INTEGRATED SAFETY ANALYSIS (ISA)

W. C. Perkins
D. A. Sharp
W. S. Durant
D. K. Craig
J. C. Huang
C. R. Lux
W. M. Massey
P. L. Fisk

JULY 1994

Westinghouse Savannah River Company
Savannah River Site
Aiken, SC 29808

PREPARED FOR THE U.S. NUCLEAR REGULATORY COMMISSION UNDER STANDARD ORDER
FOR DOE WORK DOCUMENT NUMBER 5094056

Westinghouse
Savannah River Company

P.O. Box 616
Aiken, SC 29802

July 26, 1994

EPD-SAE-940011

Mr. Richard I. Milstein
Policy Development and Analysis Staff
USNRC/NMSS, Mail Stop T8A33
1 Whiteflint North
Washington, DC 20555

Dear Mr. Milstein:

INTEGRATED SAFETY ANALYSIS TRANSMITTAL (U)

Enclosed are two copies of the Integrated Safety Analysis document that we have prepared for the Nuclear Regulatory Commission under Standard Order for DOE Work Document Number 5094056. Per your request, we have added additional information to the HAZOP examples to conform to the AICHE guidance, provided a diagram for the checklist example, and expanded the chemical matrix information.

We appreciate the opportunity of performing this work and hope that it will be of significant value to the Commission in the area of integrated safety analysis for the fuel cycle industry. Should you have further comments or questions, please contact me on (803) 644-5410.

Sincerely,

William S. Durant
Senior Advisory Engineer
Safety Engineering Department

INTEGRATED SAFETY ANALYSIS (ISA)

W. C. Perkins
D. A. Sharp
W. S. Durant
D. K. Craig
J. C. Huang
C. R. Lux
W. M. Massey
P. L. Fisk

JULY 1994

Westinghouse Savannah River Company
Savannah River Site
Aiken, SC 29808

SAFETY • RESPONSIBILITY • SECURITY
SRS
SAVANNAH RIVER SITE

PREPARED FOR THE U.S. NUCLEAR REGULATORY COMMISSION UNDER STANDARD ORDER FOR DOE WORK DOCUMENT NUMBER 5094056

Non-Disclosure Notice

The information and/or data contained in this document was developed in support of a contract with the Nuclear Regulatory Commission (NRC). Its content requires the recipient to have a specific and obvious need to know related to the satisfactory completion of the NRC Contract requirements. Permission is not granted, nor shall it be presumed, to publish, use, reproduce, transmit or disclose to another, any information and/or data contained herein, for any purpose other than in the satisfactory completion of the aforementioned NRC Contract work.

INTEGRATED SAFETY ANALYSIS (ISA)

CONTENTS

	Page
LIST OF FIGURES AND TABLES	ix
1. INTRODUCTION	1
1.1 Background	1
1.2 Purpose of the Document	2
1.3 Scope of Applicability	2
1.4 Approach	2
1.5 References	3
2. DEFINITIONS	4
2.1 Terms	4
2.2 Acronyms	6
3. BASIC ELEMENTS OF THE INTEGRATED SAFETY ANALYSIS	8
3.1 Identification of Hazards and Accidents Potentially Affecting Facility	8
3.1.1 Facility Description	8
3.1.1.1 Environs	8
3.1.1.2 Plant Structure(s)	8
3.1.1.3 Work Force	8
3.1.2 Process Description	8
3.1.2.1 Process Operations	9
3.1.2.2 Process Equipment	9
3.1.2.3 Safety Features	9
3.1.3 Definition of Systems to be Analyzed	9
3.1.4 Qualitative Hazards Identification Techniques	12
3.1.4.1 Checklist	12
3.1.4.2 Matrix	14
3.1.4.3 Process Hazards Analysis	14

