
KIDNEYS	2.87E-13
LIVER	4.53E-07
SPLEEN	3.89E-16
PANCREAS	1.21E-16
S TISSUE	1.34E-04
OTHER	7.23E-10
Total	1.50E-04

RSAC Output

View RSAC Output File | Done

Summary Results | Inhalation | **Ingestion** | Ground Surface

For LHS results, double click in the table for the organ of interest.

Organs	Dose per Event Sequence (rem)
LUNGS	1.14E-08
S WALL	7.49E-11
SI WALL	3.91E-08
ULI WALL	6.24E-08
LLI WALL	1.19E-07
GONADS	3.64E-08
BREASTS	1.37E-08
BONE SUR	4.71E-08
R MARROW	2.81E-08
THYROID	4.66E-02
KIDNEYS	5.72E-10
LIVER	2.75E-08
SPLEEN	1.05E-15
PANCREAS	5.28E-16
S TISSUE	4.76E-04
OTHER	2.47E-08
Total	1.88E-03

RSAC Output

View RSAC Output File | Done

Summary Results | Inhalation | Ingestion | **Ground Surface**

Organs	Dose per Event Sequence (rem)
LUNGS	2.07E-06
STOMACH	1.57E-06
S INT	1.20E-06
UL INT	1.82E-06
LL INT	1.39E-06
TESTES	5.46E-06
BREAST	8.09E-06
SKELETON	3.39E-06
RED MARR	9.93E-07
THYROID	3.94E-06
KIDNEYS	3.21E-06
LIVER	1.69E-06
SPLEEN	1.43E-06
ADRENALS	1.64E-06
PANCREAS	1.10E-06
SKIN	9.11E-06
BRAIN	1.18E-06
THYMUS	2.51E-06
BLADDER	2.14E-06
MARROW	3.29E-06
HEART	1.12E-06
OVARIES	1.55E-06
UTERUS	9.39E-07
Total	3.90E-06

For LHS results, double click in the table for the organ of interest.