QUALITATIVE METHODS FOR ASSESSING RISK

Jeffery A. Mahn
Sandia National Laboratories
P.O. Box 8500, M.S. 1037
Albuquerque, New Mexico 87185-1037

G. William Hannaman
Science Applications International Corporation
10210 Campus Point Drive, M.S. A1
San Diego, California 92121

Paul Kryska
Science Applications International Corporation
2109 Air Park Road, SE
Albuquerque, New Mexico 87106

"This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000."

ABSTRACT

The Department of Energy's (DOE) non-nuclear facilities generally require only a qualitative accident analysis to assess facility risks in accordance with DOE Order 5481.1B, *Safety Analysis and Review System* [DOE, 1986]. Achieving a meaningful qualitative assessment of risk necessarily requires the use of suitable non-numerical assessment criteria. Typically, the methods and criteria for assigning facility specific accident scenarios to the qualitative severity and likelihood classification system in the DOE order requires significant judgment in many applications. Systematic methods for more consistently assigning the total accident scenario frequency and associated consequences are required to substantiate and enhance future risk ranking between various activities at Sandia National Laboratories (SNL).

Currently, Sandia National Laboratories' Risk Management and National Environmental Policy Act (NEPA) department has initiated a project to develop improved criteria for performing qualitative risk assessments in accordance with the DOE order requirements. Products of this effort are an improved set of qualitative descriptions that permit: (1) definition of the severity for both technical and programmatic consequences that may result from a variety of accident scenarios and, (2) qualitative representation of the likelihood of occurrence. These sets of descriptions are intended to provide, in a qualitative manner, definitions that can be compared with the DOE criteria for assessing facility risks.

NOMENCLATURE, DEFINITIONS AND ACRONYMS

AIHA: American Industrial Hygiene Association.
AL: DOE Albuquerque Operations Office.
D: Demand. Used in conditional failure probability expressions.
DOE: Department of Energy.
EPA: Environmental Protection Agency.
ERPG-1: Emergency Response Planning Guideline (ERPG). The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing other than mild, transient adverse health effects or perceiving a clearly defined objectionable odor [AIHA, 1989].
ERPG-2: The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing or developing irreversible or other serious health effects or symptoms which could impair an individual's ability to take protective action [AIHA, 1989].
ERPG-3: The maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing or developing life-threatening health effects [AIHA, 1989].
ES&H: Environment, Safety and Health.
FREQUENCY: The chance of occurrence in units of per hour or per year and applies to initiating events, component failure and accident sequences. A frequency can be

DISCLAIMER

of times of occurrence during a measured time interval.

HEP: Human Error Probability.

HRA: Human Reliability Analysis.

IDLH: Immediately Dangerous to Life and Health. The IDLH concentration represents the maximum concentration of a substance in the air from which healthy male workers can escape without loss of life or irreversible health effects under conditions of a maximum 30 minute exposure (NIOSH).

IE: Initiating Event.

Kpa: Kilo Pascals.

LIKELIHOOD OF OCCURRENCE: The chance of occurrence of part or all of an accident sequence, encompassing both frequency and probability of success.

LOC: Level of Concern. The concentration of an extremely hazardous substance in the air above which there may be serious irreversible health effects or death as a result of a single exposure for a relatively short period of time (EPA).

NAS: National Academy of Science.

NEPA: National Environmental Policy Act.

NIOSH: National Institute for Occupational Safety and Health.

OR: Operator response as planned.

Pe: Probability of event occurring per year.

PROBABILITY OF FAILURE: The chance of occurrence of failure of a safety element given a demand on the element. It can be determined as the ratio of the number of failures to the total demands on the element from a sample of similar events.

PSI: Pounds per Square Inch.

SCENARIO: Description of an accident from the perspective of consequences as the magnitude of release that represents a group of sequences.

SEQUENCE: A description of an accident sequence from the perspective of the likelihood of occurrence as a set of failure and success descriptions that lead to a consequence. A number of sequences may be grouped together to represent a single scenario, when the consequences are expected to be similar.

SNL: Sandia National Laboratories.

SR: Structural response as planned.

SSC: Structure/System/Component

SY: System response as planned.

TNT: Trinitrotoluene.

TWA: Time Weighted Average. "The time-weighted average concentration for a normal 8-hour workday and a 40-hour work week, to which nearly all workers may be repeatedly exposed, day after day, without adverse effect." [ACGIH, 1994]

WSRC: Westinghouse Savannah River Company.

A. INTRODUCTION

Statement of Problem

The Department of Energy (DOE) is chartered with the responsibility for conducting its operations in accordance with Environmental, Safety and Health (ES&H) laws and regulations. The protection of the health and safety of its workers and the public is a fundamental mandate of the DOE's mission. As a means for fulfilling this mission, all DOE owned nonreactor facilities and projects must have an auditable safety analysis. The safety analysis report provides DOE and its managing contractors with a facility specific formal review of operations; including identification of hazards, their elimination or control, assessment of the risk, and documented management of the operation. Procedures and guidelines for conducting such a safety analysis are described in DOE/AL 5481.1B. This supplemental order specifies the criteria used to evaluate risk assessments of a proposed operation or process. The evaluation criteria consist of two basic components, consequence and frequency. Table 1.3 of DOE/AL 5481.1B [Table 1 in this document] presents the qualitative hazard severity, or consequence evaluation criteria. The frequency probability, or likelihood of occurrence, component is described in Table 1.4 of DOE/AL 5481.1B [Table 2 in this document]. A value of assigned risk is determined as a function of the factors contributing to severity and those factors that contribute to the probability.

When one attempts to apply the criteria, it becomes evident that the definitions provided need to be expanded to more precisely address a range of issues at a particular facility. For example, the severity criteria in Table 1 for evaluating consequences resulting from technical hazards can be expanded to evaluate consequences resulting from programmatic hazards. Programmatic hazards cover a broad spectrum of issues that can present risks in addition to those typically addressed within the technical realm. Within this context, programmatic hazards can include items such as the existence of political, regulatory compliance, or legal entanglements. Using a similar argument, providing a truly qualitative assessment of probability, or likelihood or occurrence, using the criteria in Table 2 leads to many differences of opinion about the adequacy of the assessment. As a result, the DOE criteria for risk decision making presents problems as one attempts to make judgments about the acceptability of risk on the basis of a qualitative assessment of the consequences and likelihood of occurrence of an individual hazard scenario. Without a justifiable basis, such assessments remain subjective, and open to debate about their validity.

Background

Facility specific guidance for performing qualitative evaluations of "technical" risks can be found in a supplement to DOE Order 5481.1B, *Safety Analysis and Review System*, that was issued in January 1988 by the DOE Albuquerque Operations Office (AL). This supplement, DOE/AL 5481.1B [DOE, 1988a] provides "guidance for the AL Safety Analysis

Program". Chapter I, Paragraph 6 of the guidance specifies the format and content for site and facility safety analysis reports. Subparagraph 6.b(7) specifically states that:

"risk will be determined in the following manner....,

(a) The accident analyses should provide a quantitative risk assessment of various postulated accident scenarios....

(b) If it is determined that a quantitative analysis is not practical, then an analysis will be performed using the qualitative descriptors for accident severity and probability of occurrence as specified in Tables 1.3 and 1.4."

The referenced tables are reproduced as Tables 1 and 2. The definitions, from a qualitative standpoint, are vague and often lead to divergent interpretations when applied to a specific facility.

TABLE 1. QUALITATIVE ACCIDENT HAZARD SEVERITY FROM DOE/AL 5481.1B.

HAZARD CATEGORIES	CONSEQUENCES TO THE PUBLIC, WORKERS, OR ENVIRONMENT
Category I - Catastrophic	May cause deaths, or loss of the facility/operation, or severe impact on the environment.
Category II - Critical	May cause severe injury, or severe occupational illness, or major damage to a facility/operation, or major impact on the environment.
Category III - Marginal	May cause minor injury, or minor occupational illness, or minor impact on the environment.
Category IV - Negligible	Will not result in a significant injury, or occupational illness, or provide a significant impact on the environment.

TABLE 2. QUALITATIVE ACCIDENT PROBABILITIES FROM DOE/AL 5481.1B.

DESCRIPTIVE WORD	SYMBOL	NOMINAL RANGE OF FREQUENCY PER YEAR
Likely	A	$Pe > 10^{-2}$
Unlikely	B	$Pe = 10^{-2}$ to 10^{-4}
Extremely Unlikely	C	$Pe = 10^{-4}$ to 10^{-6}
Incredible	D	$Pe < 10^{-6}$

Pe = Probability of event occurring per year.

Purpose of this Document

The purpose of this document is to describe a qualitative risk assessment process that supplements the requirements of DOE/AL 5481.1B. Although facility managers have a choice of assessing risk either quantitatively or qualitatively, tradeoffs are involved in making the most appropriate choice for a given application. The results that can be obtained from a quantitative risk assessment are significantly more robust than those results derived from a qualitative approach. However, the advantages derived from quantitative risk assessment are achieved at a greater expenditure of money, time and convenience. This document provides the elements of a framework for performing a much less costly qualitative risk assessment, while retaining the best attributes of quantitative methods. The approach discussed herein will; (1) provide facility managers with the tools to prepare consistent, site wide assessments, and (2) aid the reviewers who may be tasked to evaluate the assessments. Added cost/benefit measures of the qualitative methodology include the identification of mechanisms for optimally allocating resources for minimizing risk in an expeditious, and fiscally responsible manner.

B. PROCESS FOR QUALITATIVE RISK ASSESSMENT

Both qualitative and quantitative risk assessment techniques are valuable for analyzing the safety of nuclear and non-nuclear facilities. Their aim is to help identify the important safety aspects of the design, operation, and maintenance of a facility by estimating the sources and magnitude of risk. Then priorities for resource allocation can be established on the basis of risk. The DOE uses risk-based methods to refine the safety programs for a range of facilities and operations, including reactors. For example, a facility may use a graded safety analysis approach to identify the risk associated with potential hazards, and then allocate resources for controls to minimize the risk [DOE, 1994b].

Any risk assessment process integrates information from various sources to ensure effective identification of risk issues at specific facilities. Searching for and ranking of potential hazards requires consideration of many factors, including the design, reliability, maintenance requirements, applicable regulations, and operating history. This process should involve personnel with expertise and experience in the facility being assessed, as well as those who understand the methods of defining accident sequences.