3.1.4.4 Hazards Identification Technique (HIT) 15
3.1.5 Qualitative Accident Identification Techniques 16
3.1.5.1 Brainstorming 16
3.1.5.2 Hazards and Operability Study (HAZOPS) 17
3.1.5.3 Event Tree Analysis 21
3.1.5.3.1 Introduction 21
3.1.5.3.2 Functional Event Tree Description 22
3.1.5.3.3 Event Success Criteria 22
3.1.5.3.4 Systemic Event Tree Analysis 23
3.1.5.3.5 Example Event Tree 25
3.1.5.4 Failure Modes and Effects Analysis 26
3.1.5.5 Fault Tree Analysis 29
3.1.5.5.1 General Description 29
3.1.5.5.2 Concepts 29
3.1.5.5.2.1 Initiators 29
3.1.5.5.2.2 Enablers 30
3.1.5.5.2.3 Mitigators 32
3.1.5.5.2.4 Faults and Failures 32
3.1.5.5.2.5 Active and Passive Components 32
3.1.5.5.2.6 Fault Classification 33
3.1.5.5.2.7 System Definition 33
3.1.5.5.2.8 Common Cause Analysis 34
3.1.5.5.3 Fault Tree Construction Rules 34
3.1.5.5.4 Computer Codes for Fault Tree Analysis 35
3.1.6 Quantitative Accident Frequency Analysis Techniques 37
3.1.6.1 High-Frequency Events 37
3.1.6.2 Low Frequency Events 37

