HAZARD AND BARRIER ANALYSIS GUIDANCE DOCUMENT

EH-33

OFFICE OF OPERATING EXPERIENCE ANALYSIS AND FEEDBACK

Rev 0 **November, 1996**

This work was performed for the Department of Energy, Office of Operating Experience Analysis and Feedback by P. Neogy and A. L. Hanson of the Department of Advanced Technology, Brookhaven National Laboratory; P. R. Davis of PRD Consulting, Inc., and T. E. Fenstermacher of Research Planning, Inc.

ACKNOWLEDGMENTS

The Hazard and Barrier Analysis Guide is largely a product of the deft management and team building by Mr. Richard Trevillian. The hazard and barrier analysis methodology was developed as part of an earlier project Mr. Andrew R. Marchese sponsored and collaborated on. The Hazard and Barrier Analysis Guide benefited from comments on and constructive criticism of an earlier draft of the Guide by several Department of Energy safety managers and safety experts.

TABLE OF CONTENTS

Page

FIGURES

Page

TABLES

EXECUTIVE SUMMARY

The Department of Energy (DOE) Office of Operating Experience Analysis and Feedback (OEAF) is sponsoring the development of simplified analytical techniques and tools for the analysis of operating events at DOE facilities to promote its theme of safety management through analysis. This effort was initiated to augment the usual anecdotal discussion of events that has been relied upon in the past to derive lessons learned from incidents and accidents. Initial results of this effort on safety management through analysis have been published as articles in OEAF's Operating Experience Weekly Summary and Safety Notices. The purpose of this Hazard and Barrier Analysis Guide is to document the analytical techniques developed in greater detail. More importantly, the Guide is meant to provide to the DOE complex a set of simple and straightforward tools to devise effective strategies for preventing accidents, and to evaluate accidents and accident precursors which have occurred across the DOE complex.

Although the Hazard and Barrier Analysis Guide was developed independently of the Department's recently published Integrated Safety Management Plan, it conforms closely to the core safety management functions of the Plan. The Guide is intended to provide techniques and tools for the safe execution of work. As such, it may be regarded as an example of a key element of the Safety Management Plan: *implementing a variety of activities to share, recruit, acquire, develop and train Departmental technical expertise for effectively implementing the Safety Management System.*

The Hazard and Barrier Analysis Guide was developed to achieve the following results: (1) identification of hazards that are associated with a specific activity, (2) identification, evaluation and implementation of a set of effective barriers that protects workers from these hazards, and (3) estimation of barrier failure likelihoods to arrive at an estimate of the risk of injury, fatality, environmental release, or property damage. In developing the Guide an extensive set of investigation reports of recent accidents (those occurring in the past decade) within the DOE complex was reviewed to arrive at appropriate techniques for Hazard and Barrier Analysis. The adaptability of Hazard and Barrier Analysis to simple risk analysis is a key attribute that was utilized to enhance the usefulness of this tool to applications that go beyond anecdotal safety assessments of past events or future activity.

A number of techniques have been developed primarily in the chemical process industry for identifying and evaluating hazards. Several of these have direct applicability to DOE operations, and some have recently been

utilized in detailed hazard analyses of complex DOE facilities. Hazard analysis techniques were carefully evaluated for their applicability to activities recorded in the accident investigation reports. Although hazard analysis techniques are often formalized processes (involving a qualified team leader and an experienced team) that may not be practical for all activities, some techniques such as the What-If/Checklist Analysis can be implemented by as few as one or two people when the operation being analyzed is fairly simple. This technique was found to be applicable to a wide variety of activities typical of the DOE complex. It was, therefore, recommended as the preferred technique unless special circumstances made it unsuitable.

Having identified the hazards inherent in an activity, it becomes necessary to identify and evaluate barriers that provide control over these hazards. Barriers may be physical barriers, procedural or administrative barriers, or human action. To aid in the process of barrier identification, a Hazard-Barrier Matrix was developed. The Hazard-Barrier Matrix was constructed by considering hazards that are typically associated with work at DOE facilities, and identifying the barriers that are likely to provide protection against these hazards. A number of categories of barriers were considered, and the barriers corresponding to the different potential hazards were entered into a matrix form to provide a convenient ready reference for hazard and barrier identification. The barriers were also color coded to provide a gradation of their perceived effectiveness (i.e., the degree of suitability or comprehensiveness of the barrier in protecting against a given hazard).

A distinction was made between the efficacy of a barrier and its reliability. The reliability of a barrier is its ability to resist failure. The objective of the process for identifying and evaluating barriers was to arrive at a set of optimum barriers, that is, a set of reliable and effective barriers. The expected failure frequencies of barriers provide a characterization of the reliability of the barriers. These failure frequencies are also important in assessing the risk associated with a particular activity. It was recognized that the expected failure frequencies of systems and components are not easy to characterize, since they depend on a number of factors such as the manufacturing process, the environment in which they operate, the age of the system or component, their maintenance record, etc. Fairly accurate reliability information can be generated by setting up a facility specific database of system and component failure rates, and updating it in an appropriate fashion as more data become available. Where facility specific databases do not exist, generic failure data are being increasingly utilized to estimate the reliability of systems and components. It should be noted that the use of generic failure rate data was the approach taken by the commercial nuclear industry before plant specific databases were developed. This was the approach adopted in the Guide for estimating both system as well as human reliability. A set of recommended generic system, component and human failure rates appropriate to DOE operations, together with guidance on utilizing them, has been incorporated in the Guide. The Hazard-Barrier Matrix, together with generic barrier reliability information, can assist in selecting appropriate barriers and assuring that they are available during work projects. Site personnel are encouraged to develop site-specific data on failure rates.

Utilization of generic system and human failure rates allowed estimation of the risk of injury associated with the activities. This was achieved in practice by constructing simplified event trees in combination with selected data to provide a quantitative estimate of the likelihood of various undesirable outcomes following the initiation of an event. The analyses aided in evaluating whether accidents that had occurred previously were likely to recur, and what strategies were available to prevent their recurrence. They also provided estimates of the likelihood of sequences of events that may not have occurred before. Several accidents, involving both radiological and toxic chemical hazards as well as industrial hazards, which have occurred at DOE facilities were analyzed in this manner, and insights were derived from the analyses. A procedure for performing these analyses has also been included in the Guide to encourage their use at DOE facilities. Users of the Guide are encouraged to share important lessons learned by utilizing the DOE Lessons Learned Standard.

While the Hazard and Barrier Analysis Guide provides and illustrates techniques for identifying hazards, identifying and evaluating the barriers against these hazards, and estimating the risk associated with activities, a systematic and comprehensive application of these techniques to the operation of a DOE facility has not been included in the Guide. Such an application to the Brookhaven High Temperature Combustion Facility has been made. This exercise provided assurance that application of these techniques to DOE facilities is feasible, and produced insights into the strengths and potential weaknesses of the methodology. The results of this application of Hazard and Barrier Analysis techniques are being published in a separate report.

1 INTRODUCTION

1.0 Introduction

This Guide was prepared to assist Department of Energy (DOE) facilities to perform work safely. It is intended to provide a set of simple and straightforward tools to devise effective strategies for preventing accidents, and to evaluate accidents and accident precursors which have occurred for the lessons that can be learned from them. Although developed independently, the Guide conforms to the Department's recently formulated Integrated Safety Management Plan[1]. It is not intended that the methods and data in the Guide become mandatory tools at DOE facilities, but rather that they would be used to augment and streamline the process of safety management. These methods are not intended to supplant more rigorous safety analyses required for other purposes, such as criticality safety analysis.

The Guide addresses three elements related to safety management: identifying hazards, identifying and evaluating barriers to mitigate hazards, and analyzing actual and potential accident sequences for insights into effective accident prevention. It is expected that important insights derived from the application of the guide will be processed and shared in accordance with the DOE Lessons Learned Standard. The hazard identification guidelines involve a summary of existing methods and combinations of methods which have been developed in the chemical process industry and applied in previous hazards analyses at DOE facilities. The barrier identification and evaluation process involves a matrix of possible barriers and their effectiveness which have been utilized to protect against various hazards at DOE facilities. This information can assist in selecting appropriate barriers and assuring that they are available during work projects. The analysis of actual and potential accident sequences involves the use of simplified event trees in combination with selected data to provide an estimate of the likelihood of various undesirable outcomes following an event. The analysis aids in a retrospective evaluation of whether accidents that occurred previously are likely to recur and what strategies are available to prevent their recurrence. It also provides prospective estimates of the likelihood of occurrence of sequences that may not have occurred before. Several accidents which have occurred at DOE facilities are analyzed in this manner, and insights are derived from the analysis.

The Guide does not address the costs of using the barriers or the costs of the accidents which would be prevented by the use of the barriers. For the present, the best judges of the costs involved are site personnel. Cost data may be added to a future revision of this report if such data becomes available.

Section 1.1 of the Guide discusses the background against which the Hazard and Barrier Analysis Guide was developed. It discusses the relationship of the techniques and tools presented in the Guide to the recently published DOE Plan for Integrated Safety Management. Chapter 2 of the Guide presents Hazard and Barrier Analysis techniques. Section 2.1 discusses hazard analysis techniques that are likely to be the most effective in identifying hazards relevant to the DOE complex. Sections 2.2 and 2.3 present a discussion of the control of hazards through barriers. A Hazard-Barrier Matrix is presented as a convenient tool for identifying and evaluating barriers once the potential hazards have been identified. General discussions on barrier reliability and human reliability are presented in Sections 2.4 and 2.5. These concepts are dealt with in greater depth in Appendices A and B. A risk-based approach to Hazard and Barrier Analysis is developed in Section 2.6, and the approach is applied to actual incidents involving a radiological and an industrial hazard in Sections 2.61 and 2.62, respectively. A detailed guide for the application of risk-based Hazard and Barrier Analysis together with several applications of the technique to selected incidents at DOE facilities is provided in Appendix C.

While the Hazard and Barrier Analysis Guide provides and illustrates techniques for identifying hazards, identifying and evaluating barriers against these hazards, and estimating the risk associated with activities, a systematic and comprehensive application of these techniques to the operation of a DOE facility has not been included in the Guide. Such an application to the Brookhaven High Temperature Combustion Facility has been made. This exercise provided assurance that application of these techniques to DOE facilities is feasible, and produces insights into the strengths and potential weaknesses of these techniques. The results of this application of Hazard and Barrier Analysis techniques are being published in a separate report.

1.1 Background

Operations at DOE facilities have generally enjoyed a safe history. The accidental death rates and injury frequencies for DOE operations have been comparable to or better than commercial industrial rates. However, accidents, some of them serious, continue to occur within the DOE complex, some of which are recurrences of previous events suggesting that more could be gained by gleaning the lessons learned from these events. In addition, when one considers unexpected or rare events which have not occurred in the lifetime of most DOE facilities, there are potentially significant risks which could be lessened by cost-effective means. Furthermore, the changing DOE mission, from weapons production to environmental cleanup and restoration, implies that work activities with hazards and risk somewhat different from those that were usually encountered will be increasingly undertaken. In view of these factors, DOE (EH) has considered it appropriate to develop guidelines and plans to assist operating contractors in maintaining and, if necessary, improving their safety culture by promoting safety management through analysis. The recently published "Department of Energy Plan for the Development and Implementation of Integrated Safety Management" also provides such guidelines and planning. The five core safety management functions within the Integrated Safety Management Plan are:

(1) define scope of work,
(2) identify and analyze hazards associated with the work,
(3) develop and implement hazard controls,
(4) perform work within controls, and
(5) provide feedback on adequacy of controls and continuous improvements in defining and planning work.

Although the Hazard and Barrier Analysis Guide was developed independently of the Integrated Safety Management Plan, it conforms closely to the core safety management functions of the Plan. The Guide is intended to provide techniques and tools for the safe execution of work. As such it has particular relevance to one key element of the Safety Management Plan: implementing a variety of activities to share, recruit, acquire, develop and train Departmental technical expertise for effectively implementing the Safety Management System.

In examining serious events which have occurred at DOE facilities, two global insights become apparent: (1) accidents tend to occur when familiar activities are undertaken in an environment where subtle or unrecognized changes have occurred which transformed normally safe activities into high risk situations, and (2) conventional industrial hazards appear to pose as important (or, in some cases, even greater) risks to the workers as radiological or toxic chemical hazards. This Guide was therefore developed to assist contractors in : (1) extracting more useful information and insights from previous accidents and accident precursors involving industrial as well radiological and toxic chemical hazards, and (2) utilizing this information to devise effective strategies to reduce the accident potential for planned activities at DOE sites.

2 HAZARD AND BARRIER ANALYSIS TECHNIQUES

This chapter of the Guide deals with techniques for analyzing hazards associated with work and identifying the barriers that provide protection from these hazards. The term “barriers” is used to describe systems, components, structures, procedures and human actions. It is roughly equivalent to the term “controls” that has been used in the Department’s Safety Management Plan. The Target-Barrier-Hazard analysis methodology, utilized by the DOE Plutonium Working Group,[2] incorporates some of the attributes of the Hazard and Barrier Aanalysis techniques described in this chapter.

2.1 Hazard Identification

Several techniques have been developed primarily in the chemical process industry for identifying and evaluating hazards. The interested reader is encouraged to consult *Guidelines for Hazard Evaluation Procedures*,[3] published by the Center for Chemical Process Safety of the American Institute of Chemical Engineers, which has been used as a principal source for this chapter of the Guide. Hazard analysis techniques are often formalized processes involving a qualified team leader and an experienced team. For all hazard and barrier analysis applications, such formalized processes may not be practical. However, some of the hazard evaluation techniques, such as the What-If Analysis discussed below, can be implemented by as few as one or two people when the operation being analyzed is fairly simple, which is typically the case for many DOE facilities. Furthermore, the thinking process behind all these techniques is likely to be useful in all Hazard and Barrier Analysis applications. A central issue in all hazard identification techniques is that of completeness – assuring that the list of hazards is as exhaustive as appropriate. One way that the issue of completeness is addressed is by putting together a multi-disciplinary hazard evaluation team. The combined experience of the team is expected to provide assurance that no important hazards are overlooked. Another way of addressing the issue of completeness is to use more comprehensive techniques for those processes that are perceived to pose the highest risk—a graded approach. A discussion of hazard identification techniques likely to be of most value is provided in sections 2.11 through 2.14.

2.11 Checklist Analysis

A checklist analysis is an experience based approach in which a list of specific items is used to identify known types of hazards, potential accident situations, or design deficiencies. Checklists are often used in the evaluation of new processes to identify and eliminate hazards that have been recognized in the previous operation of similar systems.

Checklists are developed specifically for a process or an operation, and a Checklist Analysis includes a tour of the environment in which the process or operation is to take place. Checklists should be regarded as living documents that need to be audited and updated regularly. Lessons learned and recent applicable operating experience should be incorporated after a formal review. Traditionally, checklists have been used to ensure that organizations are complying with standard practices. Checklist Analysis includes a review of the process or operation by the hazard evaluation team members. This review responds to the checklist issues based on observations, systems documentation, interviews with operators, and personal perceptions. The hazard evaluation team documents any deficiencies observed, and provides recommendations for safety improvements.

While Checklist Analysis is a structured, systematic process, it is of limited use in uncovering unique or unexpected or unlikely hazards. There are hazard evaluation techniques involving more creative, brainstorming processes that are better suited to identifying such unique or unexpected hazards. Two such techniques: What-If and HAZOP Analysis are described briefly in sections 2.12 and 2.13.

2.12 What-If Analysis

The What-If Analysis technique is a flexible, creative examination of a process or operation for potential hazards. Members of the hazard evaluation team are encouraged to ask What-If questions or discuss specific issues that concern them. The What-If Analysis reviews the process or operation systematically from the beginning to the end (or the boundary defined by the scope of the analysis). The team leader guides the analysis in any appropriate logical way, although the objective is to be as comprehensive as possible while economizing on time and effort. The analysis usually focuses on a particular type of consequence such as environmental contamination, or worker and public safety. This is a powerful hazard evaluation technique in the hands of a skilled leader and an experienced team, but could lead to incomplete results otherwise. For simple systems or operations the analysis can be conducted by as few as one or two people.

Documentation is a key to transforming the findings from a What-If Analysis into measures for hazard elimination or reduction. The team's findings are often recorded in a What-If Worksheet like the one shown below. In addition to the worksheet, the team usually develops a list of suggestions to improve the safety of the operation or process based on the What-If Analysis results.

2.13 HAZOP Analysis

Hazard and Operability (HAZOP) analysis operates on the principle that a group of experts with different backgrounds working together on a project can interact in a creative fashion and identify more problems than when working separately and combining their results. Although HAZOP Analysis was originally developed for a new design or technology, it is applicable to almost all phases of a process's lifetime. The HAZOP study focuses on specific process sections or operating steps called "study nodes." The hazard evaluation team examines each study node for potentially hazardous deviations with the help of a set of established guide words: "No," "Less," "More," "Part Of," "As Well As," "Reverse," and "Other Than." The guide words are systematically applied to the process parameters at each study node to ensure that all relevant deviations of the process parameters and their consequences have been evaluated. HAZOP, more than any other hazard evaluation technique, is geared towards a multi-disciplinary team approach. Although the HAZOP Analysis thought process can be used by one person, the results of such a study cannot be called HAZOP Analysis.

Table 2.1 Typical format for a what-if analysis worksheet

Area:

Operation/Process:

Meeting Date:

Team Members:

What-If	Consequence/Hazard	Safeguards	Recommendation

2.14 What-If/Checklist Analysis

The creative, flexible, brainstorming nature of a What-If Analysis can be combined with advantage with the systematic, structured approach of a Checklist Analysis in what is known as a What-If/Checklist Analysis. This method capitalizes on the strengths of the two methods while compensating for the shortcomings of the individual methods. The Checklist Analysis, being an experience based technique, may miss hazards if the checklist is not complete. The What-If Analysis encourages the team to consider potential hazards that are not covered in the checklist. Conversely, the checklist portion of the analysis lends a more structured and systematic nature to the What-If Analysis.

The checklists used in the What-If/Checklist Analysis are somewhat more general than conventional checklists used in Checklist Analysis. This fact, together with the flexible, brainstorming approach of What-If Analysis allows What-If/Checklist Analysis much wider applications than a conventional, narrow focus Checklist Analysis. A What-If/Checklist Analysis, combining as it does the flexible, exploratory approach of a What-If Analysis with the structured, disciplined approach of a Checklist Analysis, is expected to be an optimum choice for a variety of work planning processes. Based on our experience of work being performed at DOE facilities, we recommended that What-If/Checklist Analysis be considered first as a hazard identification tool before other methods are tried. Additionally, we recommend that the teams be true teams in that the groups should have successfully gone through some recognized team-building experiences and training.

An example of a Hazard Checklist (from Reference 3) usable with What-If/Checklist Analysis is presented in Table 2.2.

Table 2.2 Example of a hazard checklist

Acceleration (uncontrolled - too much, too little)

- inadvertent motion
- sloshing of liquids
- translation of loose objects

Deceleration (uncontrolled - too much, too little)

- impacts (sudden stops)
- failure of brakes, wheels, tires, etc.
- falling objects
- fragments or missiles

Chemical Reaction (nonfire)

- disassociation of product into separate components
- combination to form new product from mixture
- corrosion, rust, etc.

Electrical

- shock
- burns
- overheating
- ignition of combustibles
- inadvertent activation
- electrical explosion

Explosions

- commercial explosive present
- explosive gas
- explosive liquid
- explosive dust

Flammability and Fires

- presence of fuel - solid, liquid, gas
- presence of strong oxidizer - oxygen, peroxide, etc.
- presence of strong ignition force - welding torch, heater, etc.

Table 2.2 (continued)

Heat and Temperature

- source of heat - nonelectrical
- hot surface burns
- very cold surface burns
- increased gas pressure caused by heat
- increased flammability caused by heat
- increased volatility caused by heat
- increased activity caused by heat

Mechanical

- sharp edges or points
- rotating equipment
- reciprocating equipment
- pinch points
- weights to be lifted
- stability/toppling tendency
- ejected parts or fragments

Pressure

- compressed gas
- compressed air tool
- pressurized system exhaust
- accidental release
- objects propelled by pressure
- water hammer
- flexible hose whipping

Static

- container rupture
- over pressurization
- negative pressure effects

Leak of Material

- flammable
- toxic
- corrosive
- slippery

Radiation

- ionizing radiation
- ultraviolet light
- high intensity visible light
- infrared radiation
- electromagnetic radiation
- laser radiation

Toxicity

- gas or liquid
  - — asphyxiant
  - — irritant
  - — systemic poison
  - — carcinogen
  - — mutagen
- combination product
- combustion product

Vibration

- vibrating tools
- high noise level source
- metal fatigue
- flow or jet vibration
- supersonics

Miscellaneous

- contamination
- lubricity

2.2 Identification and Selection of Optimum Barriers

Barriers provide control over hazards associated with a job. Having identified the hazards posed by an activity, it becomes possible to identify the barriers that are available to control these hazards. Barriers may be physical barriers, procedural or administrative barriers, or human action. Examples of physical barriers are a glove box or a ventilation system for containing radioactivity, packaging for containing hazardous material, a guard or a shield protecting the operator from machinery, protective clothing and equipment used against electrical, chemical or radioactive hazards, etc. Examples of procedural or administrative barriers are Technical Safety Requirements (TSRs) that define the safety envelope of a nuclear process or a system, the double contingency principle for assuring nuclear criticality safety, procedures for the safe operation of a crane or a fork lift, emergency procedures for evacuating a building, etc. Human action is often, but not always, associated with a procedural barrier. Examples of human action serving to control a hazard are controlling and extinguishing a fire, de-energizing an electrical circuit either in response to a procedure or as part of safe work practice, evacuating a building in response to a fire or a criticality alarm, etc.

It will be apparent from the variety of barriers available for hazard control that some barriers will be more successful than others in providing protection. It is useful to think in terms of the reliability and the effectiveness of barriers. Reliability of barriers is related to their ability to resist failure. A safety system with a failure frequency of 10^{-4} per demand is a more reliable barrier than one with a failure frequency of 10^{-2} per demand. The effectiveness of a barrier is related to how suitable or how comprehensive the barrier is in protecting against a particular hazard. Limiting the inventory of fissionable material is an effective barrier against inadvertent criticality because it does not allow the criticality event to occur. A criticality alarm is not as effective a barrier because the alarm may sound too late for personnel in the vicinity of the accident to take effective action. One objective of the barrier identification process is to identify one or more optimum barriers against a hazard. To aid this process, it is useful to think in terms of “steel” barriers (effective and reliable barriers) and “paper” barriers (less effective or reliable barriers). The aim is to identify one or more “steel” barriers rather than a number of “paper” barriers.