The risk assessment process typically begins by dividing the facility into logical sub elements according to processes, physical systems, structures, human actions, and potential initiating events. Hazard screening on each element can help identify the potential contributors to risk. Many risk sequences can be eliminated from additional consideration, if the potential consequences of the hazard are insignificant. This process can also define the role of each safety feature for limiting the frequency or consequences of potential accident sequences. Once complete, the results of the assessment can then be evaluated for acceptability by comparison with the DOE's criteria [DOE, 1994b]. If necessary, risk management actions can be taken to ensure that each accident sequence meets the criteria.

The general development of a process that maximizes the qualitative aspects of a facility risk assessment, as shown in Figure 1, includes hazards screening, bounding sequences, and an accident binning matrix derived along the lines prescribed in DOE-STD-3009-94. The graded approach to risk assessment, suggested in DOE-STD-3009-94, recommends using a matrix as an adjunct to risk assessments. The matrix frequency bins are vertical and increase in the upward direction. The frequency bin boundaries, measured in events per year, range over two orders of magnitude. The consequence bins are horizontal, and increase to the right. The consequence scales generally include health effects, process effects, environmental effects and even cost. The only quantitative aspect is that both the consequence and frequency bins have numerical boundaries.

An aim of the qualitative risk assessment is to select the appropriate "bin" in the matrix for a given accident sequence. The selection should be based on the least effort which gives a reasonable confidence that the bin with appropriate bounds is selected. For system elements with a significant potential consequence, accident sequences can be developed and assigned to risk bins using a variety of means. For the more significant consequence hazards, hypothetical accident sequences can be derived by combining postulated failures in active systems, components and structures with human errors derived from plant operator actions, administrative procedures and management controls. This step may require construction of event trees to illustrate how the various elements combine into an accident sequence. To make a risk assignment, each element of a defined sequence needs to be assigned a probability of occurrence. The combined frequency should consider facility specific conditions such as causal factors associated with equipment, personnel, environment, mission, and configuration. Figure 1 shows the data elements that provide a starting point for qualitative risk assessments. For example, some of the initiator rates and sequences are well known within a factor of three, which easily permits assignment of bounds on the frequencies of certain accidents. Similarly, a known passive system resistance capability for certain accidents permits bounding of the consequences within specific bins. When the elements of an event sequence are properly analyzed, the appropriate likelihood and consequence bins can be assigned. Tools to help the facility manager perform an assessment include example binning assessments as provided in this document. Additional tools may include guidelines, analytical models, and computer support systems. The process shown in Figure 1 helps the facility manager identify the important risk contributors and determine the graded level of risk management attention required.

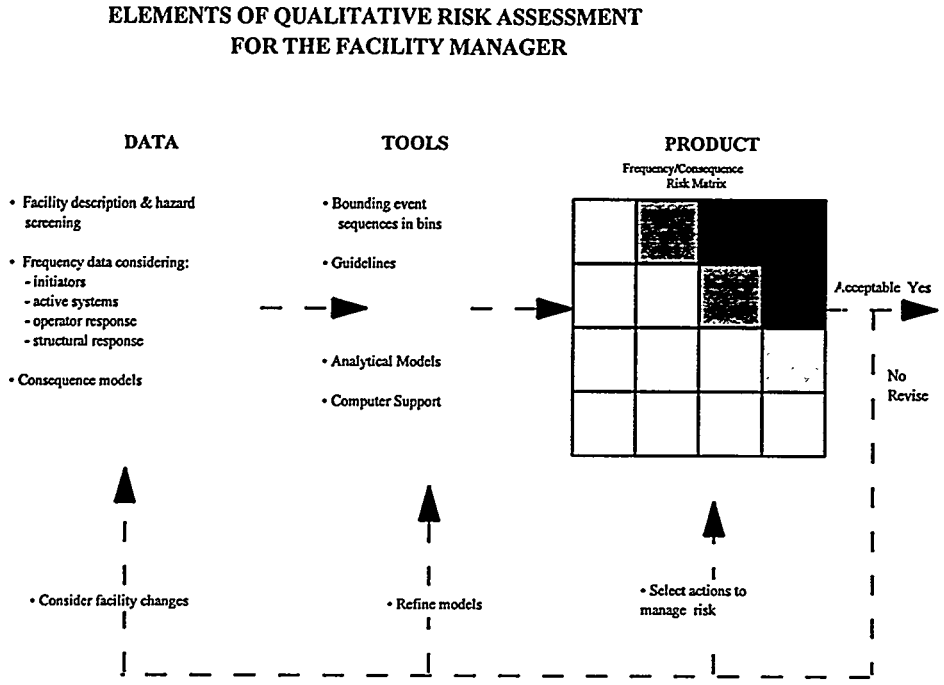

FIGURE 1. QUALITATIVE RISK ASSESSMENT ELEMENTS.

The philosophy depicted in Figure 1 conforms with the "graded approach" recommended in DOE-STD-3009-94 which allows the risk assessment and management resources to be expended in proportion to the risk involved. This adjunct to the graded approach can provide a quick and effective categorization to help prioritize risk management efforts. Details of the development and use of the matrix within this general qualitative approach are contained in the following sections. Depending on the perceived importance for accuracy of the binning as well as on the macroscopic knowledge of behavior of specific accidents, one can use whatever analytical sophistication may be required for high confidence in the choice of binning. The qualitative approach described here provides pre-assigned likelihood of occurrence bins for typical sequences using generic data for initiating events, structure/system/component (SSC) failures and operator errors, and together with experience from many risk studies to support the bin assignments. This allows more resources to be spent on determining the risk management controls that keep accident sequences in acceptable bins rather than on defining accident sequences from independent component failure descriptions typically developed in hazard assessments.

An independent safety review is needed to determine if the assessment properly assigned both the likelihood and consequence required for binning. To perform such a review, qualitative criteria are needed for roughly representing the failure probability of each element of the accident sequence. Then the review can be based on a comparison between the elements of the safety system and typical failure probability ranges for similar sub-elements. To accomplish this comparison, qualitative criteria for describing typical accident sequences in each bin are needed. Then probability scales are used to qualitatively represent the features of each facility (e. g., redundant or diverse backup system for the normally operating protection system which maintains the protective barrier). While the probability assessments typically use detailed fault tree data, some typical values have been developed, and can be used to verify the rationale for the qualitative binning step for accident likelihood. Hence, Section C provides a basic accident structure to support the qualitative assignment of binning frequencies.

These qualitative risk criteria and the risk assessment process establish a framework for addressing safety using a graded approach. This permits the application of resources as needed to control the key systems, components, structures and human activities that can affect the overall risk profile. This approach allows managers to pro-actively allocate resources to hazards to the degree that they are anticipated to produce undesirable consequences. This proactive culture for safety management reduces the potential for discovering important hazards through hindsight alone.

C. DESCRIBING ACCIDENT SEQUENCES

For facilities with hazards beyond typical industrial or office hazards, an initial hazards screening assessment or risk review is necessary to define a representative spectrum of accidents. If potentially high consequence activities are carried out, the facility needs to define a spectrum of accident scenarios to characterize the facility risk profile. The risk profile provides qualitative insights on potential accident sequences ranging from high frequency-low consequence to low frequency-high consequence. This characterization provides the basis for efficiently managing the important risk contributing sequences.

For any facility, a spectrum of accident sequences can be produced by qualitatively linking basic initiating events to the successes and failures of the facility safety elements. These elements can include: normal system and component responses; active back-up system responses; emergency operator actions; and passive systems and structures that act as barriers to the consequences. The assignment of the accident frequency ranges then depend on the reliability of the systems, structures and components for each element of the accident sequence quantification. The consequences are qualitatively assigned by considering the hazard assessment results and the conditions of the barriers as defined by the success and failures in the accident description.

The centerpiece of this task is the logic tree of Figure 2. Figure 2 divides the elements of an accident sequence into 1) initiating events that are caused internally by component failures or externally by events such as fires, flooding, seismic events, etc., 2) system responses, 3) operator mitigating actions; and 4) structural responses. These elements have been represented in the logic tree of Figure 2 as top events. The down branches represent failure conditions, and up branches successful conditions. Bounding probability values are used to assign the initial likelihoods to the accident sequences. Consequences for each bin are estimated by considering the system conditions described by each sequence.

The generic event tree of Figure 2 is used to qualitatively define the sequence logic for potential accidents by combining successes and failures of the systems, components, structures and human actions involved in the accident sequence. A number of key assumptions are made to make binning assignments.

- Hazard Assessment - In order to reach this point in the safety assessment it is assumed that the amount of material stored or processed would exceed protective levels for health and safety of the public and workers if exposed.

- Facility Design - It is assumed that the facility uses tanks, pipes, and pumps for storage or processing of liquid hazardous materials; or fans, ductwork, filters and glove boxes to contain particulate and gaseous materials. In all cases it is assumed that the facility has been designed to the appropriate building codes for the type of hazardous material or plant equipment used.

- Initiating events - It is assumed that the facility is operating in a normal mode when standard initiating events challenge the safety system, although shutdown and transition conditions should also be examined for risk potential. In case of special initiating events, such as fire or failure of rotating machinery, it is assumed that the fuel or energy stored is enough to damage the facility so that functional capability would be lost for a significant time and there is a potential for injury to workers.

- System Response - In some sequences credit for system reliability may be taken for automatic backup systems by reducing the system unavailability in accordance with the level of redundancy or diversity provided to the normal system.

- Human Interactions - The facility operators are expected to have instruments that indicate an approach to a limiting safety setting where mitigating actions may be taken to shutdown the normal systems and stop the process to prevent or limit exposure to the hazardous material or accident threat. These actions are expected to be described in procedures upon which the operators are periodically trained. The level of operator action reliability assigned should reflect the type of training, procedures and information systems actually available.

- Structural Response - Barriers such as vessels, tanks, and concrete buildings are expected to operate passively, that is without support from power systems, to limit release of material. For example, a pressure relief valve might open and close as designed to limit release to a small amount. However, if the relief valve fails in the open position the passive structural barrier would be failed.