3.1.6.2.1 Event Tree Analysis 37

3.1.6.2.1.1 Event Tree Quantification 38

3.1.6.2.1.2 Determination of Relevant Failure Experience 38

3.1.6.2.1.3 Other Means of Obtaining Quantitative Data 39

3.1.6.2.2 Fault Tree Analysis 40

3.1.6.2.3 System Failure Analysis 41

3.1.6.3 Non-Credible Accidents 41

3.1.7 Quantitative Accident Consequence Analysis Techniques 42

3.1.7.1 Accident Selection 42

3.1.7.2 Source Term Determination 43

3.1.7.2.1 Masses of Materials Involved in an Accident 43

3.1.7.2.2 Curies of Materials Involved in an Accident 43

3.1.7.3 Consequence Calculation 44

3.1.7.4 Consequence Severity Determination 46

3.1.7.5 Identification of Potential for Propagation of Accidents 46

3.1.8 Determination of Risks of Accidents 47

3.1.8.1 Risk Identification (Qualitative Method) 47

3.1.8.2 Risk Based Analysis (Quantitative Method) 53

3.1.8.2.1 Formats for Presentation of Risk Results 53

3.1.8.2.2 Complementary Cumulative Distribution Functions 54

3.1.8.2.3 Annual Risk 55

3.1.8.3 Uncertainty Analysis (Quantitative Method) 58

3.1.8.3.1 Method 59

3.1.8.3.2 Sources of Uncertainty 60

3.1.8.4 User-Established Criteria 60

3.2 Assurance that Controls are in Place and Capable of Controlling Hazards or Accidents 61

3.2.1 Operational Safety Requirements 61

3.2.1.1 Safety Limits and Limiting Control Settings 61

3.2.1.2 Limiting Conditions for Operation 61

3.2.1.3 Surveillance Requirements 61

3.2.1.4 Design Requirements 62

3.2.1.5 Administrative Controls 62

3.2.1.6 Bases 62

3.3 Assurance that Controls Are Maintained 62

3.3.1 Availability of Safety Systems 62

3.3.2 Preventive Maintenance 62

3.3.3 Testing 63

3.3.4 Administrative Controls 63

3.3.5 Emergency Preparedness 64

3.3.5.1 Introduction 64

3.3.5.2 Emergency Response Organization (Internal) 64

3.3.5.3 Offsite Response Interfaces 64

3.3.5.4 Operational Emergency Event Classes 64

3.3.5.5 Notification and Communication 65

3.3.5.6 Consequence Assessment 68

3.3.5.7 Protective Actions 68

3.3.5.8 Medical Support 68

3.3.5.9 Recovery and Reentry 68

3.3.5.10 Public Information 68
3.3.5.11 Facilities and Equipment 68
3.3.5.12 Training 68
3.3.5.13 Drills and Exercises 69
3.3.5.14 Emergency Management Program Administration 69
3.4. Assurance that Integrated Safety Analysis is Adequate 69
3.4.1 Training of Analysts 69
3.4.2 Management Support 69
3.4.3 Lessons Learned from Accidents 70
3.4.3.1 Management Oversight and Risk Tree 70
3.4.3.2 Root Cause Analysis 71
3.4.4 Good Practices 74
3.4.4.1 Team Approach 74
3.4.4.2 Employee Buy-In 74
3.4.4.3 Incident Records 74
3.4.4.4 Unreviewed Safety Question Determination 75
3.5. References 76
4. DOCUMENTATION 79
4.1 Purpose 79
4.2 Quality Assurance 79

		Page
APPENDICES		A1
APPENDIX A	QUALITATIVE HAZARDS IDENTIFICATION TECHNIQUES	
APPENDIX A.1	Example Checklist Analysis of Uranium Fuel Fabrication	A2
APPENDIX A.2	Example Process Matrix	A6
APPENDIX A.3	Example Chemical Matrix for ADU Process	A8
APPENDIX A.4	The HIT Method	A11
APPENDIX B	QUALITATIVE ACCIDENT IDENTIFICATION TECHNIQUES	
APPENDIX B.1	Accident Lists	B1
APPENDIX B.2	HAZOP Table for UF_6 Dry Conversion	B5
APPENDIX B.3	HAZOP Table for Uranyl Nitrate Bulk Storage	B44
APPENDIX B.4	Example Failure Modes and Effects Analysis for Instrument Air	B60
APPENDIX B.5	Event Tree Example for Scrap Recovery Solvent Extraction Favorable Geometry Vessels	B63
APPENDIX B.6	Qualitative Fault Tree Example for Release of UF_6 During Vaporization	B64
APPENDIX B.7	Fault Tree Example for Scrap Recovery Solvent Extraction Favorable Geometry Vessels	B75
APPENDIX C	QUANTITATIVE ACCIDENT FREQUENCY DETERMINATION	
APPENDIX C.1	Quantitative Event Tree Example for Airborne Activity Release	C1
APPENDIX C.2	Quantitative Fault Tree Example for Nuclear Criticality	C4
APPENDIX D	ASSURANCE THAT CONTROLS ARE IN PLACE AND CAPABLE OF CONTROLLING HAZARDS OR ACCIDENTS	
APPENDIX D.1	Example Operational Safety Requirements (OSRs)	D1
APPENDIX E	ASSURANCE THAT INTEGRATED SAFETY ANALYSIS IS ADEQUATE	
APPENDIX E.1	Management Oversight and Risk Tree	E1
APPENDIX E.2	Example of Root Cause Analysis in Incident Investigation	E12

LIST OF TABLES AND FIGURES

LIST OF TABLES

		Page
3.1-1	Example Hazards Checklist	13
3.1-2	HAZOPS Guide Words	19
3.1-3	Specification of Desired Data for Event Tree Analysis	25
3.1-4	Typical Hazards, Initiators, and Enablers	31
3.1-5	Qualitative Consequence Severity Classification	48
3.1-6	Qualitative Probability Classification	49
3.1-7	Qualitative Risk	50
3.4-1	Uses of an Incident Data Base	75

LIST OF FIGURES

3.1-1	Selection of Overall and Individual Analyses	11
3.1-2	HAZOPS Examination Record	20
3.1-3	Example Event Tree for Airborne Releases	27
3.1-4	Risk Zones	51
3.1-5	Risk Zone Assignment	52
3.1-6	Societal CCDF	56
3.1-7	Individual Risk	57
3.3-1	Prompt Classification Matrix	66
3.4-1	MORT Logic Diagram	72

INTEGRATED SAFETY ANALYSIS (ISA)

1.0 INTRODUCTION

This introduction to the document reviews the background of this project and gives the purpose, scope, and approach of the document.