One should bear in mind that the identification of barriers for a specific activity is best performed by individuals with a knowledge of the proposed activity, the environment, and the applicable procedures. The tools discussed in this Guide are meant to augment the processes of hazard and barrier identification rather than replace processes already in place to achieve these objectives.

2.3 The Hazard-Barrier Matrix

The Hazard-Barrier Matrix is a convenient tool for identifying and evaluating barriers after the potential hazards have been recognized. A suggested form of the Hazard-Barrier Matrix is presented in Figure 2.1. The Hazard-Barrier Matrix is constructed by considering the hazards that have been included in recent hazard studies[4,5] of DOE facilities and identifying the barriers that are likely to provide protection against these hazards. A number of categories of barriers is considered, and the barriers corresponding to the different hazards are entered into a matrix form to provide a convenient ready reference for hazard and barrier identification. The barriers are also color coded to provide a gradation of their perceived effectiveness. A discussion of the reliability of the barriers is provided in Section 2.4 and Appendix A.

An important purpose of the Hazard-Barrier Matrix is to provide a degree of completeness in the identification of hazards and barriers. We suggest that the generic matrix presented in Figure 2.1 be modified and augmented to ensure that the hazards and barriers that are most relevant to a particular facility are given due importance. The Hazard-Barrier Matrix provides an important step in Hazard and Barrier Analysis. This step can be followed up, as necessary, by considering the reliability of the barriers and the risk implications of their failure as discussed in Sections 2.4 through 2.6. The Hazard-Barrier Matrix should be a focal point for the safety management aspects of the planning process for work at facilities involving hazards to workers, the public and the environment. It should play an important role in integrating the safety planning of work.

2.4 Barrier Reliability

As discussed in Section 2.2, the expected failure frequencies of barriers provide a quantitative description of the reliability of the barriers. Such descriptions of the reliability of barriers are important in making an optimum choice of barriers against a particular hazard. Expected failure frequencies are also important in estimating the risk associated with a particular activity as will be discussed in Section 2.6. The expected failure frequency of a system or a component, however, is not easy to characterize since it depends on a number of factors such as the manufacturing process, the environment in which it operates, the age of the system or component, its maintenance record, etc. Fairly accurate reliability information can be generated from a facility specific database of system and component failure rates, and updating it in an appropriate fashion as more failure data become available (see Appendix A). Such databases, when

Figure 2.1 Hazard-Barrier Matrix

Hazard Sources	Examples	Deenergize	Lockout and Tagout	Physical Barrier	Proper Anchoring	Glove Boxes	Isolation (Valves, Piping, Vacuum)	Pressure Relief Valve	Double Contingency	Distance	Protective Clothing/Eqpmnt	Geometry	Inventory Control	Warning Sound/Light	Proper Packaging	Exclusion Zone
Electrical Sources	High Voltage and Current Sources	✓	✓	*						*	*			✓		*
	Transformers	✓	✓	*						*	*					*
	Batteries			✓						✓	✓					✓
	Static Electricity			✓						✓	✓					✓
Motion Sources	Shears, Sharp Edges, Pinch Points, Machinery			✓						✓						✓
	Vehicles/Forklifts and Trucks			✓						✓				✓		✓
	Mass in Motion			✓						✓						✓
Gravity-Mass Sources	Falling			✓												
	Falling Objects			✓	✓					✓						✓
	Lifting															
	Tripping, Slipping															
	Earthquakes				✓									✓		
Pressure Sources	Chemical Reactions						✓			✓	✓		✓		✓	✓
	Noise									✓						✓
	Confined\Compressed Gases						✓	✓							✓	
	Extreme Wind			✓										✓		
Chemical Sources	Corrosive Materials						✓			✓	✓		✓		✓	✓
	Flammable Materials						✓			✓	✓		✓		✓	✓
	Toxic Materials						✓			✓	✓		✓		✓	✓
	Reactive Materials						✓			✓	✓		✓		✓	✓
	Carcinogenic Materials						✓			✓	✓		✓		✓	✓
	Oxygen Deficiency						✓			✓	✓			✓	✓	✓
Heat Sources	Electrical	✓	✓	✓						✓	✓					✓
	Plasma Torch	✓	✓	✓						✓	✓					✓
	Natural Gas						✓			✓	✓					✓
	Friction									✓	✓					✓
	Spontaneous Combustion						✓			✓	✓					✓
Cold Sources	Cryogenic Materials			✓						✓	✓			✓		✓
	Ice, Snow, Wind, Rain									✓	✓					✓
Radiant Sources	Radioactive Materials			✓		✓	✓			✓	✓		✓	✓	✓	✓
	Ionizing Radiation	✓		✓						✓	✓			✓		✓
	Rf Fields	✓	✓	✓						✓				✓		✓
	Infrared Sources	✓	✓	✓						✓				✓		✓
	Ultraviolet	✓	✓	✓						✓				✓		✓
	Plasma Beam\Laser Beam	✓	✓	✓						✓	✓			✓		✓
	Chemical Reactions			✓			✓			✓			✓	✓	✓	✓
	Nuclear Criticality			✓			✓		✓	✓		✓	✓	✓	✓	✓

Barrier Effectiveness

🟦 🟩 🟧 🟥

Most Effective → Least Effective

*Needed if deenergizing is not available

available, can provide very useful barrier reliability information. For most applications, however, comprehensive facility specific data will not be available. Increasingly in these situations generic failure data are being utilized to get a semi-quantitative estimate of the reliability of the barrier. Where semi-quantitative estimates are to be made using generic failure data, local subject matter experts are probably best suited to make those estimates.

Tables 2.3, 2.4 and 2.5 present generic failure data for typical components, systems and structures thought to be useful for planning purposes at DOE facilities. The tables are taken from a recent paper by J. A. Mahn, G. W. Hannaman, and P. Kryska.[6] The third column of each table provides a probability range for each element representing an eighty percent confidence interval for typical U.S. facilities designed under consensus codes and standards using commercially available components. The value in the second column is a nominal value. Adjustment factors are provided to increase or decrease the nominal values based on adverse or beneficial conditions. If more than one adjustment factor is applicable, the nominal value is multiplied by all the applicable adjustment factors.

Table 2.3 Generic component failure frequencies

Description of component and failure mode	Point estimate (per hour)	Range of failure rates (per hour)	Adjustment factor	Need for adjustment factor
Standby compressors, diesels, pumps: Do not start or run on demand	1E-3	1E-4 to 1E-2	10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
			0.3	A proactive preventative maintenance program and margin in design.
Active components such as turbines, electric motors, pumps, valves, breakers, and control and protection circuits do not operate on demand	1E-5	1E-6 to 1E-4	3	If no periodic maintenance
			0.5	Preventative maintenance program
Transformers short	1E-7	1E-8 to 1E-6	10	If overloaded or no periodic oil testing.
Piping leaks	1E-7	1E-8 to 1E-6	2	Pumping abrasive or corrosive material.
			0.1	Pumping water with a controlled chemistry.
Tanks and structures - leak rupture	1E-9	1E-10 to 1E-8	10	No in-service inspections.
Steel vessels - leak rupture	1E-10	<1E-10	0.1	Full inspection and continual monitoring to detect leak before break.

Table 2.4 Generic system failure frequencies

Description of system and failure mode	Point estimate (per demand)	Range of failure probabilities (per demand)	Adjustment factor	Need for adjustment factor
Single channel system (pump, piping, valves, motor, breaker or wires). Controlled by signal from system state to provide flow or mixing of material, or to transmit electricity.	5E-2	0.5 to 1E-2	10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
			0.1	A proactive preventative maintenance program is controlled under administrative procedures.
A redundant system which includes two or more trains made up of the elements of the single train; includes common cause failures	5E-3	5E-2 to 5E-4	10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
			0.1	A proactive preventative maintenance program is controlled under administrative procedures.
Partly diverse system of two or more trains using different types of pumps or power (steam vs. AC); includes common cause failures.	1E-3	1E-2 to 5E-5	10	Material pumped is abrasive or corrosive (not water). Replacement upon failure
			0.1	A proactive preventative maintenance program is controlled under administrative procedures.
A fully diverse system of two or more trains using different power sources, and different functional ways of achieving the desired objective; includes common cause failures.	1E-4	1E-3 to 5E-6	10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
			0.1	A proactive preventative maintenance program is controlled under administrative procedures.
Two diverse systems consisting of two redundant trains within each diverse segment. The safety objective can be satisfied with one or two trains using different functions; includes common cause failures.	5E-6	1E-4 to 5E-7	10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
			0.1	A proactive preventative maintenance program is controlled under administrative procedures.

Table 2.5 Generic structure failure frequencies

Description of typical structure and failure mode	Point estimate (per demand)	Range of failure probabilities (per demand)	Adjustment factor	Need for adjustment factor
A low pressure, or single wall structure, e.g., a tank with pressure relief system, or atmospheric pressure storage drum. Failure mode is leak caused by corrosion.	5E-2	0.5 to 1E-2	10	Contains abrasive or corrosive material and replacement is due to failure.
			.1	A proactive surveillance and inspection program under administrative procedures is used to monitor the condition of the structure.
A pressure vessel, double wall or redundant structure with multiple penetrations used in pressurized processes; designed to withstand accident transient pressures and temperatures by means of pressure relief valve opening. Example failure mode is opening of relief valve with failure to reclose following transient.	5E-3	1E-2 to 1E-3	10	Contains abrasive or corrosive material, and replacement is due to failure
			.1	A proactive surveillance and non-destructive inspection program under administrative procedures monitors the condition of the structure. Procedures for restoration of boundary exist.
A pressure vessel, double wall or redundant structure used primarily for storage. Designed to withstand accident transient pressures and temperatures with relief valves opening, and has reclosable leak path. Example failure modes include: 1) Leaving valve or penetration open after filling, draining, or maintenance. 2) Leaking valve from erosion or wear. 3) Load accidentally exceeds the structural strength.	1E-3	<1E-3	10	Contains abrasive or corrosive material, and replacement is due to failure.
			.1	A proactive surveillance and non-destructive inspection program under administrative procedures monitors the condition of the structure. Procedures for restoration of boundary exist.

In general, the analyst would like the simplest “screening” level data of Tables 2.3 through 2.5 to characterize the accident sequences. For cases where the reader may need data more detailed than the generic screening data of table 2.3 through 2.5, Appendix A provides point estimates for recommended failure rates of various components and systems in the US industry and specific DOE facilities.

2.5 Human Reliability

The analysis of many accidents have led to the appreciation that these often involve multiple equipment failures and process deviations combined with faulty human decisions and actions. Safety assessments, therefore, are not complete unless the interactions between equipment failure and human actions are considered. The approach to human reliability assessment followed in the Guide is to arrive at semi quantitative estimates of human failure rates following the prescriptions of J.A. Mahn et al.[6], and use these as appropriate in the semi-quantitative hazard and barrier analysis described in Section 2.6.

Since human behavior is complex, and does not lend itself immediately to relatively straightforward reliability models, Mahn et al. suggest the following classifications of human interactions that typically group all activities that need to be considered:

(1) Pre-initiator human interactions involving maintenance, testing, calibration, planning, etc.

(2) Initiators of accidents that involve operator awareness of potential accident initiators caused by errors in tests, or reconfiguration conditions involving control systems, protective logic, computer controlled functions and manual control, and

(3) Post initiator interactions that involve procedure specified actions and recovery actions developed from training and experience.

These classifications of human interactions can be related to a simple error classification system consisting of three categories: (1) slips, (2) non-response, and (3) mistakes. This classification scheme can then be used to qualitatively incorporate human errors in accident scenarios. Table 2.6 provides generic human error probabilities for use in accident scenario assessment. Other sources of human reliability data are discussed in Appendix B.

Table 2.6 Generic human failure probabilities

Human Error Probability	Description of human interaction and error	Adjustment factor	Example factors for a facility specific adjustment
3×10^{-3} to 3×10^{-4}	Pre-Initiator actions - Test, maintenance, and calibrations leaving a component, or system with unrevealed fault. Includes typical errors in maintenance that cause overall system unavailability (10^{-3})	× 10	No written procedure available, or newly defined action; verbal instructions, no checking for completed action, poor equipment/procedure identification label matching.
	Errors include: slips, non-responses, or mistakes leading to skipping a procedure, selecting an incorrect procedure, omitting a step in a procedure, improper communication, transposition of labeling, or misunderstanding task responsibility.	× .1	Use established, practiced, written procedures, discussed in training, work progress verified with signed checklist, apply self checking, use tag-out system to maintain configuration control, etc.
1×10^{-2} to 1×10^{-4}	Initiator actions - Test, maintenance and calibration activities that trigger events. Includes contribution of errors that cause initiating events - covered in initiating event frequencies (10^{-3})	× 10	Signals and instruments inappropriate for the action and procedure, lack of cues, or verbal instructions for interlocks, need for process knowledge, requires interpretation of indirect information, etc.
	Typical error modes include slips, nonresponses and mistakes.	× .1	Indications permit easy transfer through procedures, discussed in training, practiced before hand, administrative control of tags, training involves understanding of the basic principles, and feedback of lessons learned from event precursors.
l to 1×10^{-3}	Post-Initiator actions - Response actions that are not successful in terminating or mitigating the event. Includes recovery actions subsequent to initiating events: (.1) following multiple failures and (.03) directly following an initiating event.	× 30	Actions typically outside control room, involves more than one person, lack of a clear cue, knowledge of the process required, process knowledge substituted for emergency procedures, etc.
	Errors include slips, mistakes, and nonresponses for control and mitigation actions following an initiating event.	× .03	Actions in a control room, include redundant cues, memorized and practiced responses, clear man-mach. interface, action priorities stressed in training which includes simulation of process dynamics, recoverability from errors, training on infield procedures and long time available for action.

2.6 Risk-Based Approach to Hazard and Barrier Analysis

Hazard and Barrier Analysis is a tool that has important applications both as a proactive aid in safe work planning and in systematic after-the-fact investigations of incidents and accidents to characterize the safety/risk significance of operating events. The adaptability of Hazard and Barrier Analysis to simple risk analysis enhances the usefulness of this tool for applications that go beyond anecdotal discussions of past events or future work.

Hazard and Barrier Analysis consists of the three following steps: (1) identification of hazards that are associated with a specific task, (2) identification and implementation of a set of effective barriers that protect the worker from these hazards in the course of the work, and (3) estimating the likelihood of failure of the barriers to arrive at an estimate of the risk of injury or other undesirable consequences. The first two steps in Hazard and Barrier Analysis have been discussed in Sections 2.1 through 2.5 of this Guide. This Section of the Guide discusses the third step—estimating the risk of injury. A more detailed discussion of Hazard and Barrier Analysis, together with guidance for performing event tree analysis and several illustrative applications of Hazard and Barrier Analysis to actual incidents that occurred at DOE facilities, is provided in Appendix C.

Figure 2.2 provides a schematic illustration of risk-based Hazard and Barrier Analysis. For purposes of illustration, it is assumed that the barriers to injury consist of: (1) an adequate work plan, (2) proper implementation of procedures, and (3) proper functioning of protective systems or equipment. It is also assumed that either the second barrier (proper procedure implementation) or the third barrier (proper functioning of protective system or equipment) can prevent injury. The simplified event tree in Figure 2.2 shows the combinations of barrier failures that lead to injury. If the likelihood of failure of the barriers is known, the event tree also provides an estimate of the likelihood of sustaining injury. The estimated likelihood of injury provides a means for determining whether the barriers selected are adequate. The importance of the first barrier, an adequate work plan, is more than apparent at first. Hazard and Barrier Analysis of actual incidents and accidents shows that adequate work planning plays a crucial role in injury prevention, often reducing the likelihood of injury by an order of magnitude or more by reducing the likelihood of failure of subsequent barriers (see Section 2.62 and Appendix C).

Event trees such as the one showed in Figure 2.2 can be constructed either for incidents or accidents that have occurred in the past, or for some task that is yet to be undertaken. In the former application, the analysis provides important insights or "lessons learned" from the incident, e.g., the actual efficacy of the barriers analyzed. In the latter application, the analysis provides important proactive safety insights into the task to be performed, thus allowing safety to be managed better. Specifically, risk-based Hazard and Barrier Analysis provides a measure of risk associated with individual operations. It provides a measure of risk reduction associated with the implementation of individual barriers, and allows judgment to be exercised on the relative importance of hazards and barriers.

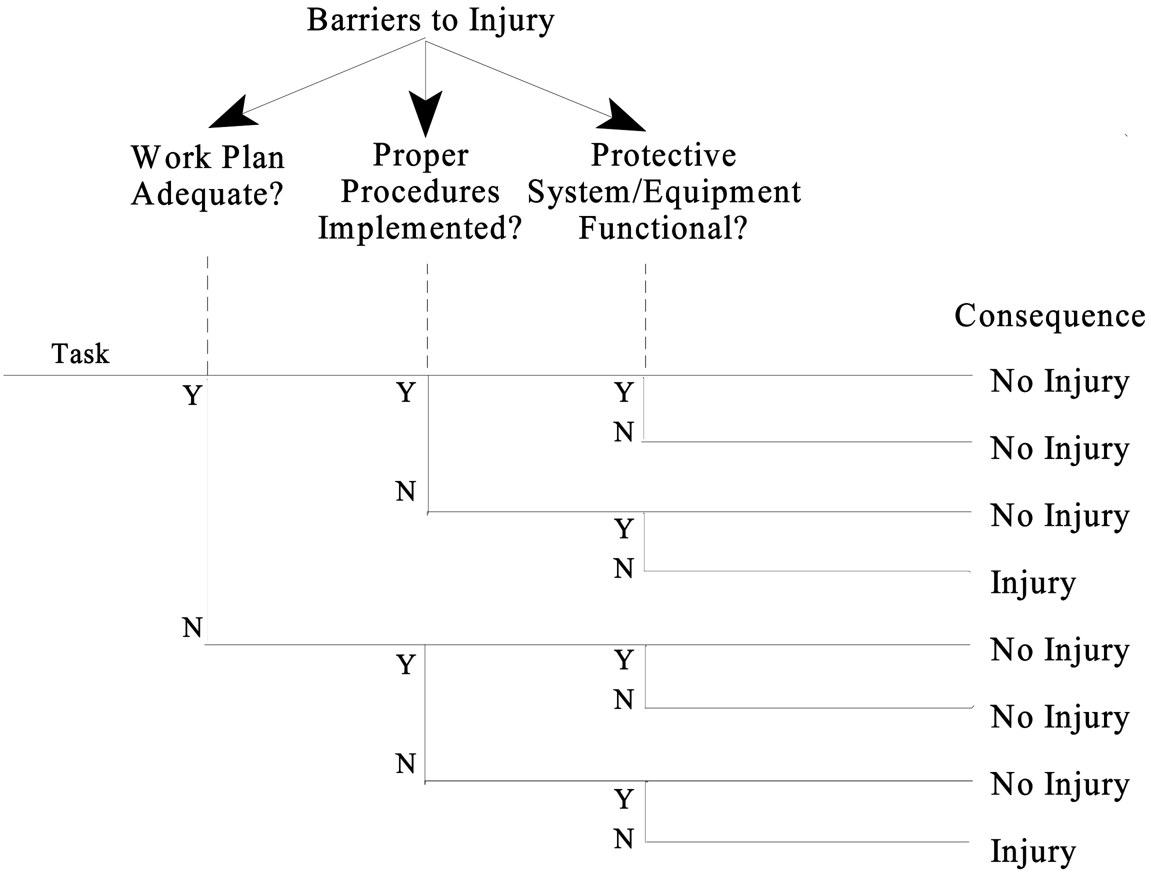


Figure 2.2 Schematic of risk based hazard and barrier analysis

Applications of risk-based Hazard and Barrier Analysis to a glove box fire incident and an incident involving an electrical hazard are provided in Sections 2.61 and 2.62. This choice of events is made in part to demonstrate that the technique is applicable to radiological as well as non-radiological, industrial hazards. These analyses have been previously published as Safety Notices,[7,8] and Operating Experience Weekly Summary[9,10] articles. A detailed guide for the application of risk-based Hazard and Barrier Analysis together with several more applications of the technique to incidents at DOE facilities is provided in Appendix C.

2.61 Analysis of a Glove Box Fire

In November 1994, rags contaminated with Pu^{238} and drying on the floor of a glove box in a plutonium processing and fabrication facility were found to be undergoing spontaneous combustion. The glove box was successfully isolated from any source of oxygen, and the smoldering rags were subsequently allowed to burn to completion by controlling the flow of oxygen to the glove box. No radioactivity was released from the glove box as a result of this event.

Given the observed event, spontaneous combustion of contaminated rags in a glove box, several barriers existed to prevent the release of radioactivity to the laboratory in which the glove box is located. These included: (1) detection of the fire and intervention by a worker to contain it, (2) maintenance of the glove box containment despite the fire, and (3) the ventilation system which maintains the glove box at a negative 0.8 inch water column pressure with respect to the room, and minimizes a release when the glove box containment is lost.

Figure 2.3 presents a simplified event tree for radioactive release based on the barriers discussed above. The likelihood of the fire being detected by a worker depends on how frequently the room is checked by a worker during normal operating shift or by a security personnel at other times. The likelihood of the fire being contained after detection by the worker will also depend in part on the skill and training of the worker to perform this non-routine task. The fact that the fire was detected and contained in this particular instance indicates that the likelihood of detecting and successfully containing the fire is not far from 100%. In the absence of more detailed information or analysis, this likelihood was estimated to be about 0.5 or 50%. If the fire escapes detection, there is still some likelihood that the fire would burn itself out without breaching the glove box containment. This likelihood will depend on the size of the fire and its location within the glove box (proximity to the gloves). Since the amount of material available for combustion in this event consisted of only about a quarter pound of rags probably placed near the center of the glove box floor, the fire had the potential to be small and localized. The likelihood of the glove box containment to be maintained despite the fire burning undetected was again estimated to be about 0.5. At the facility in question, there have been incidents of release of radioactivity from a glove box after it is breached due to improper ventilation or improper worker response. The likelihood of the ventilation system being defeated after the breach of glove box containment is estimated to be about 10^{-2}. The likelihood of radioactive release from this event results from the product of the three probabilities on the branch leading to significant release in Figure 2.3, and is, therefore, 0.5 × 0.5 × .01 or 2.5×10^{-3}.