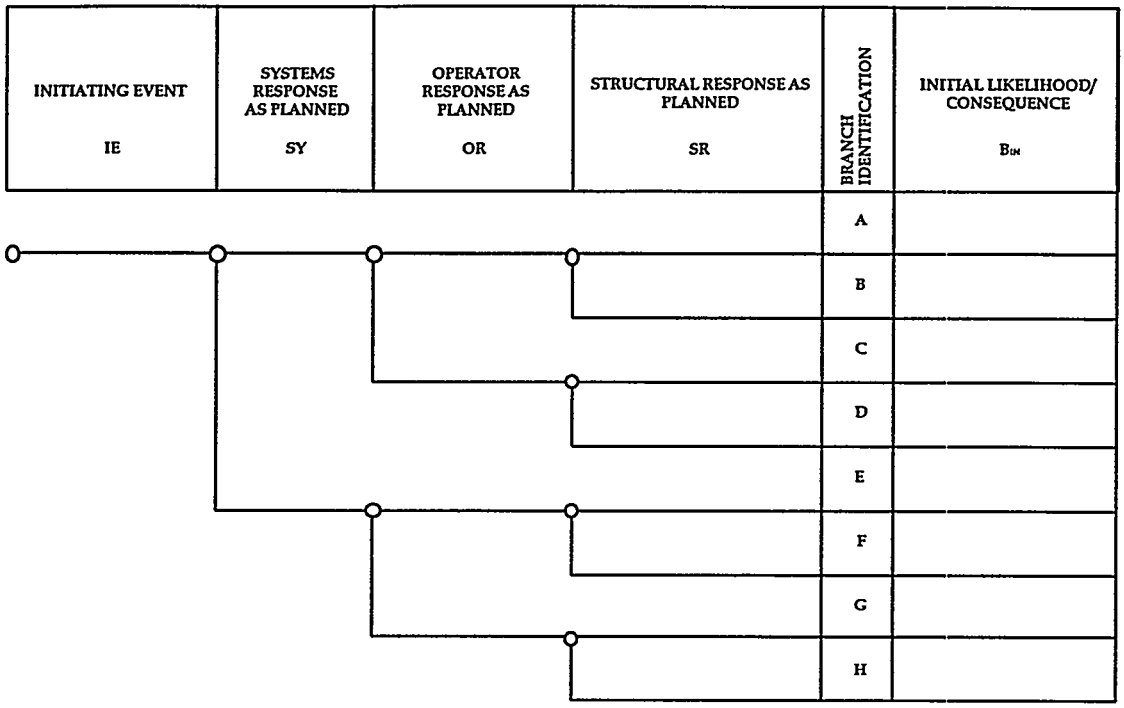

FIGURE 2. GENERIC EVENT TREE FOR ACCIDENT SEQUENCE DEVELOPMENT.

C.1 Frequency Bin Assignment

The frequency of a sequence can be estimated for the purpose of binning by assigning probabilities for each failed element in the sequence. For example, branch E in Figure 2 combines the elements for the initiating event and a failed systems response with successes in operator response and structural integrity. This can be represented as:

$$IE \times \underline{SY} \times OR \times SR = \text{Sequence E} \qquad (1)$$

(where underline means failure)

Assuming a loss of electrical power and a redundant system, substituting typical values from Tables 5 - 9 yields:

$$.3 \times .005 \times .9 \times .95 = .0013/\text{yr.} \qquad (2)$$

This frequency estimate is less than 10^{-2} /year, but greater than 10^{-4} /year, and would therefore be classified in the B frequency bin of Table 2. Table 2 provides the criteria for the frequency bins.

C.2 Combining Likelihood and Consequence Assessments

Using the consequence scales presented in Section D and the likelihood of occurrence values derived from inserting values from Section E into the event tree of Figure 2, the matrix display in Figure 3 for likelihood and consequences has been developed. The qualitative descriptions of accident sequences in each bin provide risk assessment reviewers with target criteria for each bin.

The Figure was constructed from the elements and ranges defined in Tables 1 and 2. The placement of each qualitative description was derived by using conservative values to quantify the sequences in Figure 2 for each initiating event in Table 5, using values from Tables 7 through 9 and considering common cause failures linked to each initiating event. The results from each initiating event were compared and placed in the most conservative likelihood/consequence bins of Figure 2 for each sequence representing a branch scenario. Then the sequence characteristics were qualitatively described and placed in the bins of Figure 3. Even though conservative assessments were used in assigning the generic accident sequence elements to specific bins, conditions can exist where the facility features and operations could produce event sequences that should be in bins A-II or A-I.

Using this mapping approach (Appendix A), both risk assessment reviewers and facility managers should be able to verify the role that risk management activities play in controlling potential accident sequences. Most facilities should be able to show that their accident frequencies can be reduced when credit is taken for the risk management effects of design features, operations and accident management. The frequency of sequences can be reduced through design features such as redundancy or diversity, recovery systems (for example, use of a block valve to isolate a failed open relief valve) and information systems that provide appropriate cues for operator mitigation responses. Operational risk management activities that reduce accident risks include the use of recovery procedures, training on mitigation instrumentation, a consistent preventive maintenance program, surveillance and inspections to verify system/component operability and structural integrity, and focused accident training. Consequence bins can be reduced through the use of specific consequence mitigation systems such as barriers, emergency preparedness, and the use of emergency response procedures by facility operators. The initial qualitative mapping of accident sequences to a risk matrix (such as Figure 3) permits risk assessment reviewers to compare the features and operations of a specific facility with the sequence risk assignment.

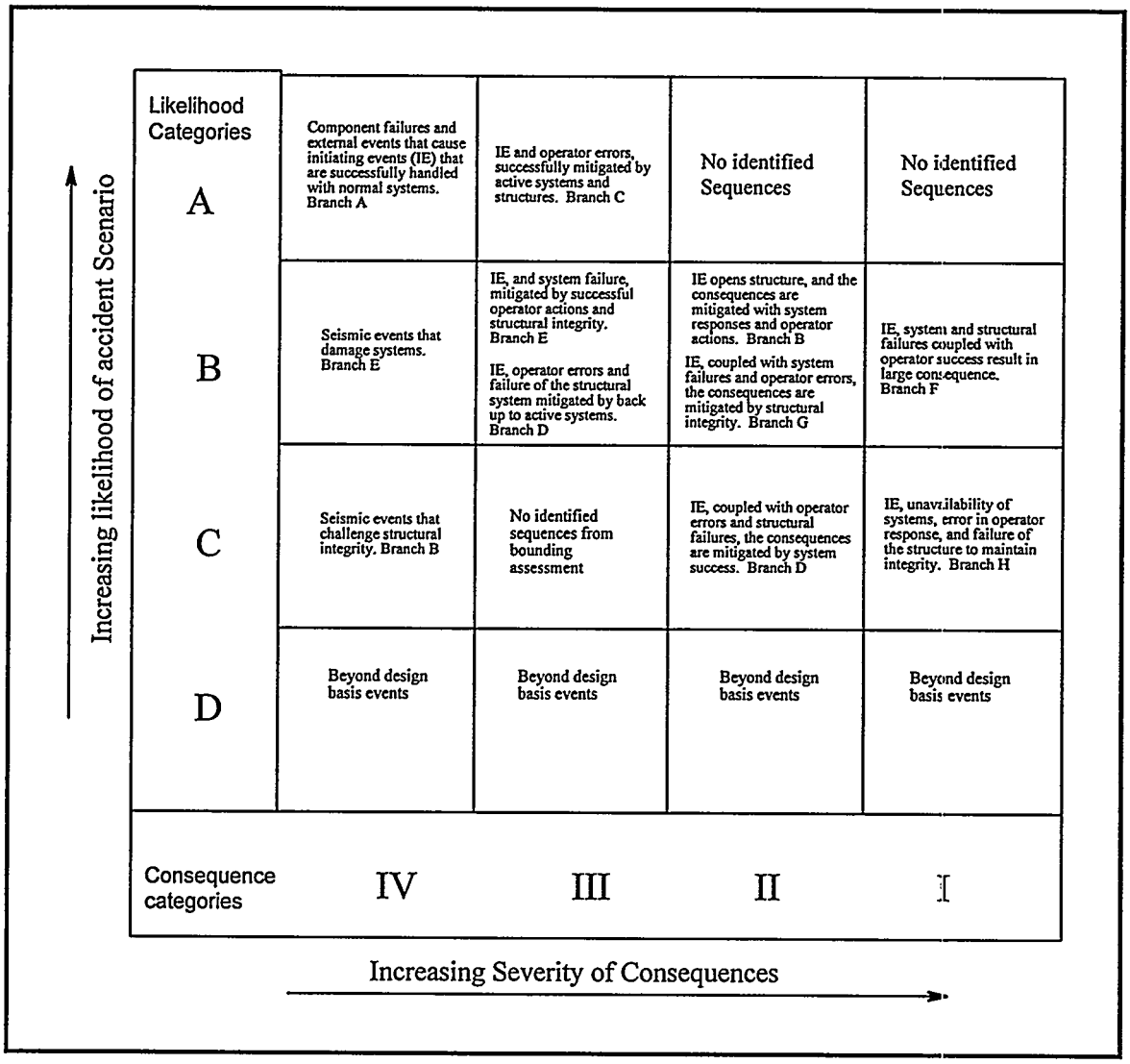

FIGURE 3. MAPPING OF QUALITATIVE DESCRIPTIONS OF ACCIDENT SCENARIOS USING PRELIMINARY BINNING DATA FOR FREQUENCY AND CONSEQUENCE.

D. CONSEQUENCE CRITERIA

This section discusses the different categories of accident consequence, such as human injury, environmental damage, and programmatic impact. The consequence categories are subdivided into four levels of severity which coincide with DOE/AL 5481.1B's nomenclature for accident severity. The section also provides guidance on matching various categories of accident consequences to the criteria developed. When accident scenario consequences include several types, the highest severity consequence should be used in determining accident risk. Table 3 depicts the various consequence categories and the levels of severity for each.

D.1. DOE/AL 5481.1B Consequence Criteria

DOE/AL Supplemental Order 5481.1B, *System Safety Analysis and System,* uses the following four levels to define consequence severity. This order also provides the rank values found in Table 3.

Catastrophic	May cause deaths, or loss of the facility/operations, or severe impact on the environment.
Critical	May cause severe injury, or severe occupational illness, or major damage to the facility/operation, or major impact on the environment.
Marginal	May cause minor injury, or minor occupational illness, or minor impact on the environment.
Negligible	Will not result in a significant injury, or occupational illness, or provide a significant impact on the environment.

D.2. Environmental, Safety and Health Consequences

The consequence categories discussed under this heading address ES&H concerns, such as impact to human health and the environment. Detailed guidance regarding effects of exposure to chemical, radioactive and energy releases are provided.

D.2.1 Human Impact. The criteria provided herein address the consequences of accidents to humans: off site and on site, and the worker/operator. The criteria are broad enough to fit nearly all immediate impact accidents. In addition, further detailed criteria are provided as a means to correlate specific accident consequences to these criteria. All human consequences should be evaluated using these criteria. The detailed criteria developed below for ES&H consequences are health based and attempt to match the criteria found in DOE/AL 5481.1B. The criteria below are not regulation-based and the user should recognize that it is possible to have a negligible consequence that is reportable.