The working definition of integrated safety analysis is as follows. Integrated Safety Analysis (ISA) is 1) a systematic examination of a fuel processing or fabrication facility and its processes to ensure that all relevant hazards which are associated with normal processing, and credible accidents which could result in unacceptable consequences, have been adequately evaluated, 2) appropriate protective measures capable of performing the desired function have been identified, 3) assurance is provided that the protective measures are maintained, and 4) assurance is provided that the ISA is complete.

1.1 Background

The Nuclear Regulatory Commission (NRC) regulates nuclear fuel cycle facilities under the requirements of 10 CFR Part 40 and 10 CFR Part 70 by the mechanism of a license. The specifics of this license largely form the basis for assessment, inspection and necessary enforcement. The Regulatory and International Safeguards Branch in the Office of Nuclear Material Safety and Safeguards is currently developing regulatory guidance and technical requirements to be used to identify information needed for, and direction to evaluate the safety analysis supplied with, fuel cycle facility license applications for initial approval, amendment, and renewal.

The necessary content of an application for a license includes (10CFR70.22 a[8]): "Proposed procedures to protect health and minimize danger to life or property (such as procedures to avoid accidental criticality, procedures for personnel monitoring and waste disposal, post-criticality accident emergency procedures, etc.)."

The requirement for procedures implies a need for the applicant and the Commission to assess the adequacy of the bases for these documents and practices. This can be accommodated by provisions of 70.22, especially 70.22(d): "The Commission may at any time after the filing of the original application, and before the expiration of the license, require further statements in order to enable the Commission to determine whether the application should be granted or denied or whether a license should be modified or revoked."

The Commission requires a safety demonstration or safety analysis for license actions. As the commercial fuel cycle industry is a mature industry, the focus of the Regulatory and International Safeguards Branch has been on license renewals. Regulatory Guide 3.52, Reference 1, was developed to provide a standard format and content for the health and safety sections of license renewal applications for uranium processing and fuel fabrication. This guide identifies the components of the ISA as:

- Analysis of each step of the process
- Identification of design features, systems, and procedures important to safety for both normal and abnormal conditions
- Adequacy of administrative controls.

Then, Regulatory Guide 3.57, Reference 2 was issued to endorse ANSI Standard ANS-8.19, which outlined minimum administrative programs to support a criticality safety program. This standard specifies a safety analysis with:

- Analysis of normal and credible abnormal conditions
- Identification of clear and adequate controls
- Documentation of analysis and controls
- Independent review

A review of recent renewal applications and the findings of recent incident investigations demonstrate that more guidance for licensees and NRC staff review is necessary. Renewal applications do not show evidence of an ISA that demonstrates that the scenarios which could result in an unacceptable accident are well understood or have been comprehensively compiled. Inasmuch as the issue of accident identification is not well developed, the effectiveness and comprehensiveness of the controls cannot be evaluated. Hence, the basis for procedures does not exist to a necessary or sufficient degree.

1.2 Purpose of the Document

This document is intended to provide technical guidance to the major fuel cycle licensees and license applicants on methods and criteria for conducting Integrated Safety Analysis (ISA). This will assure licensee management and the NRC that the health and safety risks of operation are understood and controlled by the licensee.

1.3 Scope of Applicability

The methods of analysis to be presented here apply to uranium hexafluoride production, uranium enrichment, nuclear fuel fabrication, and the processing of scraps, offgases, and wastes therefrom. Thus, the part of the fuel cycle of concern begins at the start of the uranium hexafluoride production process and ends with the delivery of fuel for transportation to the reactor site.

1.4 Approach

A range of types of safety analysis methods is available for the ISA. The extent of the ISA is governed by an approach that is commensurate with the perceived degree of risk and/or complexity of operation of the subject facility or unit operation being analyzed. A complete ISA can be expected to be an integration of many documents, or differentials, into composite system.

Described below are approaches of increasing complexity to ISA that may be appropriate to a specific facility. In general, the approaches may be categorized as the Qualitative Method (for lower-risk, simpler systems) and the Quantitative Method (for higher-risk, more complicated systems). It is anticipated that most ISAs can be accomplished using qualitative methods.