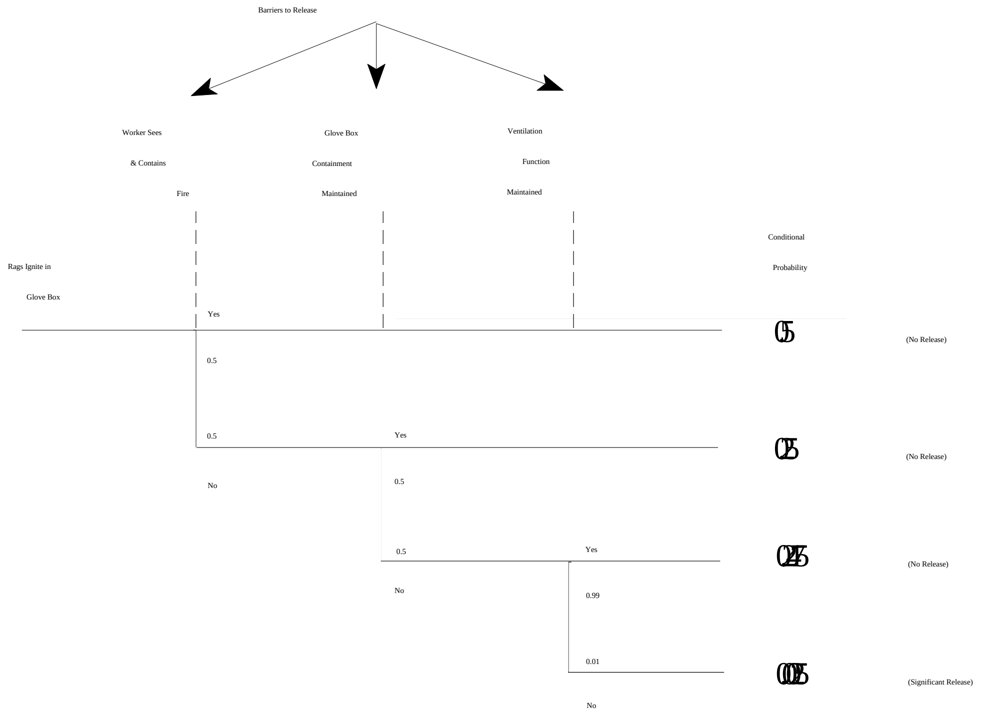


Figure 2.3 Simplified event tree for glove box fire

The potential consequence from this event is the inhalation of Pu^{238} by a worker in the room. The inventory of Pu^{238} in the rags was not measured or estimated in the occurrence report. For the purpose of this analysis, based on a heating rate of about 10 W (enough to heat a quarter pound of rags to the point of smoldering), the amount of Pu^{238} in the rags is estimated to be about 18 g (using a Pu^{238} heat output rate of 0.57 W/g). The fire causes a fraction of the Pu^{238} particles to become airborne within the glove box atmosphere. It is assumed that 10% of the airborne Pu^{238} particles escape into the room and distribute themselves over the volume of the room (311 m^3). The worker is assumed to breathe the contaminated atmosphere for 10 seconds before evacuating the room in response to a continuous air monitor alarm or a fire alarm.

The inhalation dose is given by:

$$Dose = \frac{MAR \times ARF \times RF \times SA \times BR \times T \times CEDE}{V} ,$$

where

MAR is the mass of material at risk (18 g × 0.1),
ARF is the airborne release fraction of Pu238 subjected to high temperatures (6×10^{-3}),
RF is the corresponding respirable fraction (1×10^{-2}),
SA is the specific activity of Pu^{238} (17.2 Ci/g),
BR is the breathing rate (3.5×10^{-4} m^3/s),
T is the time for which the worker breathes the contaminated air (10 s),
CEDE is the committed effective dose equivalent (4.6×10^{2} rem/microCurie), and
V is the volume of the room (311 m^3).

Therefore, Dose = 9.6 rem.

That is, under uniform dilution conditions, the average dose to the worker would be 9.6 rem. The dose to the maximally exposed worker would be higher. In an earlier incident involving radioactive release from a glove box in the same facility, the concentrations of radioactivity at three locations within the room were measured with continuous air monitors. The largest reading was found to be approximately twice the average reading of the three monitors. Assuming the same ratio of the maximum to the average dose, gives a dose to the maximally exposed worker of about 20 rem. Utilizing a conditional probability of release of 2.5×10^{-3}, and a maximum dose of 20 rem, a point estimate of the product of the dose and the conditional probability is 5×10^{-2} rem. Using a risk coefficient[11] of 4×10^{-4} fatality per rem, the fatality risk from the event is 2×10^{-5} fatality per event.

Figure 2.4 presents the fatality risk from the event and compares it to two reference or benchmark risk values. The first of these is the threshold for significant risk as adopted by the Occupational Safety and Health Administration (OSHA) in its final benzene rule (10^{-3} fatality). The second is the average lifetime accidental fatality risk Of 4×10^{-3} in U.S. industries. This reference value is derived by multiplying the average annual accidental fatality risk in U.S. industries of 10^{-4} fatality per year by an average work life of 40 years. The fatality risk from the event is clearly small compared to either of the benchmark risks.

2.62 Analysis of an Electrical Hazard Incident

In June 1994, an electrician working on a 480-volt main distribution panel in a composite materials technology facility received serious flash burns from an electrical fault and the subsequent electrical arc blast. The electrical fault occurred when a ground wire to be installed made contact with exposed parts of energized incoming connections on the main breaker which had been turned off.

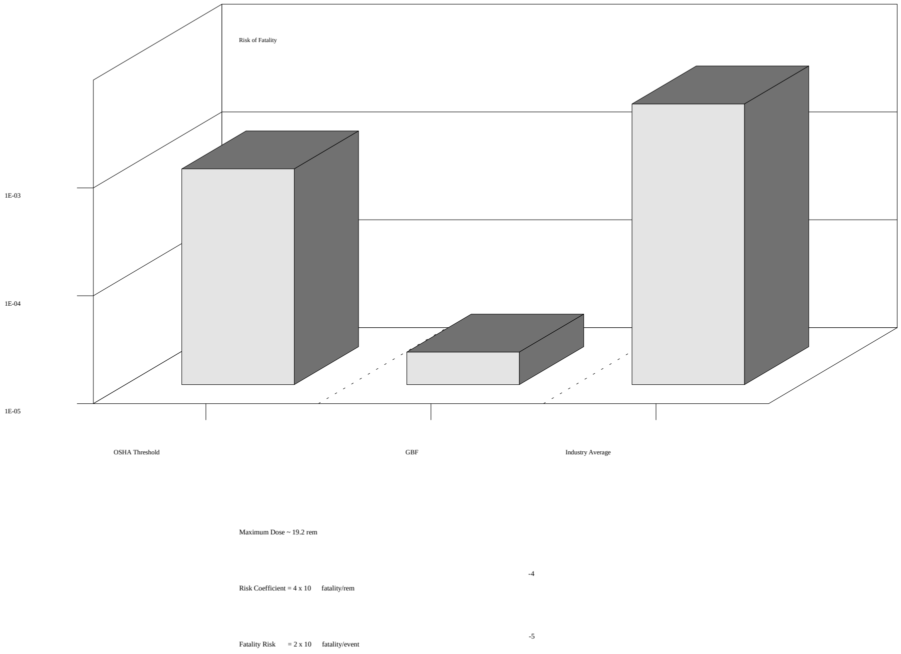


Figure 2.4 Comparison of risk to reference risk for glove box fire

After an electrician removes the protective cabinet enclosure covering a distribution panel, several barriers exist in principle to protect him from electrical hazards. The first of these is an adequate work plan that acquaints him with the hazards involved, and provides him with instructions on how to safely execute his task. A second barrier exists in the form of a procedure for electrical energy isolation and control (lockout/tagout). Lastly, protective equipment such as blankets and safety glasses provide a third barrier. It should be noted that the second and third barriers are contingent upon the first - an adequate work plan that guides the worker and alerts him to the hazards of his task. For the event being analyzed, as we shall see, the first barrier failed and consequently, the second and third failed as well.

Figure 2.5 presents a simplified event tree for the electrical hazard incident. A work plan was generated for the activity, but was deficient in several respects. The task was categorized as low risk based on considerations of *public health and safety, not risk to the worker*. The work plan was also inadequate in that it did not require a high voltage lockout/tagout to completely de-energize the panel as required by the Management and Operations (M&O) contractor policy and OSHA requirements. The work plan did not identify which protective equipment, if any, was needed for the work and, consequently, did not make any provisions for making the equipment available to the worker. The deficiencies in the work plan were due to human errors.

This category of human errors is considered to have probabilities that lie in the range of 10^{-2} to 10^{-4}. The probability may be an order of magnitude higher if a need exists for systems knowledge or for interpreting indirect information, as existed in this case. The probability of an inadequate work plan was, therefore, taken to be 10^{-1}. After the work plan failed to direct the worker on the need for lockout/tagout and protective equipment, these barriers were as likely to be not implemented as implemented. The conditional probability for a severe injury was, therefore, estimated at $0.1\times0.5\times\ 0.5 = 2.5\times10^{-2}$. Note that this result was obtained by multiplying the probabilities on the branch in Figure 2.5 that corresponds to an inadequate work plan and results in severe injury. The ratio of occurrence of death to disabling injuries in U.S. industries was 1.5×10^{-3} in 1994.[12] The ratio was higher if only incidents with the potential for fatality were considered. For example, for motor vehicle injuries, the ratio was 2.2×10^{-2}. For collisions between motor vehicles and pedestrians, the ratio was 9.2×10^{-2}. Considering that fatal injuries are about an order of magnitude less frequent than severe injuries, the conditional probability of fatality may be estimated at 2.5×10^{-3}, which is also the risk of fatality from the event. With a proper work plan, the likelihood of either of these barriers (lockout/tagout or protective equipment) not being implemented is equal to the nominal human error probability (HEP) of 10^{-2} for this category of errors, and the conditional probability of severe injury is reduced to about 10^{-4}.

Note that in defining this event so far, we have not taken the inadequacy of the work plan as a given. If we define the event as the electrician removing the cabinet enclosure after having been guided by an inadequate work plan, then the risk of fatality for this event is given by 0.5 (likelihood of no lockout being performed) x 0.5 (likelihood of no safety device being used) x 0.1 (death-to-injury ratio) = 2.5×10^{-2}. In the following, we will use this value of the fatality risk from the event.

Figure 2.6 presents the risk of fatality from the event, and compares it to the average lifetime risk of accidental fatality in U.S. industries. Clearly, the risk of fatality from this event is greater than the average lifetime risk of fatality in U.S. industries, and further efforts are needed to reduce this risk. Instead of suggesting specific corrective actions, we make the following general observations regarding the risks associated with this event, and benefits of reducing these risks. This event occurred due to human errors at two levels: (1) errors that led to an inadequate work plan, and (2) the failure on the part of the individual worker to take greater responsibility for his own safety, and use appropriate safety equipment and safe work practices. Implementation of the necessary action to ensure that work plans are developed in accordance with OSHA regulations and take into account worker risks as well as public health and safety concerns is a crucial step in reducing the frequency of similar incidents. Training given to workers to encourage them to take more responsibility for their own safety, and use appropriate safety equipment and safe work practices will also reduce the frequency and consequence of these incidents.

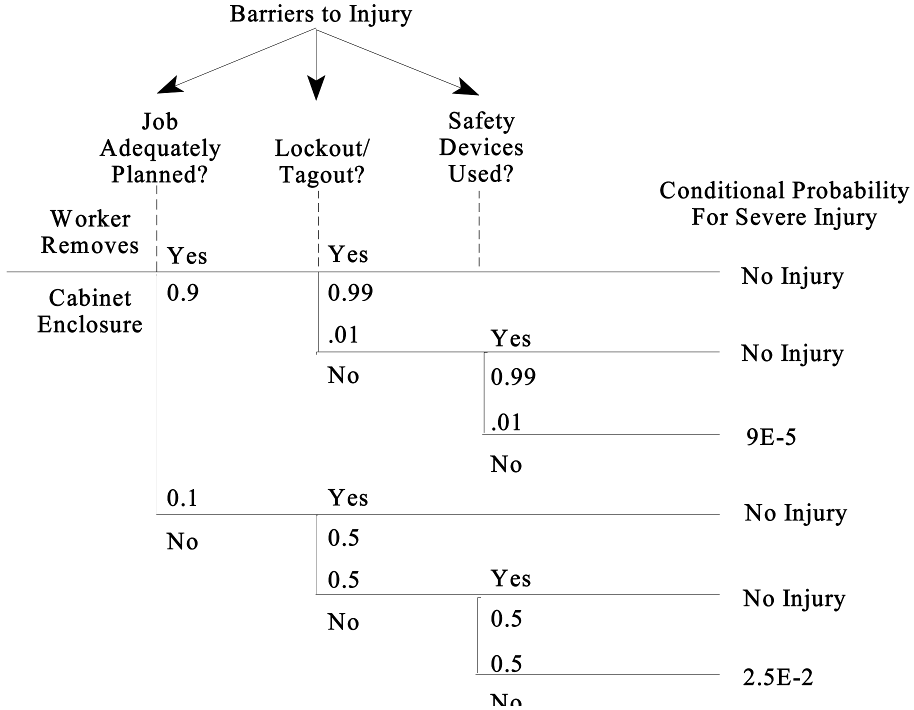


Figure 2.5 Simplified event tree for the electrical hazard incident

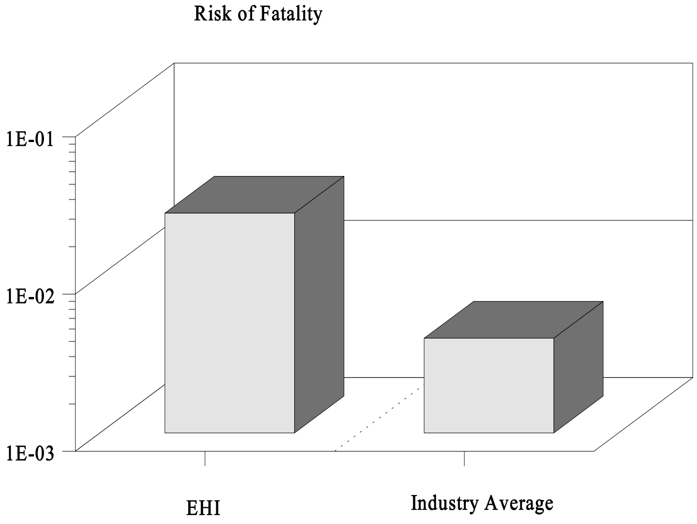


Figure 2.6 Comparison of risk to reference risk for electrical hazard incident

2.7 References

1. “Department of Energy Plan for the Development and Implementation of the Integrated Safety Management Plan,” Department of Energy, Washington, DC 20585, April 18, 1996.

2. “Plutonium Working Group Report on Environmental, Safety and Health Vulnerabilities Associated with the Department’s Plutonium Storage,” U.S. Department of Energy, November 1994 (DOE/EH-0415).

3. “Guidelines for Hazard Evaluation Procedures, “ second edition with worked examples, Center for Chemical Process Safety of the American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017.

4. “Hazards Analysis of the Los Alamos National Laboratory Plutonium Facility (TA-55),” Los Alamos National Laboratory draft report (LA-CP-94-0076), April 1994.

5. “Preliminary Hazards Analysis of the Tank Waste Remediation System (TWRS) Privatization Phase I Conceptual Facilities,” Los Alamos National Laboratory report (LA-CP-95-286), December 1995.

6. J. A. Mahn, G. W. Hannaman, and P. Kryska, “Qualitative Methods for Assessing Risk,” SAND95-0320, May 1995.

7. Safety Notice No. 95-01, “Decision Analysis Techniques,” August 1995.

8. Safety Notice No. 96-02, “Risk-Based Analysis of Electrical Hazard,”May 1996

9. Operating Experience Weekly Summary 95-19, Article 3, “Risk Based Decision Analysis Used for Glovebox Fire Operating Event,” 5-11 May, 1995

10. Operating Experience Weekly Summary 95-42, Article 6, “Risk Based Decision Analysis Applied to an Electrical Hazard Incident,” 13-19 October, 1995

11. “1990 Recommendations of the International Commission on Radiological Protection,” ICRP Publication 60, Pergamon Press, Oxford, England.

12. “Accident Facts - 1995 Edition,” National Safety Council, Itasca, Illinois 60143.

3 DETERMINING FREQUENCIES FROM HISTORICAL DATA

Analysts can use historical data to estimate the frequencies of potential and actual accidents. They can use the data to determine both the frequency of initiating events and the conditional frequencies for barrier failure. The most important sources of this data for DOE are the Occurrence Reporting and Processing System (ORPS) and the Computerized Accident/Incident Reporting System (CAIRS).

Analysts need to consider the following when using ORPS and CAIRS data to determine frequencies:

- ORPS only includes reports that meet certain reporting thresholds. The contractor determines whether a particular near misses meets the reporting threshold, so reporting may not be completely consistent at different sites.

- CAIRS includes information only on accidents the caused injuries and monetary loss.

- Neither ORPS nor CAIRS include information such as the number of work packages performed that would be useful for determining initiating event frequencies.

- The data currently available for normalization is limited to quarterly man-hour data by field office and contractor. Data for specific types of workers would be very useful, and should be available from the Work Force Information System, whichis under development.

- Analysts must use ORPS narrative search techniques with care. Searches that are broad enough to find all of the applicable reports will generally find many reports that are not applicable. Reading and classifying a sample of these reports can be used to determine the underlying frequency.]

The analyst controls only the last point. The suggested method for determining a frequency is as follows.

1. Use a broad narrative search to find all reports that might be applicable.

2. Read a random sample of the reports, classifying them as applicable or inapplicable. There will be more classes if several related frequencies are being determined.

3. Estimate the frequency based on the number of applicable occurrences.

4. Refine the selection criteria to eliminate inapplicable groups of occurrences.

5. Repeat steps 1-3 to determine the revised frequency.

6. Compare the applicable reports in the first sample to the results of the second search. If there are applicable reports that are now excluded, read them to determine how to change the search criteria to include them.

7. Repeat steps 1-6 until the results are satisfactory.

An example of this is to determine the frequencies of electrical shocks, and of possible precursors to electrical shocks. The first search for precursors used the following strategy, labeled Case 1. (ORPS Search Strategies are discussed in Appendix E.)

All Narrative: ELECTRIC@+VOLT@+KV@+(POWER LINE@+CONDUIT@)

This gave 7730 occurrences from the first quarter of 1991 through the second quarter of 1996. A random sample of 100 reports were read, and 10 of them were applicable. This gives an estimated frequency of 0.0992(0.0299 precursor occurrences2 per 200,000 man-hours, based on 1,714,845,735 contractor man-hours over the same period. The criteria used for the other cases is summarized as follows.

Case 2

All Narrative: ELECTRIC@+VOLT@+KV@+(POWER LINE@+CONDUIT@)

Nature of Occurrence: 01B+01E+01F+03A+03C+10B+10C

Case 3

Description of Occurrence: ELECTRIC@+VOLT@+KV@+(POWER LINE@+CONDUIT@)

Nature of Occurrence: 01B+01E+01F+03A+03C+10B+10C

Case 4

Description of Occurrence: SHOCK@+SHORT@+ELECTROCUT@+BURN@+EXPOSE@ +ENERGIZE@

Nature of Occurrence: +03A

Description of Occurrence: ELECTRIC@+VOLT@+KV@+(POWER LINE@+CONDUIT@), -COUNTERF@

Case 5

Description of Occurrence: SHOCK@+SHORT@+ELECTROCUT@+BURN@+EXPOSE@ +ENERGIZE@+SPARK@+FIRE@+DANGER@+LOCKOUT]

Nature of Occurrence: +03A

Description of Occurrence: ELECTRIC@+VOLT@+KV@+(POWER LINE@+CONDUIT@) +RECEPTICLE@,-SUSPECT@

The frequency estimates and standard deviations from these cases is summarized below. (The methodology for estimating the frequency from the number of occurrences, the sample size, and the number of applicable reports is given in Appendix D, along with some other useful statistical methods.)

	Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 5**
Occurrences	7730	4135	2262	1071	1628
Sample Size	100	100	94	100	100
Applicable Reports	10	21	28	52	43
Estimated Frequency	0.0992	0.01061	0.0814	0.0662	0.0835
Standard Deviation	0.0299	0.0226	0.0151	0.0091	0.0126

Seven of the applicable sampled reports in Case 5 were not found in Case 2. This can be considered a sub-case of Case 2, based on the occurrences in Case 2 not included in Case 5. When these are taken into account with the results of Case 5, the final frequency is 0.122±0.019 per 200,000 man-hours.

For the number of shocks, the criteria for Case 5 were used along with an additional criterion.

Description of Occurrence: SHOCK@

This search resulted in 168 reports. A sample of 100 of these found that 72 actually resulted in a shock. The frequency of electric shocks is .0143±0.0017 per 200,000 man-hours. Combining these results statistically, the conditional frequency of an electric shock is 0.117±0.022, given that an electric hazard exists.

This methodology can be used to estimate the frequencies of most types of occurrences that depend on the amount of work done. Some types of occurrences, such as weather phenomena, failed surveillances, and security concerns are not dependent on man-hours. Rates for these types of occurrences should be computed on an annual basis instead.

Analysts need to recognize the data limitations mentioned earlier. Because serious occurrences are always recorded, while minor ones are sometimes below the reporting threshold, frequencies will generally be more reliable for more serious types of occurrences. Normalization by total man-hours is not completely appropriate for some types of occurrence. Within these limitations, frequencies derived from historical data can be useful tools for analyzing workplace hazards.

APPENDIX A

BARRIER RELIABILITY

APPENDIX A

BARRIER RELIABILITY

The potential for harm from any accident lies not only in the severity of the hazard(s), but also in the effectiveness of any barriers constructed to protect individuals. Barriers against hazards may take a variety of forms. Procedures, training, human action, as well as, systems and components that prevent accidents or provide mitigation of consequences can constitute barriers against injury. Because of their nature, barriers can have variable reliability and effectiveness. For example, training electrical workers in safe work practices can constitute a useful barrier against injury. However, such general training is probably less effective than executing a specific precautionary measure such as de-energizing the electrical circuit. Risks from rigging and hoisting accidents can be reduced by establishing exclusion zones around the area of operation. The effectiveness of that barrier depends on the size, weight, and geometry of the item being moved in addition to the height that it needs to be hoisted. If the exclusion zone is inadequate for the particular job, the item, if dropped, may bounce, roll, or slide farther than expected, reducing the effectiveness of the barrier. Barrier failure could include: human error, failure to follow instructions; compromised shielding; failure of warning devices; or failure of protective equipment (for example, the exhaust fans from a chemical hood could fail).