Catastrophic	1) More than one employee death. 2) Significant public injuries including irreversible injuries.
Critical	1) One employee death. 2) Permanent worker disability. 3) Severed limb [not finger or toe]. 4) Permanent paralysis or hospitalization. 5) Minor injuries off site.
Marginal	1) No off site effect. 2) Mendable injuries that may require surgery, hospitalization, outpatient treatment, moderate or less rehabilitation. 3) Injury resulting in two or more worker days lost.
Negligible	1) None to minor injuries requiring none or only little immediate medical attention. 2) Less than 2 lost worker days.

The following subsections provide guidance on categorizing human impact based on certain types of exposures or accidents.

D.2.1.1 Radiological Exposure. Although qualitative risk analyses are typically prepared for facilities that do not have radioactive material inventories, it is possible to have radioactive materials and still prepare a qualitative analysis. Cited below are consequence criteria for exposure to radioactive materials. If the risk assessment investigation of specific sequences determines that a critical or catastrophic exposure scenario is possible, then the analyst should investigate the necessity for preparing a safety analysis report in accordance with DOE 5480.23 and/or a quantitative analysis. Proposed boundaries for radiation exposure have been derived by comparing the human impact levels with studies of radiation exposures that produce those effects.

Catastrophic	> 100 rem off site > 500 rem on site
Critical	> 25 rem off site > 100 rem on site
Marginal	> 0.5 rem off site > 25 rem on site
Negligible	<= 0.5 rem off site <= 25 rem on site

Appendix B provides a brief discussion of the physiological effects of radiation exposure, from which the above criteria were developed.

TABLE 3. CONSEQUENCE CATEGORIES AND LEVELS OF SEVERITY.

Rank	DOE/AL 5481.1B	Human Impact	Environmental Impact	Programmatic Impact
I	Catastrophic	-More than one death. -Significant off site injury.	-> $10,000,000 clean up cost. -Ground water or surface water in immediate danger of contamination.	-Loss > $10,000,000 -Programmatic delay greater than 1 year.
II	Critical	-One death. -Permanent disability, severed limb. -Permanent paralysis or hospitalization. -Minor injuries off site.	-$1,000,000 to $10,000,000 clean up cost. -Significant soil contamination. -Likely long term migration of contamination off site or to water source. However, does not pose any short-term threat to off site or endangered animals and fauna.	-Loss $1,000,000 to $10,000,000 - Programmatic delay between 3 months and 1 year.
III	Marginal	-Mendable injury that may require surgery, hospitalization, and/or outpatient treatment. -Moderate or less rehabilitation. -Injury resulting in 2 or more worker days lost. -No injuries off site.	-$50,000 to $1,000,000 clean up cost. -Minor soil contamination with nearly no potential for contaminant migration.	- Loss $50,000 to $1,000,000 - Programmatic delay between 1 week and 3 months.
IV	Negligible	-None to minor injuries requiring none or only little immediate medical attention. -Less than 2 lost worker days.	-< $50,000 clean up cost. -Small spills or spills that do not immediately enter into the soil. -Contamination that is quickly and readily cleaned up with on site or locally available technology.	-Loss < $50,000 - Programmatic delay less than one week.

D.2.1.2 Toxicological Exposure. This category addresses human exposure to chemical plumes in the gas or vapor form. The consequence levels defined for chemical exposure correspond to recommendations set forth within a DOE subcommittee working on this issue [WSRC, 1994]. Typical quantification of exposure is expressed as parts per million of the chemical substance. A second component of exposure is time. Typical regulatory values are based on 60 minute (for ERPG) and 30 minute (IDLH) exposures. Other values consider the average 40 hour work week (for TWA). It is recommended that the peak 15-minute average chemical concentration be compared with the relevant concentration-limit with no adjustment of the guideline value or the calculated concentration to account for differences between the recommended 15-minute exposure time and the exposure time implicit in the definition of the concentration-limit parameter [WSRC, 1994]. ERPG values are developed by the American Industrial Hygiene Association (AIHA) and can be found in the AIHA's Emergency Response

Planning Guidelines or in Material Safety Data Sheets (MSDSs). If no ERPG value exists, then a hierarchy of default limits can be substituted. In the event that ERPG data is not available, Appendix C addresses alternative values and calculation methods to be used to find a correlation to ERPG values. Although the safety documents to which this criteria apply are to be qualitative only, in order to determine the exposure levels to workers and public, plume dispersion modeling might be necessary.

The following criteria are for exposures within the time frame recommended. It is assumed that within the 15-minute time frame, the worker has the ability to put on protective equipment or exit and sound any necessary alarm. If automatic sensors are used to detect releases, then they are assumed to function in a timely manner to support the 15 minute criteria, unless otherwise stated in the accident sequence description.

Catastrophic	1) Off site exposure greater than ERPG-3
Critical	1) Off site exposure greater than ERPG-2 2) On site exposure greater than ERPG-3
Marginal	1) Off site exposure greater than ERPG-1 2) On site exposure greater than ERPG-2 3) Facility exposure greater than ERPG-3.
Negligible	1) Off site exposure less than ERPG-1 2) On site exposure less than ERPG-2 3) Facility exposure less than ERPG-3.

D.2.1.3 Explosion Effects. Explosion consequences are measured in terms of peak over-pressure, which decreases with distance from the explosion source. The pressure wave resulting from an explosion is the medium through which occur damage to structures and injuries to humans. Appendix D provides a brief summary of the effects of exposure to pressure waves on humans. In order to derive the over- pressure values, the detonated material needs to be converted into TNT equivalent pounds. Appendix D discusses the algorithm for calculating the pressure exposure. The following criteria provide consequence levels related to human exposure to explosions.

Catastrophic	-Peak over-pressure exposure in excess of 200 KPa.
Critical	-Peak over-pressure exposure between 70 and 200 KPa.
Marginal	-Peak over-pressure exposure between 20 and 70 KPa.
Negligible	-Peak over-pressure exposure less than 20 KPa.

D.2.2 Environmental Impact. The following criteria pertain to the environmental damage that an accident might cause. Typical accidents will include spills, accidental discharges, or breaches of material tanks.

Catastrophic	1) Accidents resulting in greater than $10,000,000 in clean up. 2) Ground water or surface water in immediate danger of contamination.
Critical	1) Accidents resulting in greater than $1,000,000 and less than or equal to $10,000,000 in clean up costs. 2) Significant on site soil contamination. 3) Likely long term migration of contamination off site or to water source. However, does not pose any short term threat.
Marginal	1) Accidents resulting in greater than $50,000 and less than or equal to $1,000,000 in clean up costs. 2) Minor soil contamination with nearly no potential for contaminant migration.
Negligible	1) Less than or equal to $50,000 in clean up costs. 2) Small spills or spills that do not immediately enter into the soil. Contamination that is quickly and readily cleaned up with on site or locally available technology.

D.3 Programmatic Impact

Programmatic consequences of accidents have either financial, mission or schedule impacts and are separate from ES&H consequences. Typically, programmatic consequences are not factored into ES&H risk analysis. However, from a total risk management/decision management perspective, the programmatic impacts of facility accidents are important.

D.3.1 Dollar Loss to Facility or Equipment. These criteria pertain to the financial loss or replacement costs of facility components, processes or equipment. Two perspectives are provided in the criteria, either estimated dollar loss or degree of damage to a facility.

Catastrophic	1) Complete or near complete loss of facility 2) Loss in excess of $10,000,000.
Critical	1) Damages requiring extensive repair to facility, including structural testing and design work to refurbish. 2) Loss in excess of $1,000,000.

Marginal	1) Damages requiring minor structural or facility repairs or replacement of equipment. 2) Loss in excess of $50,000.
Negligible	1) Damages requiring only replacement of minor equipment. No structural or building damage. 2) Loss less than or equal to $50,000.

D.3.2 Programmatic Delay or Mission Disruption. This category addresses the impacts that accidents can have on the mission or program function of the facility. The category does not factor in the relative importance of the mission or the research being conducted. The criteria address two types of facilities, process and research types. For process facilities, the criteria regarding time delays should be used. For research facilities, all criteria can be considered, as applicable.

Catastrophic	1) Programmatic delay greater than one year. 2) Complete and irreplaceable loss of research.
Critical	1) Programmatic delay of 3 to 12 months. 2) Extensive loss of program data or research, requiring repetition of testing, work.
Marginal	1) Programmatic delay of 7 to 90 days. 2) Minor loss of data or repeat of test step or phase.
Negligible	1) Programmatic delay of less than 7 days. 2) No loss of experimental data.

E. LIKELIHOOD OF OCCURRENCE CRITERIA

It is intended that the likelihood descriptions account, in a qualitative sense, for the frequency of occurrence of component, system, and structure failures as well as "failures" of administrative controls, and human performance errors. Each description results from characterization of a hazard mitigation barrier "failure" using probability data derived from representative equipment and system failure data, human reliability data, and expert judgment. The key elements that contribute to an accident frequency assessment are described in Table 4.

Facility safety assessments can not be considered complete unless the accidents evaluated address human interactions within the facility as designed and operated [Carnino, 1989]. Many accidents with major consequences have been shown to involve multiple equipment failures and process deviations combined with human decisions and actions [Hannaman and Singh, 1994: Hollnagel, 1993]. Reviews of these events indicate that the relationships between equipment failures and human actions in accidents can be described [Reason, 1990].

A goal for the facility risk criteria is to provide a structure for qualitatively describing sequences involving initiating events, system responses, human actions and structural responses. Once the sequence is understood, risk management actions can be defined using a classification system. Classifying system reliability and human actions by probability or frequency permits the assignment of representative data to each element in a sequence. Equipment failures and human errors have been incorporated into the assignment of each likelihood bin in Figure 3. Limitations must be recognized in using the bin assignments. These include the use of conservative assumptions about human performance issues such as errors of commission, effects of safety culture, and availability of data for addressing uncertainties in calculated probabilities. These limitations do not preclude using risk tools to support decision making for facilities with hazardous processes and materials.