However, in a few cases, an analysis that begins with the Qualitative Method, based on perceived risk, may yield a result that necessarily leads the analyst toward the more-rigorous Quantitative Method in order to provide a comprehensive, defensible ISA for the facility.

Differences between these methods are described in detail in Section 3.1.

The flow of information associated with an ISA begins with the hazards and accident analysis; a determination of those safety related items that detect, prevent, or mitigate events; incorporation

of controls and limits into a document that defines the envelop of authorized operation; and safe operation of the facility.

1.5 References

1. Standard Format and Content for the Health and Safety Sections of License Renewal Applications for Uranium Processing and Fuel Fabrication, USNRC Regulatory Guide 3.52, Revision 1, November 1986.

2. Administrative Practices for Nuclear Criticality Safety at Fuels and Materials Facilities, USNRC Regulatory Guide 3.57, October 1986.

2.0 DEFINITIONS

2.1 Terms

Accident: An unplanned sequence of events that results in undesirable consequences.

Administrative controls: Provisions relating to organization and management, procedures, recordkeeping, assessment, and reporting necessary to ensure the safe operation of the facility.

Checklist: An experience-based list of hazards, potential accident situations, or other process safety concerns used to stimulate the identification of hazardous situations for a process or operation.

Common cause failure: The occurrence of two or more failures that result from a single event or circumstance.

Consequence: The direct, undesirable result of an accident sequence usually involving a fire, explosion, or release of toxic material.

Credible accidents: Those accidents with a conservatively estimated frequency of occurrence $>10^{-6}$ per year.

Event tree: A logic model that graphically portrays the combinations of events and circumstances in an accident sequence.

Facility: Any equipment, structure, system, process, or activity that fulfills a specific purpose. In practical terms, this definition often reduces to the identification of buildings and other structures, their functional systems and equipment, and other fixed systems and equipment installed therein to delineate a facility.

Facility worker: Any individual located within the defined facility

Failure modes and effects analysis: A systematic, tabular method for evaluating and documenting the causes and effects of known types of component failures.

Fault tree: A logic model that graphically portrays the combinations of failures that can lead to a specific main failure of interest (top event).

Frequency: The number of occurrences per unit time at which observed events occur or are predicted to occur.

Hazard: A source of danger (i.e., material, energy source, operation) with the potential to cause illness, injury, or death to personnel or damage to an operation or to the environment.

Hazard analysis: The determination of material, system, process, and plant characteristics that can produce undesirable consequences, followed by the assessment of hazardous situations associated with the process or activity.

Hazard and Operability analysis: A systematic method in which process hazards and potential operating problems are identified using a series of guide words to investigate process deviations.

Hazardous material: Any solid, liquid, or gaseous material that is toxic, explosive, flammable, corrosive, or otherwise physically or biologically threatening to health.

Initiating event: The first event in an event sequence. An initiating event can result in an accident unless engineered protection systems or human actions intervene to prevent or mitigate the accident.

Limiting conditions for operation: The lowest functional capability or performance level of safety-related structures, systems, or components, and their support systems required for normal, safe operation of the facility.

Limiting control settings: Settings on safety-related structures, systems, or components that control process variables to prevent exceeding safety limits.

Mitigative feature: Any structure, system, or component that serves to mitigate the consequences of a release of hazardous materials in an accident scenario.

Operational Safety Requirements: Those requirements that define the conditions, the safe boundaries, and the management or administrative controls necessary to ensure the safe operation of a nuclear facility, reduce the potential risk to the public and facility workers from uncontrolled releases of radioactive materials or from other hazardous material and from radiation exposures due to inadvertent criticality.

Preventive feature: Any structure, system, or component that serves to prevent the release of hazardous material in an accident scenario.

Rare event: An event or accident whose expected frequency is very small. The event is not statistically expected to occur during the normal life of a facility or operation.

Risk: The combination of the expected frequency (events/year) and consequence (effects/event) of a single accident or a group of accidents.