Unlike human factors, the loss of reliability of engineered components (such as electronic components or other equipment) can be caused by a failure of the entire system, or through the failure of individual components that make up the system. An example could be a failure of a warning light that indicates the operation of a radiation source: an x-ray tube, an accelerator, or a gamma source. A failure of this system could be due to a burned out lamp, a failed circuit component, or a failed sensor/switch. Such a failure could result in radiation exposure since no warning was available to identify the radiation source. For these hazards, the system failure rate can usually be approximated by the sum of all component failure rates, assuming the component failure rates are small. If the system has a redundancy, the overall system failure rate is lowered.

In the development of generic tables for failure rates of components and systems, the data included can be gathered from field experience and from sample testing. Field experience relates to the failure rate data from equipment in use and sample testing data are obtained from set numbers of systems and components tested specifically for reliability. In using point estimates of failure rate, the analyst must realize two important facts about the tabulated failure data. First, the device’s failure is a statistical phenomenon occurring within the expected range of device’s useful operation life. This expected range cannot be all inclusive for all failures and some isolated devices may fail faster or slower than their expected failure rate. The value used by the analyst is a single point representing the entire distribution. Second, the use of the equipment being analyzed may not be similar to the use of the equipment that provided information for the data base.

Another aspect in defining the equipment failure rates is the “life” of the equipment, and when in the equipment’s “life” it is being used. Since most production, test, or assembly problems arise shortly after the equipment is put into use, the expected failure rate for a new component is higher than one operating during its expected “useful life”. If equipment is being used in the end-of-life or wear-out phase, it will likewise have higher failure rates. These aspects should be accounted for in the analyses.

In developing a generic tabulation for accident analyses, one must first consider not only barriers that were or should have been constructed, but also equipment in use at the time of the accident. A rigging accident could have various causes starting from human error: improper inspection of the equipment, improper inspection of the item being moved, error in operation such as pushing the incorrect button or failing to stop. Other causes of accidents could be equipment malfunction: failure of a mechanical switch, failure of a limit switch, failure of an eye bolt, broken sling. Once an accident has occurred, the analyst needs to consider the effectiveness of the barriers in place: Was an exclusion zone erected? Was the exclusion zone appropriate for the job? Were any shields erected to stop any falling item? Many of the accidents that analysts will be considering will include failures of simple devices and not necessarily large systems. Therefore, one might require searching tabulations that include failure rates of components and not merely of larger integrated systems.

Barriers can be divided into two major schemes, depending on the size and complexity of the barriers. The divisions are “components” and “systems”. In complicated barriers, the system is made up of several components. Analyzing these failures may not require considering the robustness of each individual component. However, for simple systems the failures (and hence types of failures and potential severity of failures) may require consideration of components. In crane operations, the failure can be from an eye-bolt or sling that is holding the item being moved. Other potential failures could be the failure of a limit switch, power switch, or the crane anchoring. Each failure will result in different consequences.

Sources of Tabulated Failure Data

The data provided here was accumulated from several sources. Because of the variability of the data, recommended values will be provided in tables of this appendix. There are several reasons for variability in the data. The reasons include statistical nature of failure, quality of original manufacture, quality of maintenance, and the environment in which the equipment is used. The references include: Green and

Bourne,[1] Henley and Kumamoto,[2] Dhillon.[3] The data in Henley and Kumamoto utilize heavily English data from Anyakora, et al.[4] Failure rates for generic systems were taken from Mahn, et al.[5] Other sources of specific failure rates include: Blanton and Eide,[6] Eide, et al.,[7] Cadwallader and Sanchez,[3] and DOE/EP-0052.[9]

At times the analyst will be faced with deciding which data set to use. An example of differences between data sets was shown in WASH-1400[10] which showed failure rate data from both the U.S. nuclear industry and general U.S. industry. When faced with choosing which data set to rely on, the analyst should determine which data set's operating conditions are most similar to the facility being analyzed. One industry can have more extreme conditions than another, but also may have different manufacture and maintenance criteria.

Use of Tabulated Data

There are two ways that the data are presented. First, for equipment that operates continuously, the failure frequency is quoted per unit time (usually per hour or per year). Second, for equipment that is operated periodically and for shorter lengths of time, the failure frequency is quoted as a failure per demand. The expected failure rate (per year) would then include the expected number of demands per year. For safety systems (such as a ventilation system) or components in a standby state which must start and operate for a specified time for success, the failure rate is the sum of the demand (fails to start) rate and the operating (fails to run) rate.

For a particular device, system or facility, "stock" data from tables may not be appropriate for the particular analyses being performed. If sufficient data exist, then failure data for that particular system can be constructed. If n is the number of failures and T is the time interval covering the n failures, the (mean) failure rate is given by:

$$\text{mean} = (2n + 1)/(2T).$$

If after the time, T, no failures have occurred, the mean failure is taken as the inverse of twice the lapsed time interval. One convenient factor that is commonly reported is the error factor (EF), which is defined as the expected ratio of the 95th percentile to the 50th percentile (or the median). For a lognormal distribution, the relationship between the mean and median is then:

$$\text{mean} = \text{median } \{\exp\ (0.5[(1\text{n(EF)})/1.645]^2)\}$$

As time proceeds, and new data become available, the analyst may need to update the already established failure rate tables using, for example, a Bayesian update procedure.

Tabulations

If the analyst requires data more detailed than the generic screening data of Tables 2.3, 2.4, and 2.5, other sources need to be considered. Table A.1 is a table of recommended point estimates for failure rates per hour for general U.S. industry, and assumes the device is operating or functioning on a regular basis. Table A.2 provides recommended point estimates for failure rates per demand for the general U.S. industry, and is the expected frequency of failures per action (such as a startup).

Some data specifically related to DOE operations have been compiled and reanalyzed over time as they relate to specific operations. In this section, some of this data is tabulated and presented. In Table A.3 data related to glove-box type accidents at TA-55 at LANL are presented. These data were presented as part of the analyses for the TA-55 FSAR and include compilations of older DOE data combined with updated TA-55 data[11] Tables A.4, A.5, and A.6 provide other data obtained from the LANL TA-55 FSAR.[12]

The data presented in the Tables A.1 and A.2 are point estimates of data selected from a variety of sources. On only a few occasions did the data differ significantly between sources. In the cases where only ranges were provided, point estimates were determined by averaging the logarithms of the bounding data. Tables showing ranges of failure probabilities and comparisons of point estimates are presented in Tables A.7 - A.9.

References

1. A. E. Green and A. J. Bourne, Reliability Technology, J. Wiley and Sons, Chichester, U.K., 1972.

2. E. J. Henley and H. Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.

3. B. S. Dhillon, Mechanical Reliability: Theory, Models and Applications, American Institute of Aeronautics and Astronautics, Inc., Washington, D.C. 1988.

4. S. N. Anyakora, G. F. M. Engel, and F. P. Lees, *Chem. Engr.* (London) 225, 396, 1971.

5. J. A. Mahn, G. W. Hannaman, and P. Kryska, “Qualitative Methods for Assessing Risk,” SAND95-0320, May 1995.

6. C. H. Blanton and S. A. Eide, “Savannah River Site Generic Data Base Development,” WCRC-TR-93-262, June 30, 1993.

7. S. A. Eide, S. V. Chmilelwski, and T. D. Swantz, “Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs,” EGG-SSRE-8875, February 1990.

8. L. C. Cadwallader, and D. P. Sanchez, “Secondary Containment System Component Failure Data Analysis from 1984 to 1991,” EGG-FSP-l0343, August 1992.

9. DOE, “Automatic-Sprinkler-System Performance and Reliability in U.S. DOE Facilities 1952-1980,” DOE/EP-0052, June 1982.

10. U.S. Nuclear Regulatory Commission, “Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants,” Appendix 3 and 4: Failure Data, WASH-1400, 1975.

11. S. A. Eide, Memorandum to D. Gordon, LANL, “Scenario Descriptions and Frequency Estimates for TA-55 FSAR - SAEI 1794,” dated September 30, 1994.

12. SAIC, “TA-55 Final Safety Analysis Report,” April 11, 1991.

Table A.1 Recommended hourly failure rates for electrical and electro-mechanical equipment, based on U.S. industry averages

		Failure frequency (hr^{-1})
Parts	Wrapped joints	1E-10
	Machine soldered joints	1E-9
	Crimped and welded joints	5E-9
	Hand soldered joints	5E-8
	Semiconductors, microelectronic circuits	2E-7
	Discrete electronic parts	3E-8
	Indicator lamps	5E-6
	Electro-mechanical parts	2E-6
	Electronic valves	2E-5
	Indicator (moving coil) meter	3E-6
	Pneumatic relay	2E-5
	Electrical relay	2E-6
	Relay - fail of NO contact to close	3E-7
	Relay - short across NO/NC contact	1E-8
	Relay - open NC contact	1E-7
	Switch - contacts short	1E-7
	Circuit breakers - premature transfer	1E-6
	Fuses - premature open	1E-6
	Wires - open	3E-6
	Wires: short to GND	3E-7
	Wires: short to PWR	1E-8
	Transformers: open CKT	1E-6
	Transformers: short	1E-6
Equipment	Ion chamber sensor	5E-6
	Thermocouple sensor	1E-5
	Circuit breakers (<33 kV)	2E-6
	Circuit breakers (<132 kV)	4E-6
	Circuit breakers (<275 kV)	7E-6
	Circuit breakers (<400 kV)	1E-5

Table A.1 (continued)

		Failure frequency (hr^{-1})
Equipment (cont.)	Distr. transformers (<15 kV)	6E-7
	Distr. transformers (15-33 kV)	2E-6
	Distr. transformers (33-132 kV)	4E-6
	Distr. transformers (132-400 kV)	7E-6
	Generators, a.c.	7E-6
	Generators, d.c.	9E-6
	Motors, induction > 200 kW	1E-5
	Electric motors, fail to run	7E-6
	Motors, induction < 200 kW	5E-6
	Motors, synchronous	7E-6
	Motors, small, general	4E-6
	Motors, stepper	5E-6
	Transistor equipments	5E-5
	Large electrical machines	4E-5
	Pumps, circulators	6E-5
	Pumps, fail to run	3E-5
	Electronic valve equipment	3E-4
	Pneumatic controller	4E-3
	Strip chart recorder	3E-5
	General instruments; fail to operate	4E-6
	Battery power supply	8E-5
Systems	General instrumentation - fail to operate	1E-6
	General instrumentation - shift calibration	3E-5
	Large electronic systems (no redundancy)	4E-3
	Large electronic systems (with redundancy)	6E-5
	Automatic protective systems (with redundancy and diversity)	6E-8

Table A.2 Mechanical component failure rates based on U.S. industry averages

Component	Point estimate (hr^{-1})
Ball bearings, heavy duty	2E-5
Ball bearings, light duty	1E-5
Roller, sleeve bearings	5E-6
Heavily stressed shafts	2E-7
Lightly stressed shafts	2E-8
Pins	1.5E-5
Pivots	1E-6
Couplings	5E-6
Belt drives	4E-5
Conveyor belts: light load	8E-6
Conveyor belts: heavy load	5E-5
Spur gears	1E-5
Helical gears	1E-6
Friction clutches	3E-6
Friction clutch fail to open	3E-7
Mechanical parts, general	4E-7
Pneumatic and hydraulic parts	4E-6
Electric clutch premature open	1E-6
Magnetic clutches	6E-6
Heavily stressed springs	1E-6
Lightly stressed springs	2E-7
Hair springs	1E-6
Vibration mounts	2E-6
Mechanical joints	2E-7
Grub screws	5E-7
Nuts and bolts	2E-8
Washers	5E-7
Hinges	3E-7
Pulleys, idler	6E-8
Rivets	1E-7

Table A.2 (continued)

Component	Point estimate (hr^{-1})
Inset locks	1E-5
Rack-and-pinion assemblies	2E-6
Knife-edge fulcrums	1E-5
Bellows	5E-6
Metal diaphragms	5E-6
Rubber diaphragms	8E-6
Gaskets	5E-7
Rotating seals	7E-6
Sliding seals	3E-6
‘O’ ring seals	2E-7
Filters, leakage and blockage	1E-6
Heavily stressed hoses	4E-5
Lightly stressed hoses	4E-6
Ducts	1E-6
General pressure vessels	3E-6
High standard pressure vessels	3E-7
Relief valves, blockage	5E-5
Relief valves, leakage	2E-6
Hand-operated valves	1.5E-5
Ball valves	5E-7
Solenoid valves	3E-5
Control valves	3E-5
Pistons	1E-6
Cylinders	1E-7
Jacks	5E-7
Pressure gauges	1E-5
Pressure switches	2E-5
Nozzle and flapper assemblies, blockage	6E-6

Table A.2 (continued)

Component	Point estimate (hr^{-1})
Nozzle and flapper assemblies, breakage	2E-7
Liquid flow measurement	1E-4
Solid flow measurement	5E-4
Liquid level measurement	2E-4
Solid level measurement	8E-4
Temperature measurement (no pyrometer)	4E-5
Radiation pyrometer	3E-5
Optical pyrometer	1E-3
Flow switch	1E-4
MOV, AOV, check valve - external leak/rupture	1E-8
Valves - general	1E-5
Pneumatic equipment	2E-4
Boilers, condensers	1E-7
Check valve - rev. leak	3E-7
Relief valve - premature open	1E-5
Pipes	2E-7
Pipes > 3"	2E-8
Pipes < 3"	1E-7
Pipe joints	5E-7
Unions and junctions	4E-7
Gaskets - leak	3E-6
Flanges, closures, elbows - leak	3E-7
Welds - leak	3E-9
Welded fittings	7E-8
Mechanical break assemblies	5E-6
Pneumatic or hydraulic break assemblies	3E-6

Table A.3 TA-55 data from 1991 FSAR - Ash Leach Criticality Accident

System	Failure probability (hr^{-1})
Break in Pu solution transfer line	1E-2
Leaking Pu handling equipment	
From overpressurization	5E-3
Valve, flange, gasket	3E-3
From corrosion/cracking	2E-3
Failure of manually actuated ball valve (fails open)	1E-3
Failure of manually actuated ball valve (Fails open with full flow)	5E-4
Glove box foot pedal valve	
Fails open	1E-3
Controller broken with valve in open position	5E-2
Fails open (time dependent)	1.0E-4
Closure mechanism fails - valve fails open (time dependent)	5E-4
Closure mechanism breaks	1E-3
Hot plate rheostat fails leaving plate on	1E-3
House LTA off-gas	
Degraded tubing attachment	4.6E-4
Off-gas system plugged	4.6E-4
Condenser plugged	1.1E-4
House vacuum down	2.3E-4
Plugged tubing	5.1E-4

Table A.4 TA-55 data from 1991 FSAR - Anion Exchange Column

System	Failure probability (hr^{-1})
Pressure relief valve plugged	1E-3
Pressure relief valve fails to relieve pressure	1E-4
Pressure regulator valve failure (results in overpressurization)	5.5E-5
Pressure gauge fails and reads low	1E-3
Gamma monitor failure	1.14E-4
AEx GB fire	2.3E-5
Eluant or nitric acid feed equipment failure	1E-3
AEx column leaks	
Piping	1E-3
Bottom valve	1E-3
Tygon tubing	1E-2
Tygon tubing connector	5E-2
Flange/Gasket	5E-2
House LTA off-gas	
Degraded tubing attachment	4.6E-4
Off-gas system plugged	4.6E-4
Condenser plugged	1.1E-4
House vacuum down	2.3E-4
Plugged tubing	5.1E-4

Table A.5 TA-55 data from 1991 FSAR - Waste Evaporator Red Oil Explosion

System	Failure probability (hr^{-1})
Interlock failure	1E-3
Steam PRC fails	4.4E-4 - 1E-2
Loss of vent vacuum	1E-2
Steam “pop-off” valve failed closed	1E-1
PRV fails open	6.8E-5
Vent relief fails	1E-1
PRV fails open − psig available	1E-2
High temperature interlock fails	2E-4
Scrubber recirculator ramp fails	1E-2
Scrubber recirculator pump fails	3E-2

Table A.6 TSTA Glovebox Failure Data from Ca92

Failure mode	Point estimate	95% upper bound
Glovebox overpressure	0.3/gb-yr	0.4
Glovebox underpressure	0.2/gb-yr	0.3
Glovebox continuous purging	0.04/gb-yr	0.1
Air inleakage events	0.1/gb-yr	0.5
Small, external tritium release events	0.04/gb-yr	0.1
Solenoid purge valve fails to close on demand	6E-6/demand	3.0E-5
Oxygen monitor fails	0.5/monitor-yr	1
Overall glove breaches	0.05/gb-yr	0.6
Breach on rim	0.02/gb-yr	.03
Pin hole lead	0.01/gb-yr	.02
Puncture	0.003/gb-yr	.008
Abrasion wearout	0.0009/gb-yr	.016
Cuts and tears	0.003/gb-yr	.008
Fires, explosions or severe overpressure (none in 79 gb-yrs)	3E-3/gb-yr	
Tritium release from gb due to internal tritium leak	5E-3/demand	
Accidental release during container loading/unloading operation	2E-2/operation	

Table A.7 Typical ranges of failure rates for electrical and mechanical parts, equipment, and systems

	Failure-rate range (hr^{-1})	Point estimate (hr^{-1})[a]	Point estimate (hr^{-1})[b]	Point estimate (hr^{-1})[c]	Point estimate (hr^{-1})[d]
Wrapped joints	1E-11 - 1E-9	1E-10			
Machine soldered joints	5E-10 - 1E-8	1E-9			
Crimped and welded joints	1E-10 - E-7	5E-9			
Hand soldered joints	5E-9 - 5E-7	5E-8			
Semiconductors, microelectronic circuits	2E-9 - 2E-6	2E-7			
Discrete electronic parts	5E-10 - 2E-6				
Indicator lamps		5E-6	5E-6		
Electro-mechanical parts	1E-7 - 5E-5				
Electronic valves	1E-6 - 1E-4	2E-5			
Indicator (moving coil) meter	5E-7 - 2E-5 (Dh)	3E-6			
Pneumatic relay			2E-5		
Electrical relay			2E-6		
Relay - fail of NO contact to close	1E-7 - 1E-6			3E-7	
Relay - short across NO/NC contact	1E-9 - 1E-7			1E-8	
Relay - open NC contact	3E-8 - 3E-7			1E-7	
Switch - contacts short	1E-8 - 1E-6			1E-7	
Circuit breakers - premature transfer	3E-7 - 3E-6			1E-6	
Fuses - premature open	3E-7 - 3E-6			1E-6	
Wires - open	1E-6 - 1E-5			3E-6	
Wires: Short to GND	3E-8 - 3E-6			3E-7	
Wires: Short to PWR	1E-9 - 1E-7			1E-8	
Transformers: Open CKT	3E-7 - 3E-6			1E-6	
Transformers: Short	3E-7 - 3E-6			1E-6	
Ion chamber sensor		5E-6			
Thermocouple sensor		1E-5			

Table A.7 (continued)

	Failure-rate range (hr^{-1})	**Point estimate (hr^{-1})[a]**	**Point estimate (hr^{-1})[b]**	**Point estimate (hr^{-1})[c]**	**Point estimate (hr^{-1})[d]**
Circuit breakers (<33 kV)	5E-7 - 1E-5	2E-6			
Circuit breakers (<132 kV)		4E-6			
Circuit breakers (<275 kV)		7E-6			
Circuit breakers (<400 kV)		1E-5			
Distr. Transformers (<15 kV)	2E-8 - 2E-5	6E-7			
Distr. Transformers (15-33 kV)		2E-6			
Distr. Transformers (33-132 kV)		4E-6			
Distr. Transformers (132-400 kV)		7E-6			
Generators, a.c.		7E-6			
Generators, d.c.		9E-6			
Motors, induction >200 kW		1E-5			
Electric motors - fail to run (nuclear industry)	3E-6 - 3E-5			1E-5	1E-5
Electric motors - fail to run (U.S. industry)	5E-7 - 1E-4				
Motors, induction <200 kW		5E-6			
Motors, synchronous		7E-6			
Motors, small, general		4E-6			
Motors, stepper		5E-6	5E-6	5E-6	
Transistor equipment	6E-6 - 5E-4				
Large electrical machines	2E-6 - 7E-4				
Pumps, circulators	2E-6 - 1E-3				6E-5
Pumps, fail to run	3E-6 - 3E-4			3E-5	
Electronic valve equipment	2E-5 - 5E-3				
Pneumatic controller		4.3E-5			
Strip chart recorder		2.5E-5			
General instruments (nuclear industry)	1 E-7 - 1E-5		1E-6		

Table A-7 (continued)

	Failure-rate range (hr^{-1})	**Point estimate (hr^{-1})[a]**	**Point estimate (hr^{-1})[b]**	**Point estimate (hr^{-1})[c]**	**Point estimate (hr^{-1})[d]**
General instruments (U.S. industry)	3E-7 - 6E-5		4E-6		
Battery power supply (I)	6E-6 - 1E-3		8E-5		
Battery power supply (N)	1E-6 - 1E-5			3E-6	
Large Electronic systems (no redundancy)	1E-3 - 2E-2				
Large electronic systems (with redundancy)	2E-6 - 2E-3				
Automatic protective systems (with redundancy and diversity)	5E-9 - 7E-7				

[a] From Green and Bourne

[b] E. J. Heneley and H. Kumamoto, **Reliability Engineering and Assessment**, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.

[c] From WASH-1400

[d] From B. D. Dhillon, **Mechanical Reliability: Theory, Models and Applications**, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, 1988.