The proposed methodology supports systematic reviews of the assigned frequency for accident sequences. For each element in Table 4, probabilities were used to assign qualitative sequence descriptions to the frequency bins in Figure 3. The probability scale values for each sequence element are provided in Tables 5 to 9. In the first column of each table, a probability range for each element is provided representing an eighty percent confidence interval for typical US facilities designed under consensus codes and standards, using commercially available components, and operators trained at the facility. The value in brackets following most of the descriptions is a nominal value. The frequency estimate for each accident sequence (from Figure 3) can be made by qualitatively comparing the features of the facility with the descriptions in Tables 5 to 9. Adjustment factors are provided to support increases or decreases to the nominal values based on facility-specific conditions such as those shown in the last column of each table.

E.1 Initiating Events

Table 5 provides approximate frequencies for initiating events that should be considered in the qualitative assessment. This list could be expanded to address initiating events needed to characterize specific dependencies between initiating events, system responses, human actions, and structural responses.

E.2 Component Reliability

Table 6 provides approximate frequencies for component failures that could be considered in the qualitative assessment. This list provides initiating events for active systems and unavailabilities for standby systems and structures. These component assessments provide finer detail than the basic event frequencies in Table 5. They also support the binning of sequences involving structural failures.

E.3 System Reliability

Table 7 provides approximate probabilities for system unavailability considering the level of redundancy as the key factor in the qualitative assessment. The failure probabilities address common cause failures of typical system designs. The failure probabilities can be used to assess system failures when assigning sequence frequency bins. Redundancy and diversity

include both the active and backup system elements in a facility process.

E.4 Human Reliability

Since human behavior is a complex subject that does not lend itself to the relatively straightforward reliability models used for component and system assessments, the following descriptions are provided for using Tables 8 to support bin assignments in the likelihood consequence matrix. The proposed classification considers three types of human interactions that typically group all actions which need to be considered [EPRI, 1984]. These are:

(1) Pre-initiator human interactions involving maintenance, testing and calibration,

(2) Initiators of accidents that involve operator awareness of potential accident initiators caused by errors in tests, or re-configured 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.

Human error for these actions can be defined as a mismatch between a performance demand and the human capability to satisfy that demand. Factors that influence human errors have been identified from detailed reviews of events at nuclear power plants. These descriptions have been related to theoretical models of human performance and information processing through testing in simulators. The results indicate that for the purposes of an accident binning assessment [Hannaman et al, 1985], a simple error classification system consisting of three categories: (1) slips, P_1; (2) non-response, P_2; and (3) mistakes, P_3; can be used to qualitatively incorporate human errors in accident sequences. The classification scheme used here can be expanded as needed to integrate additional human errors derived from experience, observations in simulators, and detailed modeling.

Application of the screening values from Table 8 requires assumptions about the accident modeling process and the system being modeled. Methods for qualitative and quantitative screening have been suggested [EPRI, 1984; Poucet, 1987; and Swain, 1988]. To help provide for quantitative screening during logic modeling, assumptions can be made to support trial applications of Human Reliability Analysis (HRA) data [EPRI, 1991]. Data for error probabilities in the human action categories have been derived from the typical human error probability (HEP) values provided in data sources such as [EPRI, 1990a; Whitehead, 1987; hall et al, 1982; Hannaman and Singh, 1994; Kletz, 1988; Swain and Guttman, 1983; Swain, 1987] and previous HRAs (e. g., in response to NUREG-1335 [NRC, 1989]). They are based on the following assumptions about the context of activities carried out in the facilities [EPRI, 1991; EPRI, 1990b]:

- Maintenance and test actions are expected to contribute to system unavailability through an "OR" gate in a fault tree at the hardware fault level. The common mode contributions from testing, and maintenance activities has been considered in the assignment of system level probabilities of failure in Table 7. The HEP contributions to a system failure probability are provided in Table 8. The HEP values can be combined with system or structural unavailabilities to produce an overall assessment.

- Human triggering events for the screening analysis are assumed to be subsumed by the values assigned for specific initiating events, and therefore need not be explicitly addressed. The HEP contributions to an initiating event are provided in Table 8. The HEP values can be combined with initiating event frequencies to produce an overall assessment.

- Mitigation actions are expected to reduce accident sequence likelihoods by incorporating the HEP through an "AND" gate in a fault tree or product term in the accident sequence as shown in the logic of Figure 2. The HEP contributions to mitigation actions are provided in Table 8. The HEP values can be used in quantifying the overall accident sequence frequency as shown in Figure 2.

  a. Screening HEPs for mitigation actions assume that an entire crew performs the functional task(s). The assigned HEP for the action can be adjusted to account for location, the type of action, emergency procedures, specific training, cues for limiting safety settings, time available and independent checks. A classification for procedure based actions includes the following:

     1. "Immediate actions" are those control room type actions that the operators have memorized and used frequently so that they are considered to be skill-based.

     2. "Response actions" are considered to be rule-based, provided in procedures, and involve simple decisions in a control room type environment.

     3. "Recovery actions" outside of a control room type environment are considered to be knowledge-based, involving diagnosis, repair, or development of alternate strategies for recovery.

  b. Mitigation actions which may or may not be proceduralized are assumed to be influenced by time. A time interval is assumed to start with a cue for the required action and end with a change in plant state. The time intervals can be defined as follows:

1. "Short time" is for actions that must be performed in less than five minutes after a cue and are not "immediate actions." It also includes actions whose system performance time is less than two times the period required by a typical crew to perform the action.

2. "Intermediate time" is for actions that must be performed between five minutes and half an hour after the cue. It also includes actions whose system performance time is between two and five times the period required by a typical crew to perform the action.

3. "Long time" is for actions that can be performed a half hour or more after the cue signal is received. It also includes actions whose system performance time is greater than five times the period required by a typical crew to perform the action.

E.5 Structural Integrity

Table 9 provides approximate probabilities for failure of a structural system based on the demand of an accident sequence. The failure probabilities assume long periods exist between demands of the safety features so that latent failure rates dominate the failure probability of the active portions of the structures. The typical structures considered in Table 9 include: drums, walls, and buildings as well as pipes, tanks and vessels designed to specific ASME codes and standards.

TABLE 4. ELEMENTS CONSIDERED IN REVIEW OF ACCIDENT FREQUENCY BINNING RESULTS.

Safety Element	Description of the Safety Element Role
Initiating Events:	Select initiating events that can trigger an accident sequence leading to consequence levels defined above. The initiating events should include: failures of system components that require a system process shutdown, specialized events within the facility such as loss of electric power, flooding, and fires, as well as external events such as seismic events, airplane crashes, etc.
Components:	Determine specific failure frequency for initiating events, or contributors to failure on demand in back up systems of key components that can initiate threats to the structures that act as barriers to hazardous material releases, considering effects of pressure, temperature, mass transport, and aging.
Systems:	Determine approximate system failure probability ranges for active systems considering component configuration and redundancy and diversity levels. These systems require power, and possibly operator interactions to maintain the integrity of a barrier to hazards under specific initiating events.
Human Actions:	Consider mitigating actions listed in emergency procedures such as those used to maintain hazard barriers through planned responses to limiting condition set points, and errors in maintenance actions that increase system unavailability. The basic human error probabilities incorporate the failure modes of mistakes, non-response and slips. These can be adjusted according to the availability of good procedures, training program, and instrumentation available for detection and feedback on actions. Human actions also may consider management control activities such as the frequency of tests, inspections, preventative maintenance, replacements, surveillances, etc. ..
Structures:	Consider ability of plant features that operate passively without electric power or cooling such as tanks with relief valves, building walls, and concrete pits; to withstand event conditions, assuming that the structure meets design requirements. This may include the ability to restore the integrity after an initial loss.

TABLE 5. INITIATING EVENT INFORMATION TO CHARACTERIZE ACCIDENT SEQUENCES.

Frequency Criteria	Description of Example Initiating Events	Adjust-ment Factor	Example Factors for a Facility Specific Adjustment
> 1 per year	Internal active component failures require shutdown to repair (3/yr)	X 3	No maintenance program to detect and repair incipient failures
		X .3	Demonstrated history and proactive preventative maintenance program
.1 to 1 per year	Loss of electric power (.3/yr)	X 3	Single line with single breaker supply
		X .5	Multiple breakers, and dual lines
	Fire in a fire boundary (.1/yr), or external fire	X 2	Flammable material near ignition sources
		X .5	Area minimizes combustible material in fire zone
.01 to .1 per year	Internal flood or leak of hazardous liquid (.05/yr)	X 2	About 100 connections including valves and piping with low pressure piping and threaded joints
		X .1	Use of high pressure piping with welded joints, and in-service inspection program
.001 to .01 per year	Missile generated by rotating equipment or high pressure containers(.008/yr)	X10	Use of non-standard fittings and minimal surveillance
		X .1	Use of continuous monitoring for vibration
	Leak or crack in hazardous material barrier assuming a ASME designed tank (.001/yr)	X 10	No in-service inspections
		X .1	Full inspections and continual monitoring to detect leak before break
<.0001 per year	Seismic event with magnitude greater than used to establish building code requirements		
	Airplane crash into site	X 10	In flight path

TABLE 6. COMPONENT SCREENING INFORMATION TO CHARACTERIZE ACCIDENT SEQUENCES.

Frequency Criteria (Failure Rate per Hour)	Description of Typical Components and Failure Mode	Adjust-ment Factor	Example Factors for a Facility Specific Adjustment
10^{-4} to 10^{-2}/hr	Standby compressors, diesels, pumps won't start or run on demand (10^{-3}/hr)	X 10	Material pumped is abrasive or corrosive (not water)
		X .3	Proactive preventative maintenance program and margin in the design
10^{-6} to 10^{-4}/hr	Active components such as turbines, electric motors, pumps, valves, breakers, and control and protection circuits experience failures that may trigger events (10^{-5}/hr)	X 3	If no periodic maintenance
		X .5	Preventative maintenance program
10^{-8} to 10^{-6}/hr	Transformers short (10^{-7}/hr)	X 10	If overloaded, or no periodic oil testing
	Piping leaks	X 2	Pumping corrosive or abrasive material
		X .1	Pumping water with controlled chemistry
10^{-10} to 10^{-8}/hr	Tanks and structures - leak rupture (10^{-9}/hr)	X 10	No in-service inspections
< 10^{-10}/hr	Steel vessels - leak rupture (10^{-10}/hr)	X .1	Full inspections and continual monitoring to detect leak before break

TABLE 7. SYSTEM SCREENING INFORMATION TO CHARACTERIZE ACCIDENT SEQUENCES.