Safety limits: Limits on process variables associated with those physical barriers, generally passive, that are necessary for the intended facility functions and which are found to be required to guard against the uncontrolled release of radioactive and other hazardous materials.

Top event: The undesired event or incident at the "top" of a fault tree that is traced downward to more basic failures using Boolean logic gates to determine the event's possible causes.

2.2 Acronyms

ALARA - As Low As Reasonably Achievable

APET - Accident Progression Event Tree

ANSI - American National Standards Institute

CCDF - Complementary Cumulative Distribution Function

CEDE - Committed Effective Dose Equivalent

CERCLA - Comprehensive Environmental Response Compensation and Liability Act

DOT - U. S. Department of Transportation

DP - Defense Programs (U.S. Department of Energy Office)

EPA - U. S. Environmental Protection Agency

EPCRA - Emergency Planning and Right -to-Know Act

ESS - Engineered Safety Systems

FMEA - Failure Modes and Effects Analysis

HAZOPS - Hazards and Operability Study

HBT - Hazard-Barrier-Technique

HIT - Hazard Identification Technique

ISA - Integrated Safety Analysis

MIL - Military (U.S. Army)

MORT - Management Oversight and Risk Tree

MOX - Mixed Oxide

NFSC - Nuclear Facility Safety Committee of the Westinghouse M&O Committee

NPRDS - Nuclear Plant Reliability Data System

NRC Nuclear Regulatory Commission

NUCLARR - Nuclear Computerized Library for Assessing Reactor Reliability

ORNL - Oak Ridge National Laboratory

OSHA - U. S. Occupational Safety and Health Administration

OSR - Operational Safety Requirements

PHA - Process Hazards Analysis

PID - Piping and Instrumentation Diagram

PRA - Probabilistic Risk Analysis

PSA - Probabilistic Safety Analysis

QA - Quality Assurance

RCRA - Resource Conservation and Recovery Act

THERP - Technique for Human Error Rate Prediction

WHC - Westinghouse Hanford Company

WIN - Westinghouse Idaho Nuclear Company

WSRC - Westinghouse Savannah River Company

3.0 BASIC ELEMENTS OF THE INTEGRATED SAFETY ANALYSIS

This section discusses the basis elements that comprise an ISA. These elements include: (1) the identification of hazards and accidents potentially affecting a facility, (2) assurances that controls are in place and capable of controlling hazards or accidents, (3) assurances that these controls are maintained, and (4) assurances that the ISA is adequate.

3.1 Identification of Hazards and Accidents Potentially Affecting Facility

This section discusses elements of the analysis that are expected regardless of the analysis methods used. These elements include: (1) thorough descriptions of the facility and the processes, (2) a precise definition of the systems to be considered in the analysis, (3) careful identification of all hazards in the process, and (4) complete identification of potential, credible accidents that can result in radiological consequences. It is essential to an integrated safety analysis that a strong basis be provided at the outset, and these four items form such a basis.

3.1.1 Facility Description

This section provides guidance on the contents of the description of the facility. The objective of this description is to define the boundaries of the analysis and identify those facility-specific factors that could have a bearing on potential accidents and their consequences. A thorough understanding of the facility, as demonstrated by documentation, is vital to assure that a complete, accurate analysis can be accomplished.

3.1.1.1 Environs

Give the facility location and the population of the surroundings. Include other industries.

Describe the histories of pertinent natural phenomena, such as winds (tornado, hurricane histories), floods, and other severe weather. Give the seismic activity history of the area.

3.1.1.2 Plant Structure(s)

Describe all of the buildings in the facility that are provided to meet the processing mission of the facility. Information of the design of the principal structures should be furnished in such detail as to support the identification of seismic-resistances and resistance to the other natural phenomena. The materials of construction of the buildings are important regarding fire resistance. Use drawings as necessary.

3.1.1.3 Work Force

Indicate the number of workers in the force, the different skills necessary for operation, and training provided for normal, abnormal, and emergency conditions.