Table A.7 (continued)

Table A.8 Mechanical component failure rates

	Failure-rate range (hr^{-1})	Point estimate (hr^{-1})[a]	Point estimate (hr^{-1})[b]	Point estimate (hr^{-1})[c]	Point estimate (hr^{-1})[d]
Ball bearings, heavy duty		2E-5			2E-5
Ball bearings, light duty		1E-5			1E-5
Roller, sleeve bearings	8E-9 - 7E-6 (d)	5E-6			
Heavily stressed shafts		2E-7			2E-7
Lightly stressed shafts		2E-8			
Pins		1.5E-5			
Pivots		1E-6			1E-6
Couplings		5E-6			
Belt drives		4E-5			
Conveyor belts: light load	4E-6 - 2E-5 (d)				
Conveyor belts: heavy load	2E-5 - 1.4E-4 (d)				
Spur gears		1E-5			1E-5
Helical gears		1E-6			1E-6
Friction clutches		3E-6			
Friction clutch fail to open	3E-8 - 3E-6			3E-7	
Mechanical parts	1E-8 - 2E-5				
Pneumatic and hydraulic parts	2E-7 - 1E-4				
Electric clutch premature open	1E-7 - 1E-5			1E-6	
Magnetic clutches		6E-6			
Heavily stressed springs		1E-6			
Lightly stressed springs		2E-7			
Hair springs		1E-6			1E-6
Vibration mounts		2E-6			
Mechanical joints		2E-7			2E-7
Grub screws		5E-7			

Table A.8 (continued)

	Failure-rate range (hr^{-1})	Point estimate (hr^{-1})[a]	Point estimate (hr^{-1})[b]	Point estimate (hr^{-1})[c]	Point estimate (hr^{-1})[d]
Nuts and bolts		2E-8			2E-8
Washers					5E-7
Hinges	2E-8 - 6E-6 (d)				
Pulleys, idler	3E-8 - 2E-7 (d)				
Rivets	1E-8 - 2E-6 (d)				
Inset locks	4E-6 - 3E-5 (d)				
Rack-and-pinion assemblies		2E-6			
Knife-edge fulcrums		1E-5			
Bellows		5E-6			5E-6
Metal diaphragms		5E-6			
Rubber diaphragms		8E-6			
Gaskets		5E-7			5E-7
Rotating seals		7E-6			4E-6
Sliding seals		3E-6	3E-6		
‘O’ ring seals		2E-7			2E-7
Filters, leakage and blockage		1E-6			1E-6
Heavily stressed hoses		4E-5			
Lightly stressed hoses		4E-6			
Ducts		1E-6			1E-6
General pressure vessels		3E-6			
High standard pressure vessels		3E-7			
Relief valves, blockage	5E-7 - E-5 (d)	5E-5	3E-6		
Relief valves, leakage		2E-6			
Hand-operated valves		1.5E-5	1.5E-5		
Ball valves		5E-7			5E-7
Solenoid valves	7E-7 - 3E-5 (d)	3E-5	3E-5 (-5E-5)		
Control valves		3E-5	3E-5 (-7E-5)		

Table A.8 (continued)

	Failure-rate range (hr^{-1})	Point estimate (hr^{-1})[a]	Point estimate (hr^{-1})[b]	Point estimate (hr^{-1})[c]	Point estimate (hr^{-1})[d]
Pistons		1E-6			1E-6
Cylinders		1E-7			1E-7
Jacks		5E-7			
Pressure gauges		1E-5	1E-5 (-1.6E-4)		
Pressure switches		1.5E-5	1.6E-5 (4E-5)		
Nozzle and flapper assemblies, blockage		6E-6			
Nozzle and flapper assemblies, breakage		2E-7			
Liquid flow measurement			(1.3E-4)		
Solid flow measurement			(5E-4)		
Liquid level measurement			(2E-4)		
Solid level measurement			(8E-4)		
Temperature measurement (no pyrometer)			(4E-5)		
Radiation pyrometer			(2.5E-4)		
Optical pyrometer			1.1E-3		
Flow switch			(1.3E-4)		
MOV, AOV, Vacuum, check valve - external leak/rupture					
Valves - general					1E-5
Pneumatic equipment	5E-6 - 7E-3				
Boilers, condensers	2E-7 - 1E-7				
Check valve - rev. leak	1E-7 - 1E-6			3E-7	
Relief valve - premature open	3E-6 - 3E-5			1E-5	
Pipes		2E-7			2E-7
Pipes >3" (industry)	1E-10 - 5E-6				

Table A.8 (continued)

	Failure-rate range (hr^{-1})	Point estimate (hr^{-1})[a]	Point estimate (hr^{-1})[b]	Point estimate (hr^{-1})[c]	Point estimate (hr^{-1})[d]
Pipes <3" (industry)	2E-9 - 5E-6				
Pipe joints		5E-7			5E-7
Unions and junctions		4E-7			
Mechanical equipment	5E-6 - 5E-4				
Pipe >3", rupture (nuclear industry)	3E-12 - 3E-9			1E-10	
Pipe <3", rupture (nuclear industry)	3E-11 - 3E-8			1E-9	
Gaskets - leak	1E-7 - 1E-4			3E-6	
Flanges, closures, elbows - leak	1E-8 - 1E-5			3E-7	6E-6
Welds - leak	1E-10 - 1E-7			3E-9	
Welded fittings	1E-8 - 5E-7 (d)				
General instrumentation - fail to operate	1E-7 - 1E-5			1E-6	
General instrumentation - Shift calibration	3E-6 - 3E-4			3E-5	
Mechanical break assemblies	3E-6 - 8E-6 (d)				
Pneumatic or hydraulic break assemblies	8E-8 - 1E-4 (d)				

[a] From Green and Bourne

[b] E. J. Heneley and H. Kumamoto, **Reliability Engineering and Assessment**, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.

[c] From WASH-1400

[d] From B. D. Dhillon, **Mechanical Reliability: Theory, Models and Applications**, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, 1988.

Table A.9 Instrument failure rates per demand

Instrument	Failure	Range of Failure Rate[a] (per demand)	Failure rate (per demand)[a]	Point estimate (hr^{-1})[b]
Motor operated valves	Failure to operate	2E-4 - 7E-2	1E-3	
Motor operated valves	Plug	6E-5 - 3E-4	3E-5	
Solenoid operated valves	Failure to operate	2E-5 - 6.5E-3	1E-3	
Solenoid operated valves	Plug		3E-5	
Air operated valves	Failure to operate	1E-6 - 2E-2	1E-4	
Air operated valves	Plug		3E-5	
Check valves	Failure to open	2E-5 - 3E-4	1E-4	
		3E-5 - 3E-4		1E-4
Relief valves	Failure to open	1.4E-5 - 3.6E-5	1E-5	
Manual valves	Plug	3E-4 - 3E-6	3E-5	
		3E-5 - 3E-4		1E-4
MOV valves	Plug	3E-4 - 3E-3		1E-3
MOV valves	Open	3E-5 - 3E-4		1E-4
SOV valves	Fail to open	3E-4 - 3E-3		1E-3
AOV valves	Plug	1E-4 - 1E-3		3E-4
AOV valves	Open	3E-5 - 3E-4		1E-4
Vacuum valves	Fail to open	1E-5 - 1E-4		3E-5
Pressure switch	Failure to operate	5E-5 - 1E-3	1E-4	
Pressure and torque switch	Failure to operate	3E-5 - 3E-4		1E-4
Limit switch	Failure to operate	1E-5 - 7E-4	1E-4	
		1E-4 - 1E-3		3E-4
Manual switch	Fail to transfer	3E-6 - 3E-5		1E-5
Relay	Fail to energize	3E-5 - 3E-4		1E-4
Electric motors	Fail to start	1E-4 - 1E-3		3E-4
Friction clutch	Fail to operate	1E-4 - 1E-3		3E-4
Electric clutch	Fail to operate	1E-4 - 1E-3		3E-4
Circuit breaker	Fail to open	3E-4 - 3E-3		1E-3
Fuses	Fail to open	3E-6 - 3E-5		1E-5
Relief valves	Fail to open	3E-6 - 3E-5		1E-5
Pumps	Fail to start	5E-5 - 5E-3©		

[a] From Heneley
[b] From WASH-1400

APPENDIX B

HUMAN ERROR PROBABILITIES

APPENDIX B

HUMAN ERROR PROBABILITIES

The first sets of data in this section will be for the frequencies of human errors constituting general operational errors. For many screening analyses, these general error rates are probably adequate and are simple to utilize. The errors related to more specific tasks will be provided later in this section. The general error rates are interesting from a perspective view since they provide a quantitative measure of the importance of worker training.

The development of a generic set of failure probabilities for human error is extremely difficult since there is a strong correlation on the actual person performing the task, complexity of the task, the time required for task completion, and the training level of the person performing the task. Additionally a worker may perform any specific task differently depending on the level of alertness due to fatigue or other factors. A relatively simple model has been developed by J. Rasmussen[1,2] to quantify human error rates based on the level of training. This model divides the behavior into three basic categories, skill-based, rule-based, and knowledge-based behaviors.

> Skill-based behaviors depend mostly on the operator's practice in performing the task. The operator can perform the task without ambiguity.
>
> Rule-based behavior is at work when the operator does not have the same level of practice at performing the required task, but has a clear knowledge of the procedures. There may be some hesitation in recalling any procedure, the procedure may not be carried out in the proper sequence, or any step may not be performed precisely.
>
> The final behavioral action is defined as knowledge-based action. This would include situations where the operator needs to contemplate the situation, interpret information or make a difficult decision. Also included in this grouping would be cases where a procedure is not well spelled out. In these cases the person performing the task must consider the actions to be taken and not act according to specific training.

Rasmussen provides per demand ranges and point estimates for these different categories. These values are presented in Table B. 1. Swain and Guttmann[3] suggest for screening purposes, 0.05 and 1 for the Rule-Based and Knowledge-Based actions. However a value of 1 means 100% error rate for the Knowledge-Based action, a value that would appear to be unrealistically high.

One problem with the Rasmussen data is that it requires subjective analysis of the operator's training and capabilities. A set of human error rates were developed by D. M. Hunns[4] for more specific tasks, not relying as much on the operator's capabilities and knowledge. These data are presented in Table B.2 and were based on extrapolation from human error rate data bases. These data are similar to the rates of Rasmussen, Table B. 1, but provide some actual examples and do not require as much subjective analysis as the Rasmussen data.

The human error rates for some specific tasks have been provided by Dhillon[5] and are presented in Table B.3. Dhillon points out that there are six basic categories of error sources that can eventually lead to an accident condition:

1. operating errors
2. assembly errors
3. design errors
4. inspection errors
5. installation errors
6. maintenance errors

Operating errors can be the result of:

1. Lack of proper procedures
2. Task complexity and overload (of operator) conditions
3. Poor personnel selection and training
4. Operator carelessness and lack of interest
5. Poor environmental conditions
6. Departure from following correct operating procedures

According to McCornack[6] the error rate for inspections is approximately 15%.

An example of human error rates from a single facility has been developed for the nonnuclear reactor operations at the Savannah River Site.[7] Some of these data are presented in Table B.4. This particular tabulation includes not only single human performances, but provides ranges based on extenuating circumstances. Also this table provides the error factor, which is the ratio between the 95th and 50th percentiles.

The final source of human error that we will consider is older data from the Reactor Safety Study: WASH-1400.[8] Part of this study included error rates for different operator functions, and when operators were under different levels of stress. This data is provided in Table B.5.

References

1. J. Rasmussen, "On the Structure of Knowledge - A Morphology of Mental Models in a Man Machine Context," RIS-M-2192, 1979.

2. J. Rasmussen, "Models of Mental Strategies in Process Plant Diagnosis," in Human Detection and Diagnosis of Systems Failures, J. Rasmussen and W. B. Rouse (Eds.), Plenum Press, New York, 1981, pp. 241-258.

3. A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August 1983.

4. D. M. Hunns, "Discussions around a Human Factors Data-Base. An Interim Solution: The Method of Paired Comparisons," Section 1.6.3 of High Risk Safety Technology, A. E. Green, ed., J. Wiley and Sons, Ltd., Chichester, U.K., 1982.

5. B. S. Dhillon, Human Reliability with Human Factors, Pergamon Press, Inc. New York, 1986.

6. R. L. McCornack, "Inspector Accuracy: A Study of the Literature," Sandia Corporation Report, SCTM 55-61, (1961).

7. H. C. Benhardt, S. A. Eide, J. E. Held, L. M. Olsen, and R. E. Vail, "Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities," WSRC-TR-93-581, February 28, 1994.

8. "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants; Appendices 3 and 4 Failure Data," WASH-1400, U.S. NRC, October 1975.

Table B.1 Error rates of Rasmussen

	Per demand error rate range	Per demand error rate point estimate
Skill-based	5E-5 to 5E-3	1E-3
Rule-based	5E-4 to 5E-2	1E-2
Knowledge-based	5E-3 to 5E-1	lE-1

Table B.2   Error rates of Hunns

Classification of error type	Typical probabilities
Processes involving creative thinking, unfamiliar operations where time is short; high stress situations	0.1-1
Errors of omission where dependence is placed on situation cues or memory	1E-2
Errors of commission such as operating wrong button, reading wrong dial, etc.	1E-3
Errors in regularly performed, common-place tasks	1E-4
Extraordinary errors - of the type difficult to conceive how they could occur; stress-free, powerful cues militating for success	<1E-5

Table B.3 Error rates of Dhillon

Error	Rate per demand	Rate per plant-month
Reading a chart recorder	6E-3	
Reading an analog meter	3E-3	
Reading graphs	1E-2	
Interpreting incorrectly an indicator	1E-3	
Turning a control in the wrong direction under high stress	0.5	
Using a checklist incorrectly	0.5	
Mating a connector	1E-2	
Choosing an incorrect panel control out of several similar controls	3E-3	
Reading a gauge incorrectly	5.0E-3	
Closing a valve improperly	1.8E-3	
Soldering connectors improperly	6.5E-3	
Actuating switch inappropriately	1.1E-3	
Failure to tighten nut and bolt	4.8E-3	
Failure to install nut and bolt	6E-4	
Improper adjustment of mechanical linkage	1.7E-2	
Procedural error in reading instructions	6.5E-2	
Connecting hose improperly	4.7E-3	
Failure to pursue proper procedure by an operator		0.040
Installation error		0.013
Misinterpretation or misunderstanding of requirements by the operator		0.0076
Inadvertent or improper equipment manipulation by the operator		0.071
Improper servicing or reassembly by the maintenance personnel		0.0l5

Table B.4 General human error rate estimates (from WSRC-TR-93-581)

	Failure	Failure type	Failure probability (mean)	Error factor	Guideline for selection
1.	Failure of administrative control	Nominal	5E-3	10	Typical circumstances
		High	5E-2	5	Unusual circumstances
		Low	5E-4	10	Routine, repetitive circumstances
2.	Failure to respond to compelling signal	Nominal	1E-2	5	Several competing signals
		High	1E-1	3	Many competing signals
		Low	3E-3	10	Few competing signals
3.	Failure to verify within control room	Nominal	1E-2	5	Good layout, procedure-driven
		High	5E-2	5	Poor layout, scanning effort
		Low	3E-3	10	Excellent, procedure-driven
4.	Failure to verify outside control room	Nominal	3E-2	5	Good layout, procedure-driven
		High	1E-1	3	Poor layout, scanning effort
		Low	1E-1	5	Excellent, procedure-driven
5.	Error in selecting control within control room	Nominal	1E-2	5	Good layout, procedure-driven
		High	3E-2	5	Poor layout, scanning effort
		Low	1E-3	10	Excellent, procedure-driven
6.	Error in selecting control outside control room	Nominal	1E-2	5	Good layout, procedure-driven
		High	5E-2	5	Poor layout, scanning effort
		Low	3E-3	10	Excellent, procedure-driven
7.	Communication error	Nominal	5E-2	5	Moderate information
		High	5E-1	2	Complex information
		Low	1E-3	10	Simple information

Table B.4 (continued)

	Failure	Failure type	Failure probability (mean)	Error factor	Guideline for selection
8.	Checker verification error	Nominal	1E-1	3	Alerted, but not active participant
		High	3E-1	3	Written materials not used
		Low	1E-2	5	Checking requires active participant
9.	Supervisor verification error	Nominal	3E-1	3	Check-off sheet, medium dependence
		High	5E-1	2	No check-off sheet, high dependence, high stress
		Low	1E-1	3	Check-off sheet, low dependence
10.	Incorrect labeling or tagging	Nominal	5E-3	10	Normal administrative controls
		High	3E-2	5	Poor administrative controls
		Low	1E-3	10	Excellent administrative controls
11.	Incorrect reading or recording data	Nominal	1E-2	5	Good display (graph)
		High	5E-1	2	Poor display
		Low	3E-3	10	Excellent display
12.	Miscalibration	Nominal	5E-3	10	Single-person, operator check
		High	3E-2	5	Single-person, no checks
		Low	3E-3	10	Two-person, operator check
13.	Failure to restore following test	Nominal	1E-2	5	Single-person, operator check
		High	3E-2	5	Single-person, no checks
		Low	5E-3	10	Two-person, operator check
14.	Failure to restore following maintenance	Nominal	5E-3	10	Single-person, operator check
		High	5E-2	5	Single-person, no checks
		Low	3E-3	10	Two-person, operator check

	Failure	Failure type	Failure probability (mean)	Error factor	Guideline for selection
15.	Failure to restore lock out	Nominal	5E-4	10	Typical lockout plan (5 to 10 lockouts)
		High	5E-3	10	Complex lockout plan (11 to 100 lockouts)
		Low	1E-4	10	Simple lockout plan (1 to 4 lockouts)
16.	Chemical addition or elution error	Nominal	3E-3	10	Typical process
		High	3E-2	5	Complex process
		Low	3E-4	10	Simple process
17.	Transfer error (/tank-hr)	Nominal	3E-6	10	Moderate activity (10 potential transfers/year)
		High	3E-5	10	High activity (100 potential transfers/year)
		Low	3E-7	10	Low activity (1 potential transfers/year)
18.	Overfilling of a tank	Nominal	5E-6	10	Moderate activity (10 potential transfers/year)
		High	5E-5	10	High activity (100 potential transfers/year)
		Low	5E-7	10	Low activity (1 potential transfers/year)
19.	Laboratory analysis error	Nominal	3E-4	10	Low dependence check
		High	1E-3	10	No check
		Low	3E-5	10	Zero dependence check
20.	Failure to verify parameter with calculation	Nominal	3E-2	5	Procedure usually used, verification
		High	1E-1	3	No verification
		Low	5E-3	10	Procedure almost always used, verification

Table B.4 (continued)

	Failure	Failure type	Failure probability (mean)	Error factor	Guideline for selection
21.	Random actuation/ shutdown of system (/hr)	Nominal	5E-6	10	Some activities could affect system
		High	5E-5	10	Many activities could affect system
		Low	5E-7	10	Almost no activities could affect system
22.	Vehicle collision with stationary object (/mi)	Nominal	1E-6	10	Typical highway environment
		High	1E-5	10	Congested road, bad weather
		Low	1E-7	10	Freeway environment
23.	Single vehicle accident (/mi)	Nominal	1E-6	10	Typical highway environment
		High	1E-5	10	Congested road, bad weather
		Low	1E-7	10	Freeway environment
24.	Vehicle collision with another moving vehicle (/mi)	Nominal	1E-6	10	Typical highway environment
		High	1E-5	10	Congested road, bad weather
		Low	1E-7	10	Freeway environment
25.	Dropping of load when using forklift (/operation)	Nominal	5E-5	10	Typical load
		High	5E-4	10	Unusual, unevenly balanced load
		Low	1E-5	10	Standardized load, spotter present
26.	Puncturing of load when using forklift (/operation)	Nominal	3E-5	10	Typical load
		High	3E-4	10	Unusual, unevenly balanced load
		Low	5E-6	10	Standardized load, spotter present

Failure	Failure type	Failure probability (mean)	Error factor	Guideline for selection
27. Dropping of load when using crane/hoist (/operation)	Nominal	1E-4	10	Typical load
	High	1E-3	10	Unusual, unevenly balanced load
	Low	3E-5	10	Standardized load, spotter present
28. Crane/hoist strikes stationary object (/operation)	Nominal	3E-4	10	Typical visibility
	High	3E-3	10	No spotter, low visibility
	Low	3E-5	10	Spotter present
29. Excavation error (/excavation)	Nominal	1E-2	5	Good review of area
	High	1E-1	3	Poor review of area
	Low	1E-3	10	Excellent review of area (survey for underground objects)
30. Diagnosis error	Nominal	1E-2	5	Knowledge-based 30 to 120 minutes
	High	1E-1	3	Knowledge-based 10 to 30 minutes
	Low	1E-3	10	Knowledge-based greater than 120 minutes
31. Failure of visual inspection	Nominal	1E-1	3	Procedure usually followed, event easy to observe
	High	5E-1	2	Event difficult to observe
	Low	lE-2	5	Procedure followed, event easy to observe (damage very prominent)
32. Failure of manual fire detection	Nominal	1E-1	3	Area occupied 80% of time
	High	5E-1	2	Area unoccupied
	Low	1E-2	5	Area occupied 100% of time

Table B.4 (continued)

	Failure	Failure type	Failure probability (mean)	Error factor	Guideline for selection
33.	Failure of manual fire suppression by occupant	Nominal	3E-1	3	Typical fire extinguisher installation/maintenance
		High	5E-1	2	Poor fire extinguisher installation/maintenance
		Low	1E-1	3	Excellent fire extinguisher installation/maintenance
34.	Failure of manual fire suppression by nonoccupant	Nominal	1E-1	3	Response by 10 minutes, typical fire
		High	3E-1	3	Response much longer than 10 minutes, difficult fire
		Low	3E-2	5	Response less than 10 minutes, simple fire
35.	Failure of long-term accident recovery	Nominal	3E-3	10	24-48 hours for recovery, simple recovery act
		High	1E-1	3	Less than 24 hours for recovery
		Low	3E-5	10	3-7 days for recovery, simple recovery actions

Note: The error factor is the 95th percentile /50th percentile (median). To convert a mean value to a median, multiply the mean by the following:

Error Factor	Mean to Median Multiplier
1	1.00
2	0.92
3	0.80
5	0.62
10	0.38

Table B.5 General error rate estimates (from WASH-1400)

Activity	Estimated Error Rate
Selection of key-operated switch vs. a non-key operated switch	1E-4
Selection of a switch dissimilar in shape or location to the desired switch (assuming no decision making)	1E-3
General human error of commission such as misreading label	3E-3
General human error of omission where there is no display of the item’s status	1E-2
Error of omission where the items being omitted are embedded in a procedure.	3E-3
Simple arithmetic errors with self checking but without repeating the calculation by re-doing it on another piece of paper.	3E-2
Given that an operator is reaching for an incorrect switch (or pair of switches), he/she selects a particular similar appearing switch, where *x*=no. of incorrect switches adjacent to the desired switch. Valid when *x*<6.	1/*x*
Monitor or inspector fails to recognize initial error by operator.	1E-1
Personnel on different shift fail to check condition of hardware unless required by check list or written directive.	1E-1
Monitor fails to detect undesired position of valves, etc., during general walk-around inspections, assuming no check list is used.	5E-1
General error rate given very high stress levels where dangerous activities are occurring rapidly.	.2-.3
Under severe time stress, as in trying to compensate for an error made in an emergency situation, the initial error rate, *X*, for an activity doubles for each attempt, *N*, after a previous incorrect attempt.	2(*N*-1)*X*
Operator fails to act correctly in the first 60 seconds after the onset of an extremely high stress condition	1.0
Operator fails to act correctly in the first 5 minutes after the onset of an extremely high stress condition	9E-1
Operator fails to act correctly in the first 30 minutes after the onset of an extremely high stress condition	1E-1
Operator fails to act correctly in the first several hours after the onset of an extremely high stress condition	1E-2

APPENDIX C

GUIDANCE FOR PERFORMING BARRIER ANALYSIS OF DOE INCIDENTS

APPENDIX C
GUIDANCE FOR PERFORMING BARRIER ANALYSIS OF DOE INCIDENTS

C.1 Introduction

The use of event trees to analyze incidents which have occurred at DOE facilities is generally straightforward and requires a minimal amount of resources. The advantages of this type of analysis, as explained in Section 2 following, can be significant and lead to insights not readily available with other types of analyses. These insights can indicate the need for implementing risk reduction initiatives, and identify strategies for reducing the risks from similar events throughout the DOE complex. The Nuclear Regulatory Commission has used this same technique for some time to evaluate the significance of events which have occurred at commercial nuclear power plants.[1] The guidance provided here is designed to make the event tree analysis effective and efficient and is tailored for applicability to events at DOE facilities. Section 3 provides seven examples of event tree analysis for selected DOE events.