Conditional Failure Probability on Demand	Description of Typical System and Failure Mode	Adjust-ment Factor	Example Factors for a Facility Specific Adjustment
.5 to 10^{-2}	Single channel system (pump, piping & valves or a motor, breaker and wires). Controlled by signal from system state to provide flow or mixing of material, or transmit electricity. ($5x10^{-2}$/D)	X 10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
		X .1	A proactive preventative maintenance program is controlled under administrative procedures
$5X10^{-2}$ to $5X10^{-4}$	A redundant system which includes two or more trains made up of the elements of the single train including common cause failures. ($5X\ 10^{-3}$/D)	X 10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
		X .1	A proactive preventative maintenance program is controlled under administrative procedures
10^{-2} to $5x10^{-5}$	Partly diverse system of two or more trains using different types of pumps or power (steam vs. AC power); includes common cause failures.(10^{-3}/D)	X 10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
		X .1	A proactive preventative maintenance program is controlled under administrative procedures
10^{-3} to $5x10^{-6}$	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. (10^{-4}/D)	X 10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
		X .1	A proactive preventative maintenance program is controlled under administrative procedures
10^{-4} to $5X10^{-7}$	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. ($5x10^{-6}$/D)	X 10	Material pumped is abrasive or corrosive (not water). Replacement upon failure.
		X .1	A proactive preventative maintenance program is controlled under administrative procedures

TABLE 8. HUMAN ERROR PROBABILITIES (HEPS) FOR ACCIDENT SEQUENCE SCREENING.

Freq. Criteria (HEP)	Description of Human Interaction and Error	Adjust-ment Factor	Example Factors for a Facility Specific Adjustment
$3X10^{-3}$ to $3X10^{-4}$	**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}) 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.	X 10	No written procedure available, or newly defined action; verbal instructions, no checking for completed action, poor equipment/procedure identification label matching.
		X .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.
$1X10^{-2}$ to $1X10^{-4}$	**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}) Typical error modes include slips, non-responses and mistakes.	X 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.
		X .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.
1 to $1X10^{-3}$	**Post-Initiator Actions** - Response actions that are not successful in terminating or mitigating the event. Includes contribution of errors that cause initiating events - covered in initiating event frequencies (.1) Errors include slips, mistakes, and non-responses for control and mitigation actions following an initiating event.	X 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.
		X .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.

TABLE 9. CONDITIONAL FAILURE PROBABILITIES OF STRUCTURES FOR ACCIDENT SCREENING.

Cond. Failure Probability on Demand	Description of Typical Structures and Failure Mode	Adjust-ment Factor	Basis for a Facility Specific Adjustment
.5 to 10^{-2}	A **low pressure, or single wall structure** (e.g., a tank with a relief system designed to the normal code requirements for processing material under pressure or a 55 gal. drum for stored material at atmospheric pressure). ($5x10^{-2}$/D)	X 10	Contains abrasive or corrosive material, and replacement due to failure is upon discovery of leak and loss of material.
	An example failure mode is leak caused by corrosion. If the material in the drum is flammable, dependence on a fire ignition source should be considered.	X .1	A proactive surveillance and inspection program is used to monitor the condition of the structure. The program is controlled under administrative procedures.
10^{-2} to 10^{-3}	A **high pressure, double wall or redundant structure** with multiple penetrations used in pressurized processes. Designed to withstand accident transient pressures and temperatures with relief valves opening, has recloseable leak paths ($5 X 10^{-3}$/D)	X 10	Contains abrasive or corrosive material, and replacement due to failure is upon discovery of leak and loss of material.
	An example failure mode is opening of relief valves and failing to close as a result of the event.	X .1	A proactive surveillance and non-destructive inspection program monitors the condition of the structure. The program is controlled under administrative procedures, and emergency procedures describe how to restore boundary.
< 10^{-3}	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 recloseable leak paths (10^{-3}/D).	X 10	Contains abrasive or corrosive material, and replacement due to failure is upon discovery of leak and loss of material.
	Example failure modes include: 1. Leaving a valve or penetration open after filling, draining, or maintenance. 2. Leaking valve due to erosion or wear. 3. Creating conditions where the load accidentally exceeds the structural strength.	X .1	A proactive surveillance and non-destructive inspection program monitors the condition of the structure. It is controlled under administrative procedures. Procedures for restoration of the barrier are available.

F. CRITERIA FOR RISK ACCEPTABILITY

Using DOE criteria for risk decision making, one must attempt to make judgments about the acceptability of risk. The binning matrix structure can support the risk decision making process by carefully partitioning scenarios to indicate the particular combinations of consequence severity and likelihood of occurrence that are considered to result in acceptably low risk, unacceptably high risk, and intermediate risk levels. For qualitative risk assessments performed in accordance with the DOE order, such a matrix provides 16 bins in which to place the various event sequences as illustrated in the matrix structure of Figure 3.

In a risk matrix, the number of bins can be varied to best represent the overall detail of the facility assessment, and hazards to be managed. The acceptability of the hazard in a specific bin can also vary. An example of acceptability can be drawn from the experience in setting dose limits for public and worker exposure to radiation accidents. Example dose acceptability limits considering frequency of the event for the public and co-located workers are summarized in Table 10. A co-located worker is someone on the same site working in areas near the operator.

Establishing the boundaries and guidelines for risk acceptability is a government responsibility. While such levels may change as technology improves or emphasis changes with regard to environmental issues, the DOE has documented, in draft form, some recommended risk acceptability limits for radiation exposure. These limits should not be considered targets that are allowed, but as upper bounds for gauging the degree to which additional consequence mitigation measures are warranted.

The matrix in Figure 4 summarizes the draft recommendations for acceptability limits based on information from Draft DOE-STD-3005, and DOE-STD-3009. These dose/probability limits can help to define the level of facility risk management activities that can be carried out to balance risk from different hazard scenarios to ensure with high confidence that the limits are not exceeded.

TABLE 10. PROPOSED RADIOLOGICAL EXPOSURE RISK ACCEPTABILITY LIMITS

Receiver	Dose limit	Probability Range	References
Public			
Option 1-Single value	25 REM	Pe $< 10^{-2}$	DOE 3005, pg. A-24 single dose criterion, [DOE, 1994a]
Option 2-Step function	<.5 REM	Pe $>10^{-2}$	DOE 5400.5, DOE 3005, pg. A-25 [DOE, 1994a]
	<5 REM	Pe $<10^{-2}$, $>10^{-4}$	10 CFR 72 [CFR10:72]
	<25 REM	Pe $<10^{-4}$	DOE Order 6430.1A, 10 CFR 100
Co-Located Worker			
	<5 REM	Pe $>10^{-2}$	DOE Order 5480.11 [DOE, 1988b]
	<25 REM	Pe $<10^{-2}$, $>10^{-4}$	10 CFR 100
	<100 REM	Pe $<10^{-4}$	DOE-STD-3005, pg. A-36

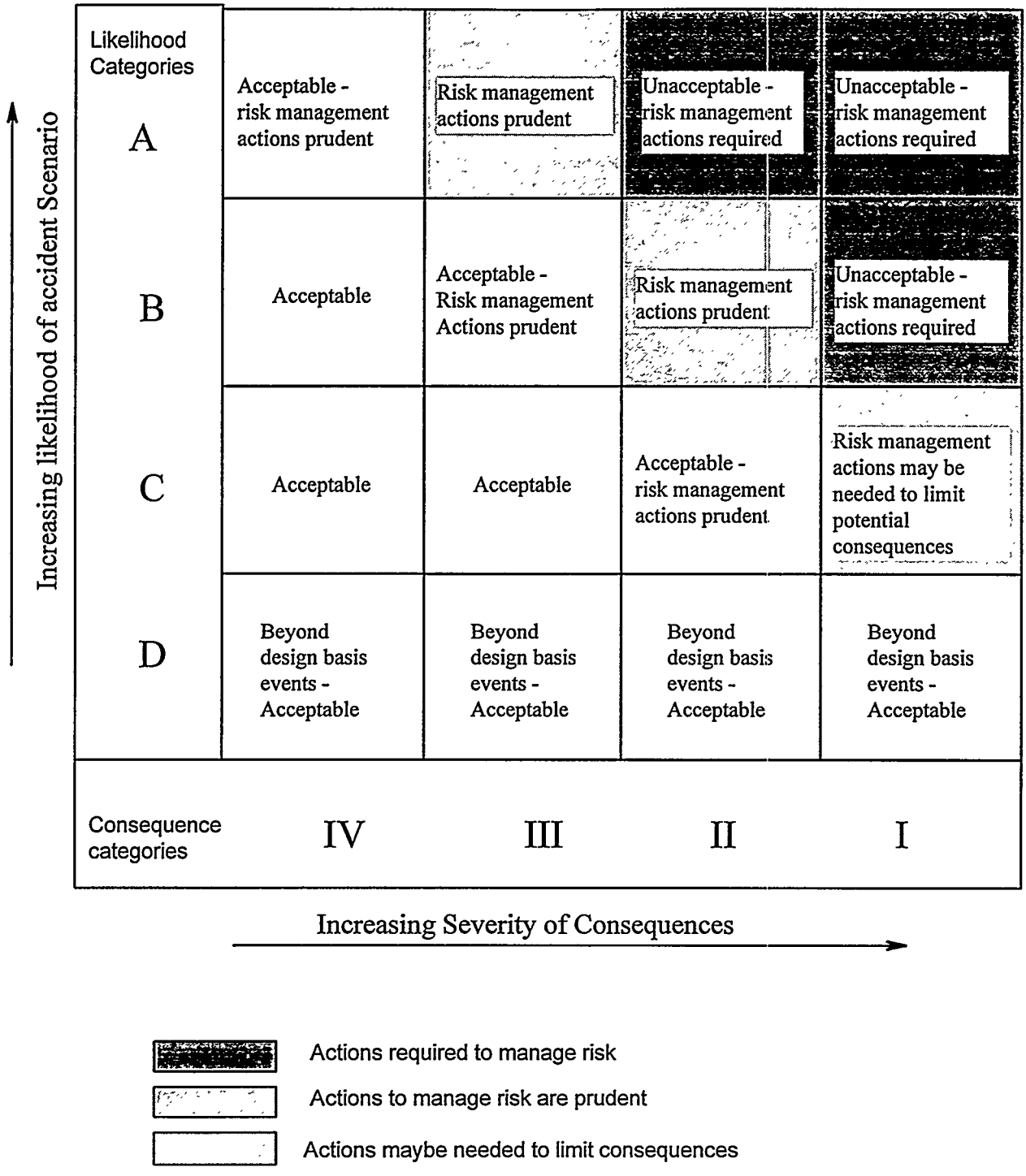

FIGURE 4. SAMPLE ASSIGNMENT OF ACCEPTABILITY FOR BASED ON DOE GUIDELINES.