3.1.2 Process Description

Discuss the process elements which involve radioactive material, the associated equipment, and the safety features. A thorough description of these items is important to an ISA. The objective is to identify all factors that could have a bearing on the initiation of accidents and on the consequences of those accidents.

If possible, describe the process in sections (or unit operations) that are essentially isolatable so as to establish a foundation for modeling activities later in the analysis. If dependencies exist between systems, they should be described and analyzed as one large system.

3.1.2.1 Process Operations

Provide a general description of the overall process from the standpoint of how the process works and its chemistry, if any. Identify feed materials, intermediates, and products. Discuss offgas treatment and waste treatment here. Include actual and potential energy sources (such as elevated temperatures, high pressure, high vacuum, high voltage or amperage, microwaves, lasers, reactive chemicals, flammable materials, etc).

3.1.2.2 Process Equipment

Describe each unit operation in some detail and identify its support systems. Include methods and equipment for recycle (e.g., of scraps) and for waste handling.

3.1.2.3 Safety Features

Recognizing the hazards in each unit operation and the potential for initiation of an accident, describe the safety features of the plant that control each hazard and thereby prevent accidents. Include those safety features to detect the accidents, e.g., fire alarms, detectors. Then, describe those safety features that mitigate the accidents, that is, reduce their potential consequences e.g., sprinklers.

Safety features can be passive (such as containment) or active (such as a flow-control valve).

Procedures important to safety should be identified for administrative control.

Safety features should be adequate to reduce the risk of accidents to acceptable levels. Safety features and controls will have to be reviewed and upgraded or processes redesigned, and another iteration of the ISA should be performed, if the ISA cannot conclude that the risks are acceptable.

3.1.3 Definition of Systems to be Analyzed

Systematically establish the boundaries or limits to be analyzed. Determine if material or energy can be transferred away from an accident in a manner that can adversely affect people, equipment, processes, or the environment. The distance outward is governed by the limits established by various regulators or by consequences judged to be significant by the analyst. Regulations generally are not specific regarding minimum values.

Next, decide on whether a single, all encompassing analysis should be made or whether to subdivide the analysis into smaller increments. Large, single analyses are typically complex and cumbersome but enable the analyst to include all interactions that can occur among systems. Dividing the overall analysis into small independent studies reduces the complexity; however, this increases the possibility of omitting common cause effects or failures. The pragmatic approach is to perform several separate analyses but ensure that both output and input of materials and energies that can affect each analysis are properly considered. This is illustrated in Figure 3.1-1.

In system A, the energy (E) released by an accident does not have an impact beyond the system boundary. The materials (M) released do not impact other systems but do contribute to the impact on the overall analysis. System A is, therefore, a candidate for an analysis independent of the other systems to be considered.

In system B, the energy released by an accident adversely impacts system C. The materials released do not impact other systems but do contribute to the impact on the overall analysis. The effects of the materials released from this system define the envelop of the overall analysis. Because system B is unaffected by the other systems, it too may be analyzed independently. However, the energy impact from system B to system C must be considered in the analysis of system C.

In system C, the energy released by an accident adversely impacts system D, and the materials released from system D adversely impact system C. Because of the interactions of the two systems, consideration should be given to analyzing both systems together to avoid omitting common cause effects that the interactions might have.

Examples of accidents that might fall into the various categories could be an uncontrolled chemical reaction in system A, an explosion in system B that damages equipment in system C, and a fire in system C that releases flammable gases in system D which, in turn, intensifies the fire in system C and propagates to system D.

Each system must be analyzed separately for each accident. Overall risk is determined later as discussed in Section 3.1.8.