Event trees are essentially logic diagrams which are useful in examining the progression of an event and identifying alternative accident sequences along with their estimated probabilities and consequences. Figure C.1 shows a generic event tree. The event tree starts with an initiating event. The initiating event is the physical activity which subsequently led to the actual incident, such as closing a valve, or welding some component. Following the initiating event, a series of items are considered which have the potential for influencing either the probability or the consequences of the incident. For analyzing DOE events, these items are exclusively known as “barriers”. The barriers can be either administrative or physical, as shown on Figure C.1. Administrative barriers are those management initiatives which involve the safety evaluation of activities and the use of procedures and training. Thus, administrative barriers include such things as safety analysis, safe work permits, training, access control, inspection policies, job planning and controls, etc. These administrative barriers are selected for each initiating event based on the following criteria, both of which must be satisfied before it is considered on the tree:

1. Did the barrier actually exist at the facility prior to or during the event, or would such a barrier normally be expected to exist at a DOE facility?

2. Would the barrier be expected to influence the probability or outcome of the incident?

Note that the barrier does not have to exist during the actual event to be included in the event tree. For example, for a particular event, a safe work permit, for whatever reason, may not have been prepared prior to the initiating event activity. However, based on the activity involved, it may be judged that such a permit would likely have been prepared at a DOE facility. In this instance, if the work permit could have had a significant influence on the probability or outcome of the incident, it should be included on the tree.

Physical barriers include those items which are put in place to protect workers or prevent activities from progressing to accidents. Such barriers include protective clothing, fire walls, remote operations, etc. Figure 2.1 is a matrix of barriers normally utilized for various hazard sources. The matrix also shows barrier effectiveness which can be helpful in assigning probabilities to barrier failures (to be discussed later). It is important to recognize that the administrative and physical barriers are not always independent. That is, if the administrative barriers exist, then it is more likely that physical barriers will also be put in place and be successful. The rules for the selection of administrative barriers (items 1 and 2 preceding) also apply for the consideration of physical barriers.

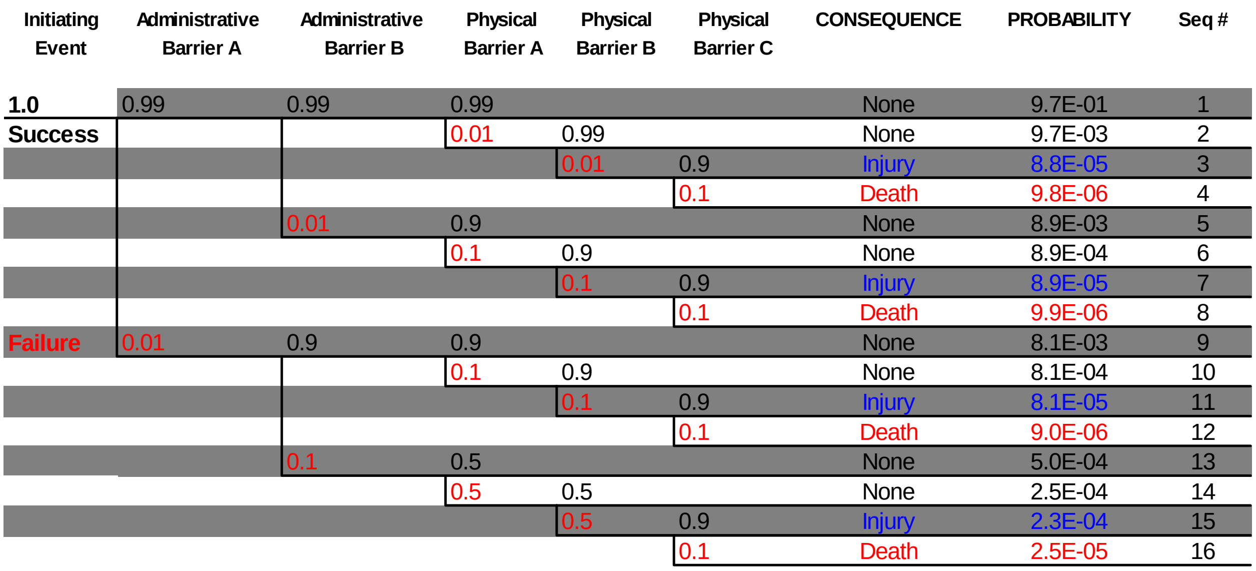
In constructing an event tree, it is useful to consider the administrative barriers first, followed by the physical barriers. This is shown in Figure C.1, where two barriers of each type (designated by “A” and “B” under administrative and physical barriers) are assumed to exist. In some cases, depending on the circumstances involved in the incident, it may be appropriate to add additional headings to the event tree which do not involve administrative or physical barriers. An example would be human error.

Following the selection of the barriers, the event tree next considers consequences. Consequences can be any undesirable outcome, but must include the outcome of the actual event being analyzed. Such outcomes include radioactive release, toxic chemical release, worker injury or death, or public exposure to radionuclides or toxic chemicals. If the consequences could have been significantly worse than the outcome of the actual event, this needs to be considered on the tree.

The final column of the event tree considers the probability of each sequence considered in the tree. This probability is the product of the probabilities assigned to each branch of the sequence.

For each event tree barrier, a probability is assigned for success or failure of that barrier. As shown in Figure C.1 this is accomplished by drawing two lines or branches under each of the barriers. The upper branch signifies that the barrier was successful, the lower branch designates failure. At the beginning of each branch under the specific barrier, a numerical estimate is made of the success and failure of the barrier (these estimates must always sum to 1.0). Arbitrary probabilities have been used in Figure C.1 to illustrate this procedure. For example, under the Administrative Barrier “A” heading, a probability of .99 is shown for success, and .01 for failure. For administrative barriers, this probability designates whether the barrier would be expected to exist during the event. For the physical barrier, the probability considers whether the barrier would be expected to exist, and if so, whether the barrier is effective in preventing the subsequent undesirable outcome. The estimate of probabilities, especially for administrative barriers, is quite subjective and uncertain. Reference 2 provides some guidance in assigning these probabilities. However, the probabilities should usually consider and be adjusted to account for the actual circumstances surrounding the event. At the same time, the probabilities need to reflect what is normally to be expected at DOE facilities. For example, if the work to be done clearly involves direct contact with hazardous material, then the probability that a safety analysis would be completed prior to the activity is quite high (typically 0.99). However, if there is some question about whether hazardous material will be directly involved, or whether the material is indeed hazardous, then the probability should be reduced (perhaps 0.9). If it is not at all clear that hazardous material, or hazardous activity, is involved, then a probability of 0.5 might be estimated. Note that these probabilities are assigned independent of whether the barrier was actually utilized in the event being considered. The probability is adjusted by considering the circumstances involved in the event. Similar considerations are appropriate for physical barriers.

In assigning probabilities, attention must be given to the potential for dependencies. Dependencies are links between barriers or events which influence probabilities of the event branch points. Event trees are helpful in displaying this dependency potential in that events are linked in a logical progression. Thus, the probability of a given branch of an event tree is conditional on the previous branch events which lead into it. Dependencies are generally of two types. The first type is a dependency which influences, or conditions, the probability of a subsequent failure. For example, if a hazard analysis has not been conducted for a particular activity, then it is less likely that an adequate safe work permit (SWP) will be prepared. Conversely, if a hazard analysis has been prepared, then it more likely that a SWP will also be prepared. The event tree must reflect this by assigning a conditional probability for the preparation of a SWP depending on whether the branch being considered has been preceded by a hazard analysis or not. The second type of dependency is where a subsequent event is actually precluded based on the occurrence of a preceding event. For example, if a fire is being considered by an event tree, the event which considers fire propagation is not



Initiating Event	Administrative Barrier A	Administrative Barrier B	Physical Barrier A	Physical Barrier B	Physical Barrier C	CONSEQUENCE	PROBABILITY	Seq #
1.0	0.99	0.99	0.99			None	9.7E-01	1
Success			0.01	0.99		None	9.7E-03	2
				0.01	0.9	Injury	8.8E-05	3
					0.1	Death	9.8E-06	4
		0.01	0.9			None	8.9E-03	5
			0.1	0.9		None	8.9E-04	6
				0.1	0.9	Injury	8.9E-05	7
					0.1	Death	9.9E-06	8
Failure	0.01	0.9	0.9			None	8.1E-03	9
			0.1	0.9		None	8.1E-04	10
				0.1	0.9	Injury	8.1E-05	11
					0.1	Death	9.0E-06	12
		0.1	0.5			None	5.0E-04	13
			0.5	0.5		None	2.5E-04	14
				0.5	0.9	Injury	2.3E-04	15
					0.1	Death	2.5E-05	16

Figure C.1 Generic event tree

considered for the branch for which the fire has been successfully extinguished. For the branch which considers that the fire has not been successfully extinguished, fire propagation is considered, and the probability is based on other factors such as the controls in place to limit the availability of combustible materials. The event tree in Figure C.1 shows some hypothetical examples of these types of dependencies. In the tree, if administrative barrier “A” succeeds, then it is assumed that “B” will be more likely to succeed (probability 0.99) than if “A” fails (probability 0.9). Also, the tree illustrates that if physical barrier “A” succeeds, then barrier “B” is not considered because, for this hypothetical example, it is assumed that either barrier “A” or “B” prevents the adverse consequences if successful.

After the event tree is completed, and probabilities computed, then insights are drawn from the results. The most important insights are the probability of the unwanted consequences, and the most effective means of reducing the probabilities. If the sum of the probabilities of the unwanted sequences are in the range of .1 to .001, then the risk can be of concern, and the potential for recurrence of the event needs to be considered. If properly constructed, the tree should clearly show which barriers are the most significant in affecting a reduction in the probability of the unwanted sequences.

C.2 Advantages of Event Trees for Analyses of Events

This report includes (Section C.3) an analysis of seven operating events which have occurred at DOE facilities. The analysis is based on a risk formulation which uses event trees to examine the progression of the event to an undesirable outcome. The approach focuses on the administrative and physical barriers (as noted in Section l) which existed, or should have existed, to prevent the event from progressing to an accident which resulted in an undesirable consequence. The purpose of the analysis is to determine the most important factors which permitted the accident to occur, and provide information to assess the need to improve the DOE safety infrastructure to prevent recurrence. A second purpose is to illustrate the methodology such that similar analyses can be performed by others when events occur in the future.

The basic structure utilized in the analyses consists of the event tree. Event trees have been used for many decades to study the progression of events and estimate the probability of various outcomes. They are easy to use and understand, and can be used to:

- Provide valuable insight regarding the interrelationships and significance of elements which contribute to or alter the various consequences from an initiating event. The most important barrier failures contributing to the event can be readily identified.

- Illustrate whether an accident was a rare event, or whether it is more likely to occur in the future under similar circumstances. This information can suggest the need and priorities for safety improvements, as well as the most effective strategy for affecting improvements.

- Provide a mechanism for examining the likelihood that the accident could have progressed further (if additional barrier failures occurred) and resulted in more significant consequences. Such analyses (not done in investigative reports) can provide further insight on the need for remedial actions.

It should be emphasized that the probabilities assigned to the barrier failures and events in this report are subjective and uncertain. The probabilities are based primarily on information contained in the investigative reports prepared for each accident, and represent estimated failure probabilities which would be expected to exist at a DOE site under the circumstances of the event. The investigative reports do not, in general, contain any failure data or probability estimates, and resources did not permit gathering any information beyond that contained in the reports. In some cases, the information provided is not complete enough to provide a basis for more than a guess at the probability of an individual barrier failure. Therefore, the probability estimates only provide a gross estimate of accident sequence likelihood. They are not meant to be recommendations for the probability of similar failures at DOE sites, but are only guides which indicate what reasonable estimates might be. More accurate estimates could be obtained by additional analysis of the events and examination of available data. Values for specific sites need to be adjusted based on local factors such as safety culture, organization details, and institutional structure. The event trees do, however, provide a template which can readily accommodate different probability values such that sensitivity studies can be performed. The process of estimating the probability values is useful in itself as it tends to expose problem areas and suggest strategies for improvement. It should also be noted that the probability estimates do not have to be accurate to provide valuable insights from the event tree analysis. Order of magnitude estimates can illustrate the important mitigative barriers and indicate if the event may have a high likelihood of recurrence.

C.3 Analysis of Events

This section provides example analyses of seven events which have occurred at DOE facilities. The events were selected to illustrate the methodology for a wide spectrum of different incidents. The analyses were performed based entirely on the investigative reports which were prepared for each incident, and therefore are dependent on the accuracy and completeness of the reports.

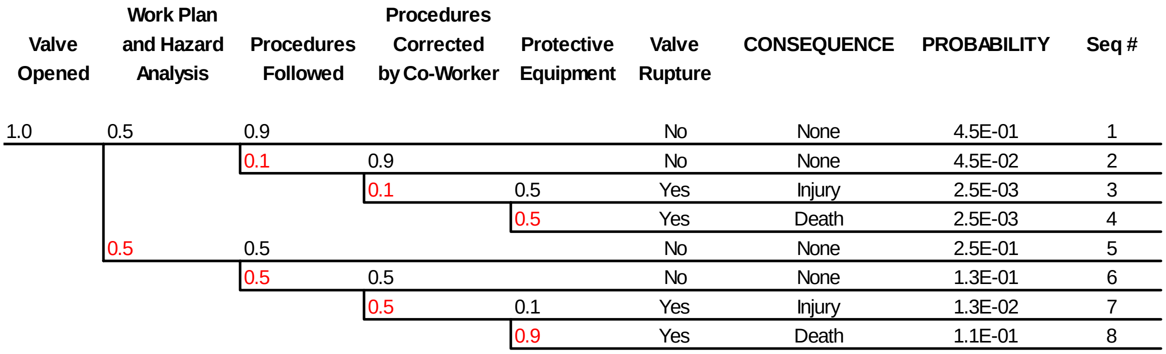
C.3.1 U-3 Steam Pit Valve Failure at the Hanford Site

This event occurred on June 7, 1993 and resulted in the death of a worker at DOE's Hanford Site. A worker entered the U-3 Pit which enclosed piping and valves associated with a steam distribution system. The worker unlocked and partially opened a valve to permit steam flow to another part of the system. A thermal-hydraulic transient occurred when the valve was opened. This transient, which involved a water hammer event, caused the rupture of another valve in the Pit which resulted in the release of steam into the pit. The worker suffered burns and respiratory system damage from exposure to and inhalation of the steam. The worker died seven days after the event from inhalation asphyxiation. The event was the subject of a Type A (most serious) Accident Investigation. The results of the investigation, and a detailed description of the event, can be found in Ref. 3.

Figure C.2 is an event tree which illustrates the progression of the event and includes the important barriers to be considered.

A. ***Valve Opened.*** This initial activity by the worker in the U-3 pit is the initiating event for the accident sequence. The next four headings across the top of the event tree which follow the initiating event depict administrative and physical barriers, which, if they had been effective, could have prevented or minimized the consequences of the event.

B. ***Work Plan and Hazard Analysis.*** This heading represents an activity which was not performed for the event being analyzed. Had this activity been performed, as will be seen, the probability of the subsequent accident progression would have been markedly reduced. The work plan with hazard analysis was apparently not performed because the activity in question was not perceived as a particularly dangerous or unusual event. Further, similar operations had been performed in the past without incident. However, under the circumstance involved, the activity to be performed was in fact quite dangerous and was not similar in some respects to previous operations. The fact that high



Valve Opened	Work Plan and Hazard Analysis	Procedures Followed	Procedures Corrected by Co-Worker	Protective Equipment	Valve Rupture	CONSEQUENCE	PROBABILITY	Seq #
1.0	0.5	0.9			No	None	4.5E-01	1
		0.1	0.9		No	None	4.5E-02	2
			0.1	0.5	Yes	Injury	2.5E-03	3
				0.5	Yes	Death	2.5E-03	4
	0.5	0.5			No	None	2.5E-01	5
		0.5	0.5		No	None	1.3E-01	6
			0.5	0.1	Yes	Injury	1.3E-02	7
				0.9	Yes	Death	1.1E-01	8

Figure C.2 Hanford U-3 steam pit

energy steam was involved, and that conditions in the U-3 Pit steam system were consistent with a possible water hammer event should have been recognized. Water hammer events had occurred at other DOE facilities prior to the U-3 event (see, for example, event No. 2 which follows). The two branches below the heading "Work Plan and Hazard Analysis" show the two alternate paths depending on whether this event was performed. The upper branch shows the subsequent estimated progression of the of the sequence if the activity had been performed and the branch which is drawn vertically downward shows the progression if the activity had not been performed. The 0.5 values on the two branches represent the estimated probability that the event would (or would not) have been performed. This is a very subjective estimate which depends on existing safety culture at a particular facility, the perception of the risks involved in the activity, and other factors.

C. ***Procedure***. Informal procedures previously used for similar valve opening activities involved slowly opening the valve to avoid sudden extensive condensation and other rapid pressure changes which could result in a water hammer. As shown in the tree, the probability of procedures not being followed is given a lower value (0.1) if a hazard analysis and work plan preceded the event. This value is based on the fact that a work plan with hazard analysis have alerted the worker to the problems involved with rapid valve opening and would likely have resulted in formal procedures. This value is considered appropriate based on the values proposed in Ref. 2. In this case, the high temperature environment and cramped space in the U-3 vault are performance shaping factors which would be expected to increase normal human error probabilities. If no work plan and hazard analysis preceded the consideration of procedures, then the probability of not following existing informal procedures is increased to 0.5.

D. ***Procedure Corrected by Co-Worker.*** According to the report on the Hanford event,[3] standard procedure at the site calls for one worker to observe the actions of another. The observing worker is expected to correct any unsafe procedure which he or she observes, and this can be considered an administrative barrier for the purposes of this analysis. In the case of the U-3 event, there was a second worker assigned to the activity for observation purposes, but she was uncertain of her actual duties, and no formal procedure was available for the activity. Also, she did not actually enter the U-3 Pit, and her view of the activities of the worker opening the valve in the Pit was somewhat obstructed. Her attention was also diverted by other activities. For the upper branch, a probability of 0.1 is assigned for failure of this event. This probability is based on the fact that procedures would have existed in this case based on the success of a preceding work plan and hazard analysis. For the lower branch, a higher probability of failure is assigned (0.5) because an adequate worker plan and hazard analysis leading to formal procedures was not available.

E. ***Adequate Design.*** This barrier is considered because the U-3 Pit equipment design was found after the event to be inadequate in several respects. The valve which ruptured was found to be of incorrect material for the intended application (cast carbon steel rather than stainless steel), and was also found to be only half as strong as it should have been. Further, the piping upstream of the valve which was opened by the worker did not have a condensate drain, and the opened valve did not have bypass lines. Either of these design features could have prevented the accident if the equipment had been properly used. It is not clear from the event analysis if proper design and fabrication of the valve which failed would have prevented the rupture or not. The failure probability of 0.1 is estimated for both of the branches on the tree for this barrier. In other words, it is expected that under similar conditions, it would be expected that a proper design would have been implemented for this type of system 90% of the time and the proper design would have prevented the accident.

F. ***Protective Equipment.*** In this accident, both an ice vest and self-contained breathing equipment were considered for use by the worker prior to entry into the U-3 Pit. This equipment was considered because of the high temperature in the Pit (about 140°F) and the possibility of asbestos in the pit from insulating materials. However, the equipment was rejected by the worker because of the anticipation of cramped working conditions. If the equipment had been worn, it is likely that a fatality would have been prevented (even though the equipment was considered for protection against a perceived hazard, asbestos, other than escaping steam). For the upper two branches, a probability of 0.9 is estimated for success of this action, based on the sequences for which an adequate work plan and hazard analysis had been completed. For the lower two branches, a higher failure probability (0.5) is assigned because these sequences did not have an adequate hazard analysis and work plan.

G. ***No Valve Rupture.*** This event considers the probability of valve rupture given the nature of the sequence preceding the event. This probability is given a range of 0.1 up to 0.9. The probability is influenced by the preceding event of “adequate design”. Since it is not clear if a properly designed valve would have ruptured or not, a value of 0.9 is assigned for this case.

H. ***Consequences.*** The next column on the event tree considers the likely consequences given the sequence being considered. The consequence choices are none (for those cases in which the valve did not fail), injury for the cases in which protective equipment was employed, and death for the other cases. For the case where protective equipment was employed, it is estimated that the probability of having only injury is quite high, 0.9, but there is still a possibility that death could occur (probability of 0.1). For the case of no protective equipment, it is assumed that death is the only consequence.

I. ***Probability.*** The last column provides an estimate of the conditional probability of each sequence. These probabilities are conditional in that the initiating event (valve opened) is assumed to occur. It should be emphasized that the probability estimates are quite uncertain. Their value is primarily to show relative probabilities of alternate sequences, show the influence of interrelationships among the events, and to illustrate how changing the probability of events can alter the probability of unwanted consequences. The figure clearly shows that the first barrier listed "Work Plan and Hazard Analysis" is the single most important barrier which could have been implemented prior to the activity. The probability of this barrier being successful influences the subsequent probabilities of procedures followed and procedures corrected, as well as the use of protective clothing. If the success probability of this event is improved, a direct improvement in each of the high probability (last six sequences with adverse consequences) sequences is realized. As shown in Figure C.2, the high probability assigned to failure of this event (0.5) directly influences all six of the adverse consequences in the lower half of the tree. Clearly this event is the single most important event affecting the probability of adverse consequences and would be the most important aspect for safety management to emphasize.