G. METHODS OF RISK REDUCTION

After the accident scenarios for a particular facility have been identified and verified by the review team, facility management needs to determine if any corrective actions need to be taken. Corrective actions are required for accident scenarios determined to be unacceptable, and recommended for intermediate risk levels. If any accident scenario can be mitigated or prevented through low cost design changes, procedural updates, or modifications to administrative controls, then implementation of the improvement is encouraged.

The following example uses the allocation of descriptive accidents binned in the matrix of Figure 3 and the acceptability matrix of Figure 4 to produce the risk management matrix shown in Figure 5. The example shows how accident sequences in initially unacceptable bins can be moved to acceptable bins. For illustrative purposes consider bin B-I where a typical accident might involve an initiating event with failures of the active systems and structures leading to a large consequence, even though the operator actions in the procedures were correctly carried out. Selecting the bounding values from Tables 5, 7 and 9, the baseline sequence frequency can be determined as the product of the three terms for scenario 5 in Figure 2:

$$(IE)x(\underline{SY})x(\underline{SR}) = (3)x(.05)x(.05) = 7.5\ E\text{-}4/yr. \qquad (3)$$

This event can be moved to bin C-I, C-II, or B-II by applying several risk management options. The risk management options for this type of accident sequence could consider: reducing the frequency or impact of the potential failure modes of the systems and structures, incorporating design features, establishing limits on operation, revising emergency procedures, changing the maintenance and inspection process, and refining administrative procedures.

To illustrate the qualitative frequency assessment, consider a process in a facility that uses ammonia from a large storage tank. The initiating event could be a breach of the control valve connecting the tank to the process. This could result in release of a toxic gas cloud capable of causing death to workers, and the nearby public. Review of Table 6 indicates that a control valve failure could occur with a frequency between .26/yr(8760 hrs/hr x 3 x 0.00001) and .04/yr(8760 hrs x 0.5 x 0.00001). A preventive maintenance program would place this value at the lower limit. Reducing the initiating event frequency would place the sequence in the C-I bin, although it is close to the bin boundary. An examination of the tanks and valving design indicates that an excess flow valve is installed at the tank. Such fast acting valves act as a back up to closing the manual control valve in the process line, closing when the flow exceeds a process demand limit. This valve design feature qualifies as a partly diverse system, so that according to Table 7 the SY term could be reduced from .05 to .001. The final term, SR, in this case is the barrier represented by integrity of the control valve and associated piping. A proactive surveillance and inspection program could reduce the potential for loss of integrity by a factor of ten. This would put the sequence into the C-I bin at $4x10^{-5}$/yr (.04/yr x .001/D).

Assuming that loss of structural integrity was the initiating event, no additional reduction of the sequence frequency can be taken. However, credit for additional safety features that mitigate releases such as distance to the public, and emergency procedures for workers can be considered in limiting the consequences. For example, given the event, off site exposure can be limited by using a fogging system to absorb ammonia vapors into water that can be contained in a basin. This feature alone could move the accident sequence from C-I to C-II. Thus, by combining these three risk management activities the new bin would be C-II as shown by the arrow in Figure 5.

In this manner initial bin assignments can be moved to new bins using qualitative assessments to demonstrate how the system and operators can defend against the sequence failures. The remaining arrows on Figure 5 show potential bin reassignments associated with risk management features. The process of assessing how each sequence is moved from one bin to another helps define risk management features. These can be existing risk management features, potential new features, or changes to procedures. Any of these features could be used to move the sequences to acceptable bins.

The selection of the features to employ is a facility management decision and should be based on the cost of implementation as well as potential trade-offs where the feature might introduce new event sequence considerations.

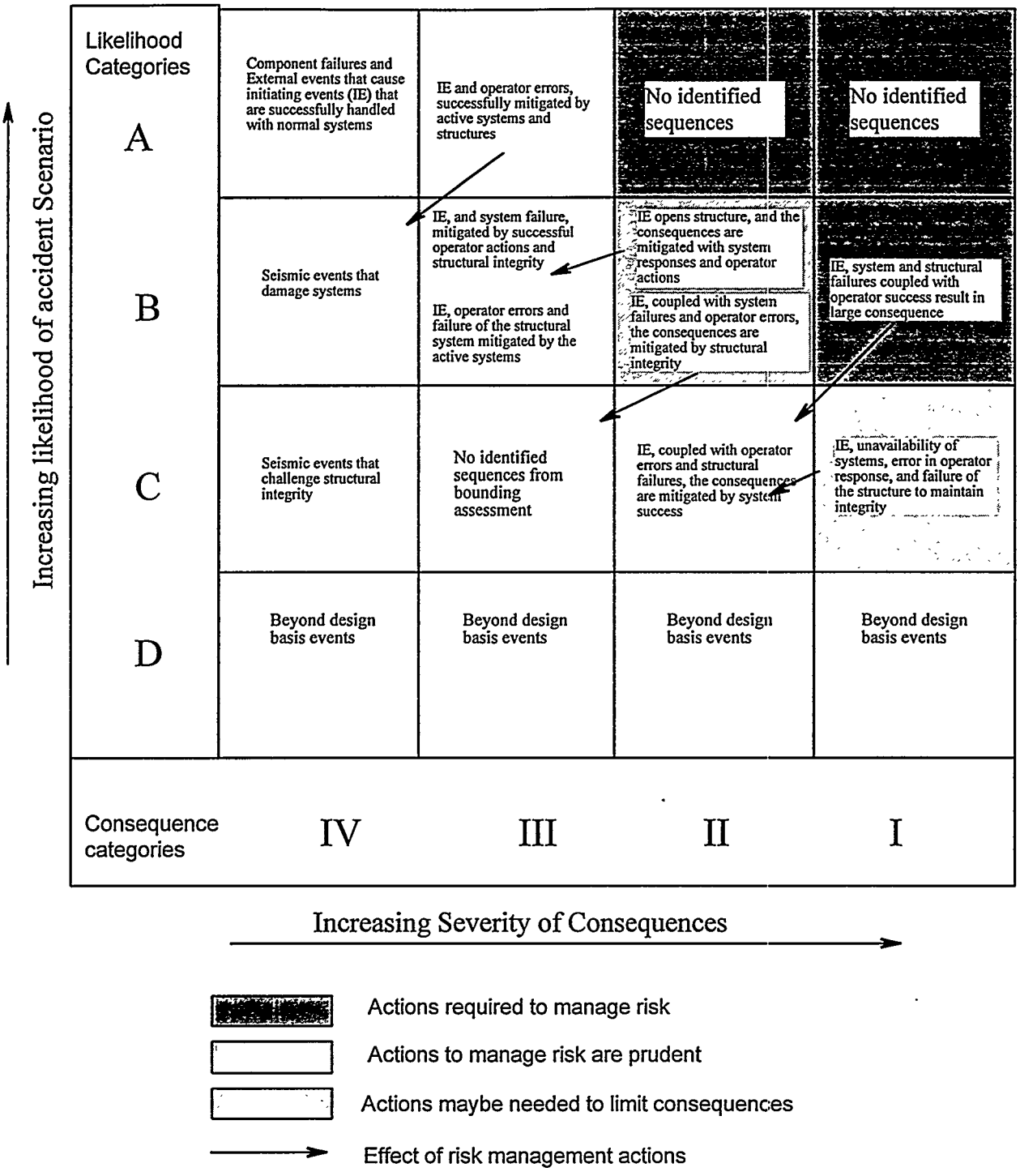

FIGURE 5. APPLICATION OF RISK MANAGEMENT ACTIONS TO REDUCE, CONTROL AND MAINTAIN AN ACCEPTABLE FACILITY RISK PROFILE.

REFERENCES

1. ACGIH, 1994, "Threshold Limit Values for Chemical Substances and Physical Agents and Biological Exposure Indices", American Conference of Governmental Industrial Hygienists, Cincinnati, OH, 1994-1995.

2. AIHA, 1989, "Concepts and Procedures for the Development of Emergency Response Planning Guidelines (ERPGs)". American Industrial Hygiene Association ERPG Committee, December.

3. Army, 1990, "Structures to Resist the Effects of Accidental Explosions." U.S. Army, document # TM5-1300.

4. Carnino A, J. Nicolet, and J. Wanner, 1989, "Man and Risks" Marcel Dekker, Inc. New York.

5. CFR10:72, "Licensing Requirements for the Storage of Spent Fuel in an Independent Spent Fuel Storage Installation", Title 10 CFR part 72.

6. CFR29:1900, 1990, "Toxic and Hazardous Substances, Air Contaminants", Code of federal Regulations: Labor: 29 CFR Part 1910.1000, Subpart Z - pp. 6-33, (Revised as of July 1, 1990).

7. DOE, 1986, "Safety Analysis and Review System". Department of Energy. DOE Order 5481.1B.September.

8. DOE, 1988a, "Safety Analysis and Review System", DOE/AL Supplemental Order 5481.1B. Department of Energy, Albuquerque Operations Office. January.

9. DOE, 1988b, "Radiation Protection for Occupational Workers". Department of Energy. DOE Order 5480.11.December.

10. DOE, 1992a, "Nuclear Safety Analysis Reports". Department of Energy. DOE Order 5480.23.

11. DOE, 1992b, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility DOE Order 5480.23, Nuclear Safety Analysis Reports". Department of Energy. DOE-STD-1027-92. December.

12. DOE, 1994a, "Evaluations Guidelines for Accident Analysis and Safety Structures, Systems, and Proposed Components". Department of Energy. DOE-DP-STD-3005-YR. Feb. 25.

13. DOE, 1994b, "Hazard Categorization and Accident Analysis Techniques for Compliance with Safety Analysis Reports". Department of Energy. DOE-STD-3009-94. Dated July.

14. DOE, 1994c, "Method for the Assessment of Worker Safety Under Radiological Accident Conditions at Department of Energy Nuclear Facilities", U.S. Department of Energy, Office of Environment, Safety and Health. Document # EH-12-94-01, June 3.

15. EPRI, 1984, "Systematic Human Action Reliability Procedure (SHARP)," Electric Power Research Institute, Palo Alto CA. EPRI-NP-3583.

16. EPRI, 1990a, "A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination," Electric Power Research Institute Palo Alto CA. EPRI-NP-6560-L.

17. EPRI, 1990b, "SHARP Methodology Report - Systematic Human Action Reliability Procedure (SHARP) Enhancement Project" EPRI Project 3206 SHARP1, Electric Power Research Institute, Palo Alto CA.