C.3.2 Steam Line Accident at Brookhaven National Laboratory

This accident occurred on Oct. 10, 1986 and resulted in the injury of four workers, two of whom died as a result of the injuries. Reference 4 provides a detailed description and analysis of the event, which resulted in a Type A (most serious) accident investigation. The event occurred when workmen were opening a valve to activate a new section of a steam distribution system at BNL. As a result of the valve opening, a water hammer (slug of water accelerated by condensation and steam pressure) occurred. The water hammer caused the extruding of gasket material in blind flanges located in the work area. The gasket failures allowed high pressure steam to flow into the work area which caused severe burn injuries.

Figure C.3 is the event tree which has been constructed for the accident based on the information in Ref. 4. The event tree headings are discussed in the following sections.

A. ***Valve Opened.*** This is the initiating event for the accident. The valve was opened manually to activate the new section of steam lines which had been installed.

B. ***Operational Readiness Review.*** ORRs are generally prepared at DOE facilities whenever a new or modified system is to be started up for the first time. It is not clear whether the activation of the new steam system at BNL should have required an ORR or not. The activation of this system was apparently perceived as a routine, non-hazardous operation since the steam system was expanded in the past. The write-up for the event[4] does not specify under what conditions ORRs were required at BNL at the time of the event. However, management and supervisory personnel should have recognized that activation of a new system with high energy steam does pose some hazard, and that precautions and adequate procedures are important to minimize the potential for accidents. Water hammer events have been known for some time as a potential problem when steam or condensate is transferred within a system. Given these considerations, the probability of performing an ORR for this event is assigned a 0.5 probability of failure (or success) in the absence of additional information. This probability split is shown on the tree, where the top of the branch indicates that an adequate ORR is performed.

C. ***Procedures Followed.*** This event covers whether procedures existed and were followed during the accident. The report of the incident[4] indicates that no written procedures were available for the workers. Two cases are considered for the procedures depending on the success of the preceding ORR event. If an ORR had been completed, it is likely that procedures would have been prepared and followed as a result. Thus, for this case, “Procedures’ is assigned a probability of 0.95. For the case of no ORR, the probability of having procedures is reduced to 0.8. It is still considered fairly likely that procedures would exist even without an ORR since work on high energy steam lines would normally be expected to involve procedures.

D. ***Adequate Steam Trap.*** During an earlier attempt to activate the steam line, workmen perceived that a steam trap in the steam line had failed. The steam trap was provided to prevent the buildup of condensate in the line. The workmen requested a change in the replacement steam trap which was approved. The new steam trap was similar to other steam traps in the system, but only had 1/3 the capacity of the original steam trap. If the steam trap had been replaced with the original design, it

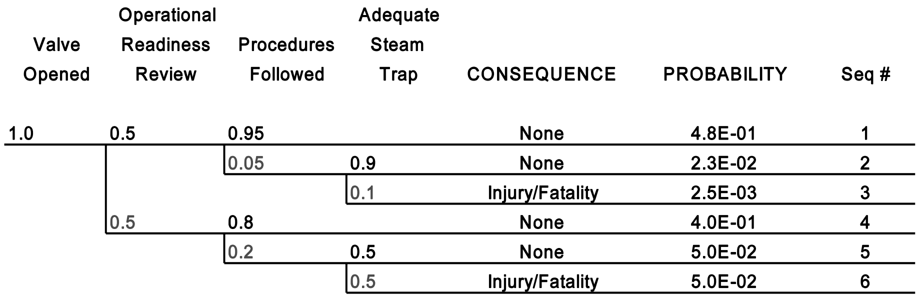


Figure C.3 Steam line at BNL

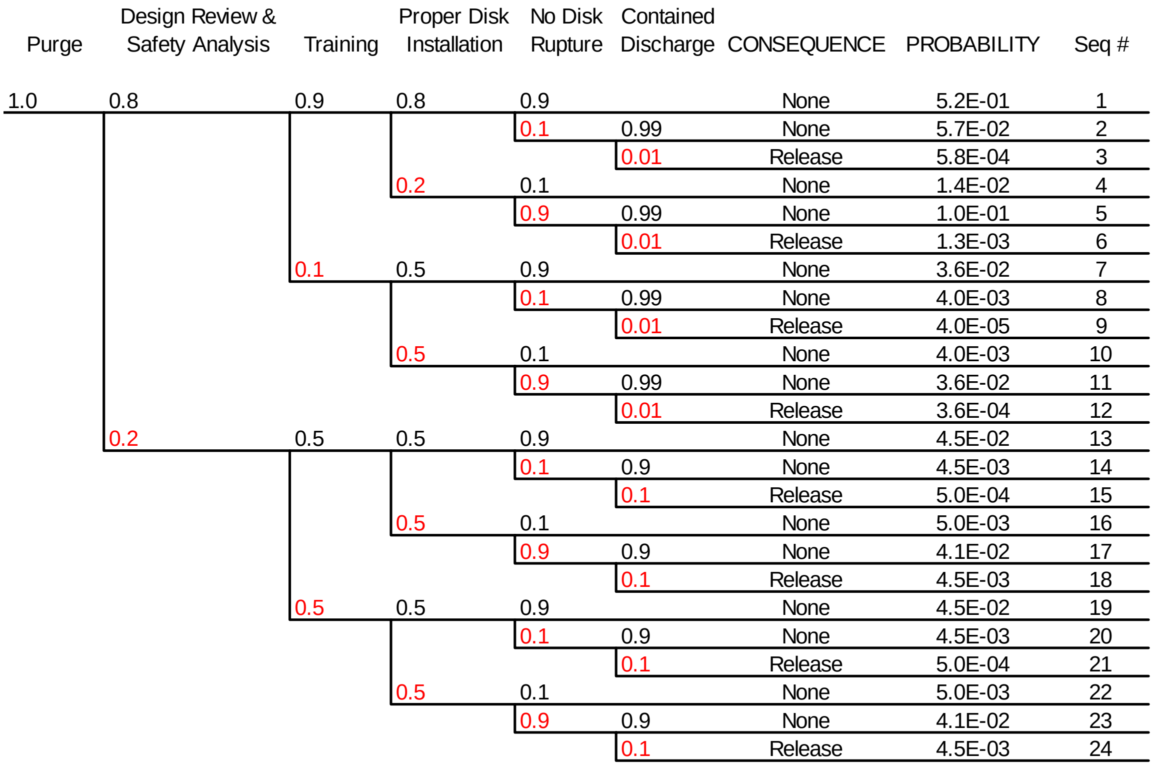
is possible that the increased condensate removal capacity would have prevented, or at least ameliorated the water hammer such that no gasket failures would have occurred. However, it is not clear from the Ref. 4 analysis how probable the prevention of the accident would have been. Thus, for this event, in the case of no ORR preparation (bottom branch), the “adequate steam trap” event is assigned a probability of 0.5 for failure to prevent the accident. In the upper branch, a lower probability of failure to prevent the accident is assigned (0.1) based on the premise that the ORR would likely have identified the inadequate steam trap and it would have been replaced.

E. ***Consequences and Probability.*** These headings indicate the expected outcome and associated probability of each of the sequences. As shown, the actual accident sequence (the lower branch) has a rather high probability of 0.05. This suggests that the event was not a bizarre rare event, but instead had a relatively high probability of occurrence under the circumstances leading up to the accident. This result suggests that some change in the safety infrastructure could be useful. The most effective change, also displayed by the event tree, would be to institute definitive requirements for ORRs, or similar safety analysis prior to undertaking activities involving hazards. This would improve the probability of adequate procedures and suggest design (or modification) improvements.

C.3.3 Release of Anhydrous Hydrogen Fluoride at the Feed Materials Production Center

During a purge of an Anhydrous Hydrogen Fluoride (AHF) transfer system at the Feed Materials Production Center on 9/29/87, a rupture disc installed for overpressure protection ruptured and released from 94 to 270 pounds (estimated range) of AHF to the atmosphere. Some 28 on-site individuals were treated for minor eye and skin exposure to AHF. All returned to work the same day. Some of the AHF eventually was transported to the Miami River and a momentary increase in concentration was noted. A complete description of the event, including a Type B investigation and analysis, is provided in Ref. 5. One of the conclusions of the investigation board report[5] was that improved isolation and diversion valve locations could have resulted in a faster termination of the release, but would not have prevented it. This consideration is not included in the event tree (although it could be readily added) since the event of interest is only the uncontrolled release of AHF.

Figure C.4 is an event tree which provides illustration of the event and examines alternate sequences.



Purge	Design Review & Safety Analysis	Training	Proper Disk Installation	No Disk Rupture	Contained Discharge	CONSEQUENCE	PROBABILITY	Seq #
1.0	0.8	0.9	0.8	0.9		None	5.2E-01	1
				0.1	0.99	None	5.7E-02	2
					0.01	Release	5.8E-04	3
			0.2	0.1		None	1.4E-02	4
				0.9	0.99	None	1.0E-01	5
					0.01	Release	1.3E-03	6
		0.1	0.5	0.9		None	3.6E-02	7
				0.1	0.99	None	4.0E-03	8
					0.01	Release	4.0E-05	9
			0.5	0.1		None	4.0E-03	10
				0.9	0.99	None	3.6E-02	11
					0.01	Release	3.6E-04	12
	0.2	0.5	0.5	0.9		None	4.5E-02	13
				0.1	0.9	None	4.5E-03	14
					0.1	Release	5.0E-04	15
			0.5	0.1		None	5.0E-03	16
				0.9	0.9	None	4.1E-02	17
					0.1	Release	4.5E-03	18
		0.5	0.5	0.9		None	4.5E-02	19
				0.1	0.9	None	4.5E-03	20
					0.1	Release	5.0E-04	21
			0.5	0.1		None	5.0E-03	22
				0.9	0.9	None	4.1E-02	23
					0.1	Release	4.5E-03	24

Figure C.4 Release of AHF at FMPC

A. ***Purge.*** The purge event was the initiating action for the accident. The purging of the AHF transfer lines was a fairly routine activity which had been performed many times in the past. However, some modifications had been performed on the purge system and it was being used for the first time in the new configuration.

B. ***Design Review and Safety Analysis.*** This activity considers whether a design review and safety analysis had been done for the newly installed system. In this case, a partial safety analysis had been completed, but had been performed with incorrect system information and had not been reviewed by all parties with approval responsibility. The success of this activity is given a 0.8 probability. It would be expected that under similar circumstances this activity would normally be performed at DOE facilities, but the fact that this system would probably be perceived as a minor, simple system with only minor changes from a system used many times in the past would reduce the probability somewhat.

C. ***Training.*** No training was provided for operating the system. Two alternatives are considered here; one for the case of successful design review and safety analysis (upper branches), and one for failure of this event. For success, the training activity is given a high probability (0.9) based on the expectation that the safety analysis would have uncovered the potential for release from failure of the rupture discs, and identified appropriate disc installation and operational practices requiring training. For the failure of the design review and safety analysis event, a 0.5 split in probability is given for training since the need for training would not be readily identified with a lack of a safety analysis.

D. ***Proper Disc Installation.*** A major contributing cause of the accident was apparently improper installation of rupture discs which were used for overpressure protection.[5] The improper installation caused damage to the discs, and reduced their pressure retaining capability. The discs were difficult to install properly. Therefore, in the absence of training, a 0.5 probability is given for improper installation as shown on the bottom three branches considered for this event. For successful training (the top branch), a probability of 0.8 is given for successful installation.

E. ***No Disc Rupture.*** This event considers eight different scenarios, as shown by the eight branch points on the tree. For the case of success of proper disc installation, a probability of 0.1 is given for disc failure under the conditions of the event. For improper disc installation, a probability of 0.9 is given. It should be noted that these probabilities are quite uncertain. In the investigative report, the results of an analysis of system overpressure is provided which indicates that a momentary overpressure transient of over 700 psi could have resulted from the event. The rupture discs were only rated at 150 psi. However, the purge activity had been performed many times in the past with 250 psi rated discs without failure (although it is not stated in the report if a liquid slug had ever been previously formed which caused an overpressure transient). Thus, it is not clear if 150 psi rated discs would have failed or not had they been installed properly.

F. ***Contained Discharge.*** This event considers the possibility that the discharge from the rupture discs (providing overpressure protection) would be routed to a contained environment rather than discharging to the atmosphere, as was the case for the actual event. This event is considered since a previous design of this system did include discharge to a tank which would have contained the AHF release. Furthermore, since AHF is considered a hazardous and toxic material, normal safety practice should have required that the single barrier represented by the rupture discs be backed up by a contained discharge provision. Accordingly, for those four cases in which a design review and safety analysis is provided, the probability of successful containment of the discharge is given a probability of 0.99. For the other cases of no design review and safety analysis, the probability is given 0.9 recognizing that normal practice would be expected to include provisions to contain the release.

G. ***Consequences and Probability.*** The event tree illustrates that this accident represents a rather unusual sequence of events, with an estimated conditional probability of 4.5E-3 given the initiating event (bottom branch on the tree). Further, the tree illustrates the importance of a second independent barrier, in this case isolation of the discharged effluent, which would eliminate the release for all sequences. Also of significance is the importance of design review and safety analysis since the sequences leading to release after this event has been successful (the upper four release sequences in the figure) have a combined probability of 2.2 E-3 versus 1E-2 for the four sequences in which this event has failed. An expansion of the event tree to consider more significant consequences with the failure of additional barriers was not done since the source term (AHF) was limited to the capacity of the purge system (270 lb.).

C.3.4 Contamination Incident at the West Valley Demonstration Project

On June 19, 1987, during normal construction activities, subcontractor personnel were contaminated while installing a pump cable sheath in the nuclear waste tank farm area. Consequently, contamination was spread to other personnel and areas prior to detection at site exit portal monitors.

Figure C.5 is an event tree covering the incident, based on the investigative report which was prepared.[6]

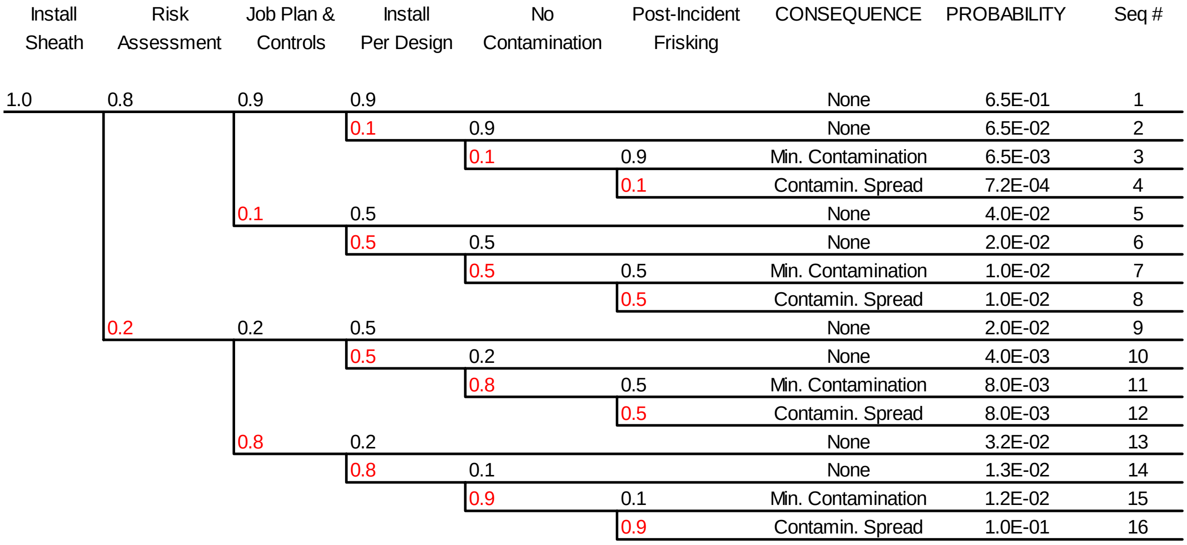
A. ***Install Sheath.*** This was the initiating event for the incident. This activity involved installation of a cable sheath for a pump in a high level liquid waste tank. The area had been previously surveyed and no detectable radioactive contamination was found.

B. ***Risk Assessment.*** This event is the performance of a risk assessment for the work to be done, which was not accomplished prior to the incident. Since the activity to be performed was standard construction practice and no contamination had previously been found in the vicinity of the activity, the performance of a risk assessment would not be expected to have a high priority. However, since the work involved an enclosed area near a source of high level radioactive waste, a risk assessment could have been perceived as appropriate. Thus, a probability of 0.8 is assigned for the performance of a risk assessment.

C. ***Job Plan and Controls.*** This activity involves preparing a job plan and instituting controls on the work. This was not done prior to the West Valley incident. Two cases are considered depending on whether a risk assessment preceded the event. For the case of a successful risk assessment, it is expected that a preparation of job plan and controls would be likely. Thus, a probability of 0.9 is estimated for the success of this event. A probability of 0.2 is estimated for success when the event is not preceded by a risk assessment.

D. ***Install per Design.*** The cable sheath was apparently not installed in accordance with the designers specifications, according to the investigative report.[6] This event is considered because it was concluded in the investigation that had the installation been accomplished according to design specifications, the contamination event would not have occurred. If both a risk assessment and job plan and controls had been previously successful, this event is given a high probability because this previous activity should have identified the importance of the installation procedure. Accordingly, the success of this event is given a probability of 0.9. If only one of these activities had preceded the installation, then a probability of 0.5 is given to the installation procedure being according to design (shown by the two middle branches of the figure). If neither of these activities preceded the installation, then a high probability (0.8) is estimated for the failure of this event.

E. ***No Contamination.*** This event considers the probability of contamination occurring as a result of the activity. If the “Install per Design” event is successful, then, as noted in D preceding, the contamination event is not considered possible. Four different branches are considered, depending on various combinations of the remaining preceding events. If only the “Install per Design” event fails previously



Install Sheath	Risk Assessment	Job Plan & Controls	Install Per Design	No Contamination	Post-Incident Frisking	CONSEQUENCE	PROBABILITY	Seq #
1.0	0.8	0.9	0.9			None	6.5E-01	1
			0.1	0.9		None	6.5E-02	2
				0.1	0.9	Min. Contamination	6.5E-03	3
					0.1	Contamin. Spread	7.2E-04	4
		0.1	0.5			None	4.0E-02	5
			0.5	0.5		None	2.0E-02	6
				0.5	0.5	Min. Contamination	1.0E-02	7
					0.5	Contamin. Spread	1.0E-02	8
	0.2	0.2	0.5			None	2.0E-02	9
			0.5	0.2		None	4.0E-03	10
				0.8	0.5	Min. Contamination	8.0E-03	11
					0.5	Contamin. Spread	8.0E-03	12
		0.8	0.2			None	3.2E-02	13
			0.8	0.1		None	1.3E-02	14
				0.9	0.1	Min. Contamination	1.2E-02	15
					0.9	Contamin. Spread	1.0E-01	16

Figure C.5 West Valley Project

(top branch), then a relatively high probability for no contamination is assigned (0.9) because the worker would be aware of the potential for contamination from the risk assessment which would likely have produced a job plan and controls minimizing the potential for contamination. If the job plan and controls event failed, then a higher failure probability is assigned (0.5) because the worker would not be guided by a job plan with controls. If no risk assessment was performed, but job plan and controls is successful, then a higher probability of contamination (0.8) is assigned since it is not considered likely that the contamination potential would have been identified without a risk assessment. If none of the preceding events are successful, then a high probability (0.9) of contamination is estimated.

F. ***Post Incident Frisking.*** This event considers the possibility that workers would have been frisked by radiation monitors following the work activity. Frisking workers after activity in an area which presents the possibility of contamination is usual procedure at DOE facilities, but was not, for unknown reasons, performed for the West Valley incident. Frisking in this instance would not have prevented contamination of the worker, but would have prevented the spread of the material to other workers and plant areas. Four different branch probabilities are considered depending on the combination of preceding events. (If no contamination occurs, then frisking is not relevant). If only the "Install per Design" event fails, then the probability of frisking is considered high since the existence of potential contamination would likely have been identified, and a probability of 0.9 is estimated. If the job plan and controls fail, then the probability of frisking is reduced to 0.5, and if only the risk assessment is not successful, then the failure probability is increased to 0.9 since it is considered likely that the job plan and controls would not identify the potential for contamination in the absence of a risk assessment. If both risk assessment and job plan and controls fail, then the failure probability is increased to 0.9.

G. ***Consequences and Probability.*** The consequences fall into three categories; none if no contamination occurs, minimal contamination if frisking is successful, and contamination spread if frisking is not successful. The probability of the event (bottom sequence on Figure C.5) which actually occurred is estimated to be 0.1, a rather high value indicating that improvements would be appropriate. The most effective improvement would be to increase the probability of job plan and controls since failure of this event contributes to all of the four high probability sequences. The event tree also illustrates the importance of having job plans and controls when, as in this case, only administrative barriers were available to prevent the incident.

C.3.5 Electrical Arc Incident at Savannah River Site K-Area

On August 28, 1991, a worker was injured by an electrical arc at a substation on the Savannah River Site. The arc occurred when the worker was examining equipment and taking measurements to assist in a future repair activity. The arc apparently occurred when a worker inadvertently moved a ruler containing a metal strip close to an energized switch contact in an open electrical cabinet. A detailed description of the accident can be found in Ref. 7.

Figure C.6 is an event tree which illustrates the event and considers barriers which could have prevented the occurrence. The analysis herein does not attempt to quantify the effects of factors such as worker qualification or safety policy. These elements could have an effect on the calculated probability used in the analysis, but are not sufficiently known to evaluate in this simplified analysis.

A. ***Electrical Equipment Examination.*** This initiating event involved an examination of electrical equipment at a substation for the purposes of assisting in future equipment repairs. The examination resulted in an electrical arc which injured the worker, causing second and third degree burns. The worker was hospitalized for three days.