18. EPRI, 1991, "ISLOCA Evaluation Guidelines," Electric Power Research Institute, Palo Alto CA, Sept. NSAC 154.

19. Hall, R. E., J. Fragola, and J. Wreathall, 1982, "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," , November. NUREG/CR-3010

20. Hannaman G. W. and A. Singh, 1994, "Human Reliability Database for In-Plant Application of Industry Data," Proceedings of PSAM-II Volume 1 Published by Apostolakis and Wu University of California, Los Angles CA.

21. Hannaman G. W., A. J. Spurgin, and Y. D. Lukic, 1985, "A Model for Assessing Human Cognitive Reliability in PRA Studies", Proceedings of IEEE Third Conference on Human Factors and Nuclear Safety, 85CH22350 Institute of Electrical and Electronic Engineers, June.

22. Hollnagel., E., 1993, "Human Reliability Analysis Context and Control," Academic Press, San Diego CA.

23. Kletz, T., 1988, "What Went Wrong? Case Histories of Process Plant Disasters", Gulf Publishing Company, ISBNO-87201-919-5.

24. NRC, 1989, "Individual Plant Examination, Submittal Guidance," U.S. Nuclear Regulatory Commission August. NUREG-1335.

25. Poucet, A., 1987, "Results of International Benchmark Exercise on Human Reliability Techniques", Joint Center of European Economic Community, Ispra, Italy.

26. Reason, J., 1990, "Human Error," Cambridge University Press, New York.

27. Swain, A. D. and He. Guttmann, 1983, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report," August. NUREG/CR-1278.

28. Swain, A. D., 1987, "Accident Sequence Evaluation Program: Human Reliability Analysis Procedure", February. NUREG/CR-4772.

29. Swain, A. D., 1988, "Comparative Evaluation of Methods for Human Reliability Analysis." GRS Project RS 688.

30. Whitehead, D.W.,1987, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP)," , Volumes 1 and 2, December. NUREG/CR-4834.

31. WSRC, 1994, "Toxic Chemical Hazard Classification and Risk Acceptance Guidelines for Use in D.O.E. Facilities (U)". Prepared by Westinghouse Savannah River Company, December 15. Document number WSRC-MS-92-206, Rev. 2.

Appendix A. Description of Accident Scenario Mapping to the Frequency Consequence Matrix.

The objective of this appendix is to identify bounding bins for the accident sequences identified in Figure 2. The sequences labeled A through H represent all combinations of success and failure for the three safety feature elements called System Response, Operator Response and Structural Response.

This mapping process bridges between the purely qualitative descriptors of accident sequences found in Figure 3 and typical quantitative models used to estimate system, human, and structural reliability; and assess accident sequence frequency. A number of assumptions must be made to map generic bin assignments to qualitative sequence descriptions of a typical hazardous facility or process. The assumptions involve the initiating events, safety features, consequences, and accident sequence dependencies as described in the following paragraphs.

First, the impact of different initiating events on each safety feature was assumed to vary because of different levels of protection in the design. A spectrum of initiating events was considered to account for changes in reliability of each safety feature with the initiating event. Initiating frequencies from Table 5, as adjusted, were assumed to represent the initiating event frequencies for the key categories of loss of power, fires, floods and other external events. The values for component failures in Table 6 were assumed to contribute to the internal initiating event. The resulting initiating event frequencies for the purpose of qualitatively binning the sequence descriptions for a hazardous material handling facility were assigned as:

Internal	**3./year**
Power	**.3/year**
Fire	**.2/year**
Flood	**.05/year**
External	**.01/year.**

Second, the facility was assumed to be designed under the current codes and standards for fire protection, flood control and seismic protection. The equipment and systems are assumed to be typical industrial grade hardware. The operators are expected to receive on the job training and some special safety training sessions on the use of emergency procedures. Under these normal conditions the safety feature failure probabilities were taken as the nominal values from Tables 7 to 9. These are SY = .05 for a single train system, OR = .03 for a trained operator error probability for an independent error in operations, and SR = .001 for failure of the facility structural integrity (success includes relief valve opening and reclosing). Maintenance errors are assumed to be included in the SY and SR categories, and mitigation failures following more than one failure are typically 0.1 as shown in Table 8.

The third assumption is that the failure probability of one safety feature can be dependent on the success or failure of other safety features. Adjustments to the nominal failure probabilities were made qualitatively to account for potential common cause failures associated with second and third failures. These qualitative adjustments were based on experience in assessing a wide range of facilities. The bolded reliabilities, which represent the basic response to an internally initiated shutdown, were adjusted up or down according to the scales from Table 7 to 9 as summarized below.

SY	OR	SR
1	1	0.05
0.1	0.1	.005
0.05	**0.03**	**.001**
0.005		
1E-04		
5E-06		

Fourth, it was assumed that the bin assignments must initially be conservative to stimulate thinking about why the sequence should be in a lower bin. For this reason the sum of the frequency assessments from the five initiating event categories was used to support the bin assignments. For example, the frequencies assessed for branches D and F were borderline between bins B and C. Because of the consideration of multiple initiators and failure dependencies these branches were categorized in the more conservative frequency bin B. The remainder of the accident branches were clearly in one

frequency bin considering either the total frequency of all initiating events, or the internal initiator frequency alone.

Fifth, to assign consequence bins it was assumed that the facility stored hazardous material in a quantity large enough to cause a catastrophic level one consequence. The accident sequence consequence bins can vary from level I to IV, depending on the protection provided by each safety feature. For facilities with a lower potential consequence the consequence bin categories can be reduced accordingly.

To illustrate specific assumptions associated with each safety element in the context of an accident sequence consider branch H. The frequency bin estimate below is based on the failure of each safety feature for the different initiating events. In addition to the assumptions listed above and in Tables 5 to 9, the following assumptions were made specifically for the accident sequences considered in branch H.

- For the internal initiating event the bolded values for each safety feature were used indicating no special dependencies, and good operating practice for operators.
- In the case of electrical power loss each safety element was reduced in reliability to account for potential system and operator dependency on power and potential sequence dependent failures of the structure.
- In the case of the fire initiating event, it was assumed that the system handles flammable material and an ignition source is present. Good fire protection systems and operator training were assumed available to limit the effect of the fire; however, the potential for structural failure of a tank is assumed to increase when exposed to high temperatures in an uncontrolled fire.
- In the case of floods the upper bound on each safety element was used, because once a flood reaches a critical level, it was assumed that nothing can be done to limit the consequences.
- The flood assumptions were repeated for the external event branch assuming that large seismic forces have an increasing probability of damaging the structure.

The resulting frequency calculation, summarized below, shows that Sequence H lies in the range of 10^{-4} to 10^{-6}/year.

	IE freq.	SY	OR	SR	Seq. Freq.
Internal	3.00	0.05	0.03	0.001	4.5E-6
Power	0.30	0.1	0.1	0.005	1.5E-5
Fire	0.20	0.05	0.03	0.05	1.5E-5
Flood	0.05	0.1	0.1	0.05	2.5E-5
External	0.01	0.1	0.1	0.05	5.0E-6

Total Branch H sequence frequency for all IE: 6.5E-5

The basic sequence assumptions were applied to the other branches as well. Because of the large range in the frequency boundaries for each bin, the assessment for sequence H presented here, which considers multiple initiating events and common cause failures, only shifted the basis for the bin assignment from the lower boundary to just above the mid range in bin C. This shows that the bin assignment for a qualitative generic scenario is not too sensitive.

The consequence assessment for branch H is assumed to be category I, since the bulk of the hazardous material would be released. It is not clear whether the effects of the initiating event or the subsequent damage scenario would produce the greatest negative impact.

Appendix B. Physiological Effects of Radiation Exposure.

The descriptions of physiological effects from radiation exposure found in Table 11 were used to develop the consequence criteria found in Section D.2.1.1 of this document.

TABLE 11. PHYSIOLOGICAL EFFECTS OF RADIATION EXPOSURE (DOE, 1994C).

Dose (REM)	Physiological Effect
100	The risk of prompt fatalities are negligible
250	Expect 10% of exposed population to experience prompt fatalities
500	Prompt fatalities, approaching 100% of exposed population.

Appendix C. Alternative Concentration Limits, Factors and Hierarchy.

The protocol is to use the primary guidelines first and then the alternative guidelines in the order presented in Table 11 for each hazard level when the primary guideline does not exist.

If application of this hierarchy to a particular chemical gives rise to a value for a lower hazard lass that is higher than the value for the next higher hazard class (e.g. ERPG-1 -equivalent value greater than ERPG-2-equivalent value), then that threshold value should be adjusted downwards to match that of the next higher hazard class.

Appendix D. Methodology for Calculating Pressure of an Explosion.

The following equation calculates the pressure wave exposure to an individual or object as a function of the distance from the source:

$$P_i = 29/Z + 552/Z^2 + 1106/Z^3 \qquad (4)$$

where

P_i peak over-pressure, or blast pressure, in psi

Z scaled radial distance, $(Z = R/W^{1/3})$

R radial distance from explosion, feet

W TNT equivalent weight, pounds.

Table 13 provides summary data on the effects of blast exposure to individuals.

TABLE 12. RECOMMENDED HIERARCHY OF ALTERNATIVE CONCENTRATION-LIMIT PARAMETERS [WSRC, 1994].

PRIMARY GUIDELINE	HIERARCHY GROUP	HIERARCHY OF ALTERNATIVE GUIDELINES	SOURCE OF CONCENTRATION PARAMETERS
ERPG-3	1	ERPG-3 EEGL (30 min) IDLH	AIHA NAS NIOSH
ERPG-2	2	ERPG-2 EEGL (60 min) LOC PEL-C TLV-C TLV-TWA x 5*	AIHA NAS EPA 29 CFR 1910.1000 ACGIH ACGIH
ERPG-1	3	ERPG-1 PEL-STEL TLV-STEL TLV-TWA x 3*	AIHA 29 CFR 1910.1000 ACGIH ACGIH

* Applicable only to chemicals whose effects are dose-dependent.

TABLE 13. STRUCTURAL AND PHYSIOLOGICAL EFFECTS OF BLAST PRESSURES. [ARMY, 1990]

EFFECTS	PEAK OVER-PRESSURE (KPa)	(psi)
Physiological:		
Knock personnel down	7	1
Ear drum rupture	34	5
Lung damage	103	15
Threshold for fatalities	241	35
50 % fatalities	345	50
100 % fatalities	448	65