B. ***Work/lnspection Planning.*** Any work, including inspections, at a substation with exposed contacts energized to 13.8 kV poses obvious hazards to workers. Such work should be planned in a systematic manner to identify the possible hazards involved and the barriers that may be utilized to protect against these hazards. According to Ref. 7, the perception prior to this activity appears to have been that the activity involved “inspection” rather than “work”, and therefore none of the work preparations and precautions normally expected were applicable. As the event clearly demonstrated, inspections are not without risk, and planning is necessary whether the activity is work or inspection. The work plan, at a minimum, should alert the worker to potential hazards, and recommend the utilization of appropriate barriers. In this case, the appropriate barriers are de-energizing the circuits involved (lockout/tagout) and the use of protective equipment such as insulating gloves, goggles, etc. (see Figure 2.1). These physical barriers will be considered as items C. and D. following. The probability of an adequate Work/Inspection Plan has been given a probability of 0.9, (as shown on Figure C.6). This seems a reasonable probability for developing a work plan considering the circumstances surrounding the event. Normally, one would expect a higher probability, but the fact that only minor inspection activities were involved tends to reduce the probability due to the perception of a relatively trivial non-work activity.

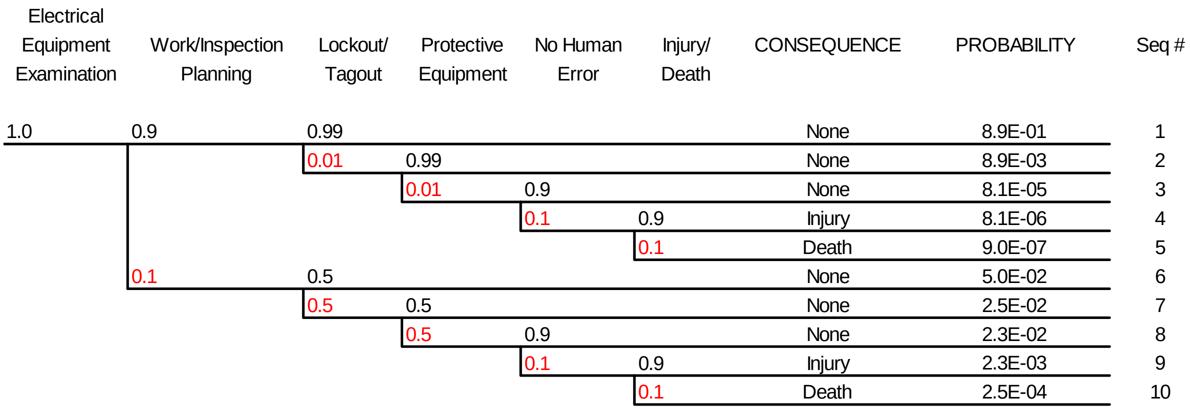


Figure C.6 Electrical arc at SRS

C. ***Lockout/Tagout.*** For the case of an adequate Work/Inspection Plan, when the worker requested access to an energized electrical panel, the electrical supply to the panel would be expected to be locked out and tagged. This should be standard procedure in a work/inspection plan, and is given a high probability of success (0.99), which is consistent with the "rule based" human error rates given in Ref. 2. For the case where the work/inspection plan has not been prepared, a much lower probability is estimated since there would be no guidance prescribing the lockout/tagout procedure. For this case, a probability of 0.5 is estimated for either success or failure of the lockout/tagout event.

D. ***Protective Equipment.*** In this case, the protective equipment of interest is insulating gloves. For the case of an adequate work/inspection plan being previously prepared, the probability of protective equipment use is given a high probability of 0.99, for the same reasons as described in C, preceding, for Lockout/Tagout. Note that, as illustrated on the event tree in Figure C.6, if lockout/tagout is successful, then the use of protective equipment is not considered since the lockout of the power source to the electrical cabinet is sufficient to prevent the accident. For the case of no work/ inspection plan, the probability is raised to 0.5 for failure to use protective equipment, similar to the lockout/tagout probability as described in C.

E. ***Human Error.*** This event considers the error made by the worker of allowing a hand held metal object (a ruler) to come near energized equipment. In this case, an error probability of 0.1 is used corresponding to the knowledge based general human error rate from Ref. 2.

F. ***Probability and Consequences.*** The consequences considered in the event tree are injury and death. Since the switch contact was energized to 13.8 kV, the incident (as pointed out in the investigative report) could have resulted in a fatality. The probability of injury is estimated to be 0.9, and death is given a probability of 0.1. This probability split between injury and death is consistent with data from the national safety council for accidents.[9] The event tree (Figure C.6) clearly shows that the probability of accident sequences which result in injury and death without a work/inspection plan (last two sequences) are much higher than those which are postulated to occur with an adequate work/inspection plant. This illustrates the very significant aspect of preparing a work/inspection plan which affects the probability of both of the important barriers considered in this analysis.

C.3.6 ANL-W Chlorine Release

On April 15, 1994 a release of 20 lbs. of chlorine gas occurred at the ANL-W site at the INEL. The release occurred when an employee attempted to remove a chlorine cylinder from service without first closing a flow control valve. About 20 persons were exposed to airborne chlorine, but none were seriously or permanently injured. A Type A Accident Investigation Board was appointed to investigate the incident. The Board prepared a report on the incident (Ref. 10) which was used in this analysis of the event. Figure C.7 is an event tree which illustrates the important elements of the incident. The following discussion covers each event of the tree.

A. ***Chlorine Cylinder Replacement.*** The initiating event for the incident was the replacement of chlorine cylinders which were used to purify potable water at the ANL-W site. Two chlorine cylinders were housed in a cabinet, one was empty and one was filled with about 90# of chlorine. The worker mistakenly attempted to remove the filled cylinder for replacement with a full cylinder.

B. ***Adequate Work Control.*** This event considers whether adequate work control was in place during the event. Work control in this instance includes safe work permitting, safety analysis, procedures, and training. Since the replacement of the chlorine cylinders was an uncomplicated and reasonably routine procedure, the probability of not having adequate work control is given a value of 0.1.

C. ***Cylinders Properly Tagged.*** Standard ANL-W procedure requires that chlorine cylinders be tagged as "empty", "in-service" or "full". This event is given a probability of 0.9 for success, which is estimated to be a reasonable probability for following the procedure of tagging chlorine bottles which are routinely used at the site.

D. ***Isolation Valve Closed.*** This event considers whether the workman would close the isolation valve prior to attempting disconnect of the chlorine cylinder. The chlorine cylinders had isolation valves as a primary physical barrier to release (see Figure 2.1). Closing of this valve is normal procedure before the disconnect activity. For the case where adequate work control has been successful, this event is given a high probability (.99) since work control procedures would have emphasized this procedure. For the case of not adequate work control, this event is given a 0.5 probability of success for a person not familiar with handling chlorine cylinders. (The worker in this case was not familiar with chlorine cylinder replacement).

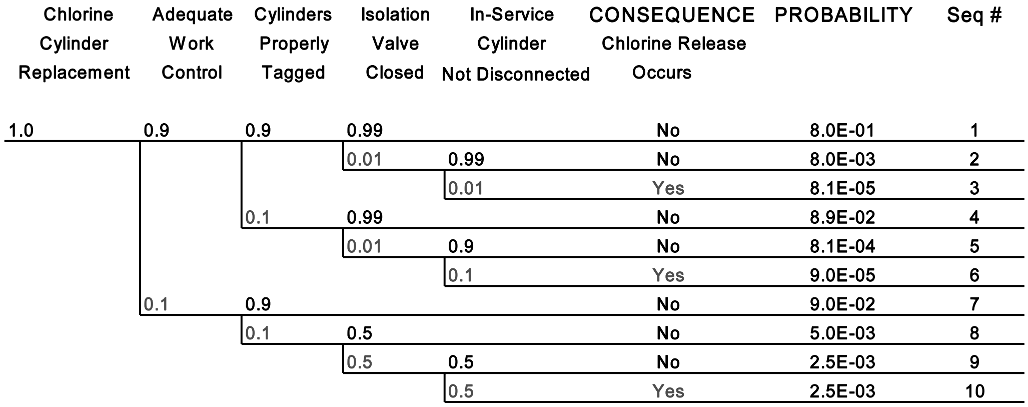


Figure C.7 ANL-W chlorine

E. ***In-Service Cylinder Not Disconnected.*** This event considers whether the worker would disconnect the in-service cylinder which contained chlorine. For the case where adequate work control succeeds and the cylinder was properly tagged ("in-service") according to procedure (top branch), this event is given a low probability of occurring (.01) since the workman would have been alerted from the tag and the adequate work control that this cylinder was not a candidate for replacement. If adequate work control succeeds, and tagging is not successful, this event is given a probability of 0.1 for failure since even if tagging fails, the adequate work control should alert the worker to check the contents of the cylinder by examining the scales which would show the weight of the contents. If both adequate work control and tagging fails, a probability of 0.5 is estimated for failure of this event. This rather high probability is assigned since the worker apparently assumed that both cylinders were to be replaced even though the in-service cylinder was on a scale which showed that the cylinder contained about 90# of chlorine. This should have been an indication that the cylinder was not empty and did not need to be replaced.

F. ***Release Occurs.*** This event considers whether a release occurs based on the sequence of preceding events. Three sequences are shown which result in a release.

G. ***Probability.*** This column estimates the probability of those sequences which result in a release. The actual sequence is estimated to have a probability of 2.5E-3, a moderate probability. The primary barrier which would have reduced the probability of the accident was adequate work control. Adequate work control would have significantly reduced the probability of success for the remaining barriers of isolation valve closed and in-service cylinder not disconnected. (Note that the Hazard/Barrier matrix lists protective equipment as a barrier when handling toxic chemicals such as chlorine. In this case the use of protective equipment would have included fully encapsulated Level B protective clothing. However, this was not considered normal procedure for the routine activity of changing out chlorine cylinders, and further, the protective clothing would not have prevented the release and the exposure of some 20 employees located outside the work area.)

C.3.7 ORNL K-25 Fire Incident

On April 25, 1991 a fire occurred at the K-25 Site TSCA Incinerator Tank Farm. The fire occurred when a polypropylene-fibre absorbent pad used to plug a suction pipe was ignited from the activity of an oxyacetylene torch which was being used to modify a nearby pump mount. The incident was the subject of a Type B investigation. The investigation board published a report on the incident (Ref. 11). This report is the basis for the analysis conducted herein. An Event Tree was constructed to evaluate the incident, and examine the major contributing elements. This Event Tree is illustrated in Figure C.8.

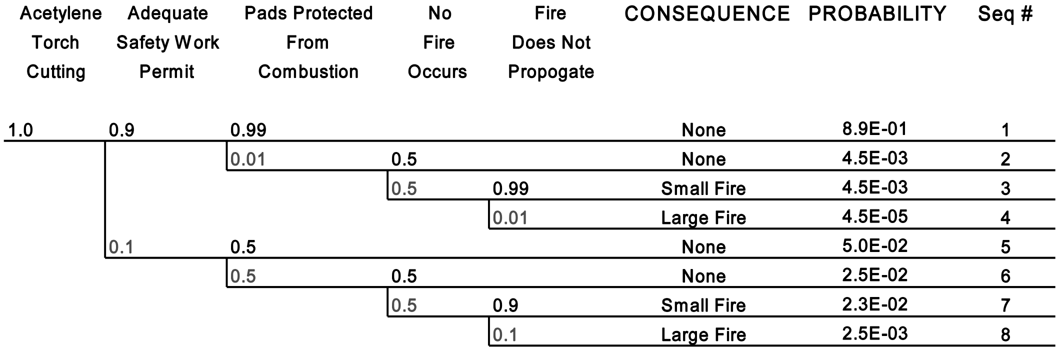
A. ***Acetylene Torch Cutting.*** This is the initiating event on the event tree. This event involved modifying a pump mount by cutting metal in the incinerator tank farm. The modifications were required for installation of a new pump.

B. ***Adequate Safety Work Permit.*** This barrier considers whether an adequate safety work permit is available for the torch cutting operation. According to the investigation board report,[11] an adequate safety work permit should provide, among other provisions, guidance regarding the distance combustibles should be removed from cutting operations, the need to protect open pipes containing combustibles and the need for a fire watcher to stand by for 30 minutes after the work is completed.

C. ***Pads Protected from Combustion.*** This barrier considers whether the polypropylene-fiber absorbent pads were protected from being ignited by the cutting torch activity. This protection could be provided by removing the pads, use of a fire blanket as a barrier between the pads and the torch cutting operations, or wetting down the pads prior to the torch cutting activity. For the case where an adequate safety work permit was previously successful (top branch) the probability of the pads being protected is quite high (.99) since the work permit, as noted in B. above would have been expected to identify the pads as a potential combustible. For the case where the permit failed, a rather high probability (0.5) is assigned for failure of this event. This probability estimate is based partly on the fact that, according to Ref. 11, the pads were not considered by many at the plant to be combustible. In fact, a fire test on the pads was conducted as part of the investigation, and ignition was not achieved. This led to a conclusion that the pads were probably soaked with a combustible liquid which leaked into the pipes, and this resulted in their ignition.

D. ***No Fire Occurs.*** This event considers whether a fire resulted during the activity. This event is only considered if the pads are not protected from combustion. In this case, a probability of 0.5 is estimated for the likelihood of combustion.

E. ***Fire Does Not Propagate.*** This event considers whether the fire, even after being extinguished, could have subsequently propagated into a major conflagration causing widespread damage and contamination. It is possible that the portion of the pad inside the drain pipe could maintain



Acetylene Torch Cutting	Adequate Safety Work Permit	Pads Protected From Combustion	No Fire Occurs	Fire Does Not Propogate	CONSEQUENCE	PROBABILITY	Seq #
1.0	0.9	0.99			None	8.9E-01	1
		0.01	0.5		None	4.5E-03	2
			0.5	0.99	Small Fire	4.5E-03	3
				0.01	Large Fire	4.5E-05	4
	0.1	0.5			None	5.0E-02	5
		0.5	0.5		None	2.5E-02	6
			0.5	0.9	Small Fire	2.3E-02	7
				0.1	Large Fire	2.5E-03	8

Figure C.8 ORNL K-25 fire

combustion even after the fire on the exposed portion of the pad was put out. The investigative report[11] speculates that, since there was no fire watch on duty following the event, the fire, if not completely extinguished, could propagate up the pipe (presumably containing flammable oil which had leaked into the pipe from a waste tank) and cause failure of an isolation valve allowing significant amounts of combustible liquid to be ignited. The probability of this occurring is given a probability of 0.01 for the case when an adequate safety work permit exists. This low probability is given because the work permit would have specified that a fire watch be maintained for 30 minutes after the completion of the work. This watch would be expected to detect the propagation of the fire. For the case when the safety work permit fails, a higher probability of 0.1 is assigned to account for the possibility that a fire watch would not be maintained following the work and the extinguishing of the small fire.

F. ***Probability.*** The probability of the two fire possibilities (large and small) is given in the last column of the event tree. The small fire probability is rather high (2.3E-2). The safety work permit administrative barrier is obviously important in reducing the probability of a fire.

References

1. "Precursors to Potential Severe Core Damage Accidents: 1993 A Status Report," NUREG/CR-4674, Vol. 19, Sept. 1994.

2. See Appendix B.

3. "Type A Accident Investigation Board Report on the June 7, 1993 U-3 Steam Pit Valve Failure Resulting in a Fatality at the Department of Energy Hanford Site," DOE/EH-0335P, August 1993.

4. "Report of Investigation of the Steam Line Accident with Fatal Injuries on October 10, 1986 at Brookhaven National Laboratory Operated by Associated Universities, Inc.," Nov. 14, 1986.

5. "Investigation Report on Release of Anhydrous Hydrogen Fluoride at the Feed Materials Production Center September 29, 1987," DOE-ORO-886, January 15, 1988.

6. "Investigative Report on the June 19, 1987 Radiological Contamination Incident at the West Valley Demonstration Project," WVDP-063, July, 1987.

7. "Type B Accident Investigation Committee Report of Personnel Burn Injury from 13.8 KV Electrical Arc at K-Area Electrical Substation Building 151-2K on August 28, 1991," NS017-79493, September 30, 1991.

8. BNL Hazard/Barrier Matrix.

9. Accidents Facts, 1995 Edition, National Safety Council.

10. “Argonne National Laboratory West Site Release of Chlorine Gas, April 15, 1994,” May 27, 1994.

11. “Investigation of Fire Resulting From Welding Activity at Toxic Substance Control Act Incinerator,” DOE/ORO-967, May 1991.

APPENDIX D

STATISTICAL AND SAMPLING METHODS

APPENDIX D
STATISTICAL AND SAMPLING METHODS

D.1 Determining the Underlying Rate Using Sampling

Occurrences reported through the ORPS are modeled as a Poisson process in which events occur randomly with an underlying rate. A good example of this is radioactive decay. The rate of decay is defined by the half-life and the amount of material, but the actual number of decays in a period of time is random. Detection of particles is a means of sampling. The number of particles detected is neither the underlying decay rate nor the actual number of decays, but it can be used to estimate both. Similarly, sampling the ORPS database does not give either the underlying rate of occurrences or the actual number reported, but it can be used to estimate both. Only the underlying rate will be estimated here.

Estimating either of these numbers from a sample requires that the probability be looked at from a different perspective. Instead of asking the question: "Given an average decay rate of 100 dpm, what is the probability of detecting 50 decays in 5 minutes with a detector of 10 percent efficiency"; the question should be "Given that 50 decays were detected in 5 minutes with a detector of 10 percent efficiency, what is the probability distribution of the actual rate, and the actual number of decays?". This is done using Bayes' theorem.

$$f(\lambda|n) = \frac{p(n|\lambda)}{\int p(n|\lambda')d\lambda'} \qquad (1)$$

where $f(\lambda|n)$ is the probability distribution function of the rate λ and $p(n|\lambda)$ is the probability of n occurrences given rate λ. A similar formulation is used to determine discrete distributions.

The Poisson distribution is given by

$$p(n|\lambda) = \frac{\lambda^{n} e^{-\lambda}}{n!} \qquad (2)$$

Equation (1) is evaluated by substituting equation (2) and integrating. This results in

$$f(n|\lambda) = \frac{\lambda^{n} e^{-\lambda}}{n!} \qquad (3)$$

This gives us the probability density function for the underlying frequency, given that n of these occurrences were found. The mean of this distribution is

$$\mu = n + 1 \tag{4}$$

and the standard deviation is

$$\sigma = \sqrt{n+1} \tag{5}$$

If the n applicable reports were found in a sample of size s of p reports found in a search, the estimates of the mean and standard deviation of the underlying rate for the time interval covered by the reports are

$$\mu = \frac{(n+1)p}{s} \tag{6}$$

and

$$\sigma = \frac{p\sqrt{n+1}}{s} \tag{7}$$

respectively. If these rates are normalized by *h* man-hours worked, the underlying rate r and uncertainty are given by the following.

$$r = \frac{200000 \qquad p(n+1)}{hs} \pm \frac{200000 \qquad p\sqrt{n+1}}{hs} \tag{8}$$

If one set of reports is a subset of another, derived from refining the search criteria, and it is found that there are applicable reports in the sample from the original set which are not included revised set of reports, a correction is required. The additional rate from these left-over reports is

$$r' = \frac{200000 \qquad p'(n'+1)}{hs'} \pm \frac{200000 \qquad p'\sqrt{n'+1}}{hs'} \tag{9}$$

where p' is the number of reports in the original set not included in the subset, n' is the number of applicable reports not in the subset, and

$$s' = \frac{p's}{p} \tag{10}$$

The two rates are added using the equations that follow for combining uncertainties.

D.2 Combining Uncertainties

The following rules are used to combine uncertainties, where μ_i and σ_i are the mean and standard deviation of variable i. For addition,

$$\mu_a = \mu_1 + \mu_2 \tag{11}$$

and

$$\sigma_a = \sqrt{\sigma_1^2 + \sigma_2^2} \tag{12}$$

For subtraction,

$$\mu_s = \mu_1 - \mu_2 \tag{13}$$

and

$$\sigma_s = \sqrt{\sigma_1^2 + \sigma_2^2} \tag{14}$$

For multiplication,

$$\mu_p = \mu_1 \mu_2 \tag{15}$$

and

.

$$\sigma_p = \mu_1 \mu_2 \sqrt{\frac{\sigma_1^2}{\mu_1^2} + \frac{\sigma_2^2}{\mu_2^2}} \tag{16}$$

For division,

$$\mu_q = \frac{\mu_1}{\mu_2} \tag{17}$$

and

$$\sigma_q = \frac{\mu_1}{\mu_2}\sqrt{\frac{\sigma_1^2}{\mu_1^2} + \frac{\sigma_2^2}{\mu_2^2}} \tag{18}$$

The addition and subtraction methods are exact for normal distributions and are very accurate for any distributions that approximate the normal distribution. The multiplication and division methods are exact for log-normal distributions, and are very accurate for distributions that approximate the normal distribution for which the standard deviation is small compared to the absolute value of the mean. The exact value of the mean and standard deviation approximated by equations 17 and 18 is undefined if the second variable can take the value 0.

APPENDIX E

ORPS SEARCH SYNTAX

APPENDIX E
ORPS SEARCH SYNTAX

Each ORPS report consists of narrative sections, codes, and dates. The codes which are frequently used in searches are Nature of Occurrence, which indicates the threshold which was met to require the report; Root, Direct and Contributing Causes which tell why the occurrence happened; Field Office, Area Office, and Facility, which tell where the occurrence happened; and contractor. The narrative fields that can be searched include Title, Description of Occurrence, Immediate Actions, Cause, and Lessons Learned. It is also possible to search all of the narrative sections together. Searches are not case-sensitive.

The terms used in the search can be combined using logical operators. The OR operator finds reports which contain either of the words joined by OR in the applicable field. The + sign may be used instead of OR. To find all reports which contain the word "VOLT" or the word "KV", use either of the following.

```
VOLT OR KV
VOLT+KV
```

The + operator can be used at the beginning of a line to add the cases found by the search to those already found.

The AND operator finds reports which contain both of the words joined by AND in the applicable field. A space or comma can be used instead of AND. To find all reports which contain both the word "VOLT" and the word "KV", use one of the following.

```
VOLT AND KV
VOLT KV
VOLT,KV
```

The AND NOT operator finds reports which contain the first words joined by AND NOT but not the second in the applicable field. The ,- combination can be used instead of AND NOT. To find all reports which contain the word "VOLT" but not the word "KV", use one of the following.

```
VOLT AND NOT KV
VOLT,-KV
```

The wildcard @ can be used to find words based on the same root. To find all word which start with "VOLT", (such as "VOLT", "VOLTS", and "VOLTAGE"), use the following.

```
VOLT@
```

The THRU operator can be used to find a range of words or numbers. The colon can be used instead of THRU. To find facilities in technical areas 10 to 25, use one of the following.

```
TA10 THRU TA25
```

or

```
TA10:TA25
```

Parentheses can be used to change the order of operations. Operations in parentheses are carried out first.