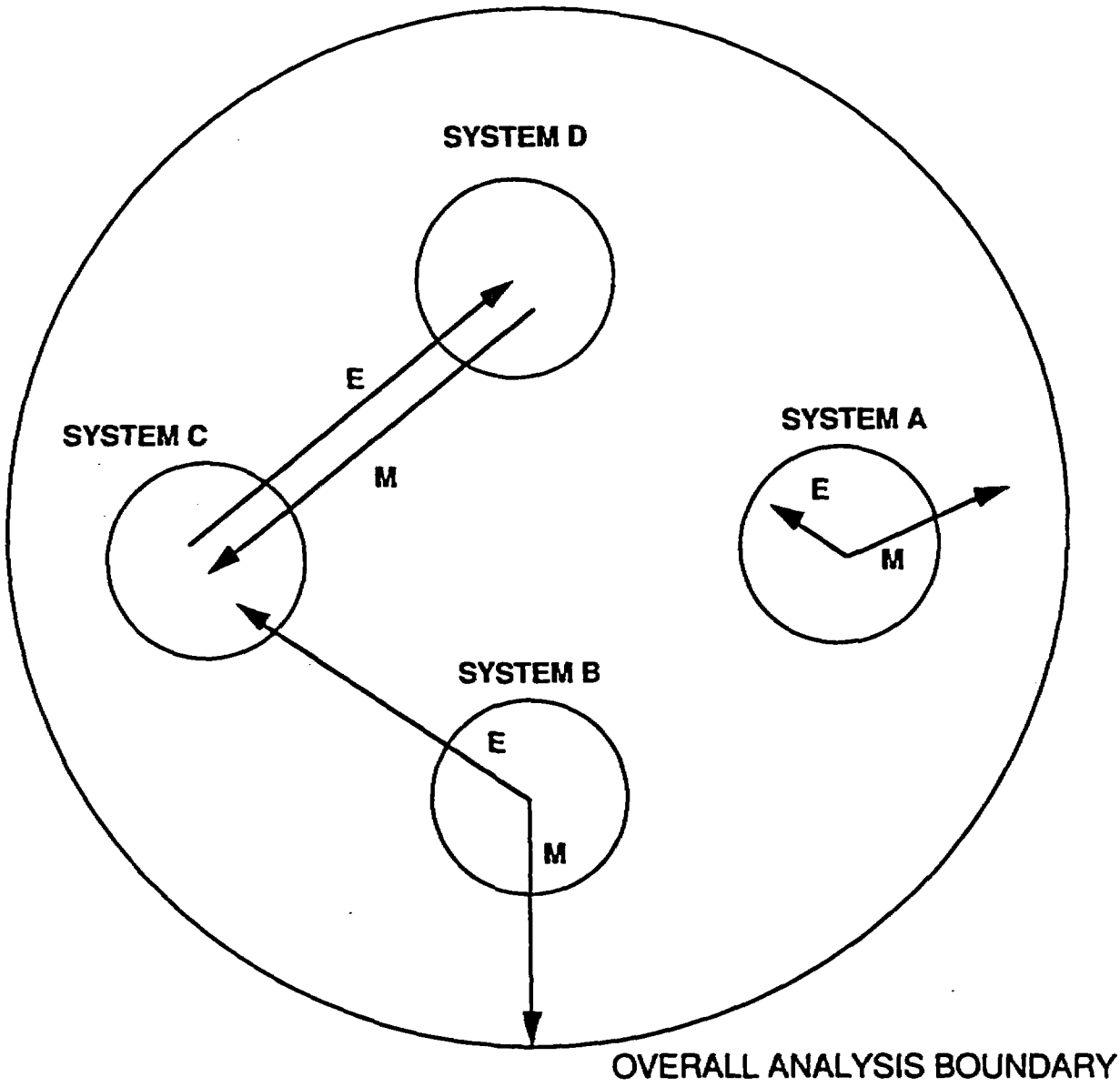


Figure 3.1-1 Selection of Overall and Individual Analyses

3.1.4 Qualitative Hazards Identification Techniques

Describe methods of hazard identification in detail with appropriate examples to aid the analyst or user. The objective is to identify all of the hazards associated with the process or unit operation being analyzed. The hazards should be characterized in the level of detail needed for the analysis and for the report.

A hazard is a source of risk. Usually, it is a necessary part of the process. The hazards of concern here are associated with process startup, operation, shutdown, and maintenance activities, not construction of the facility nor equipment installation.

The hazards to be considered in the ISA are those deriving from the processing of radioactive materials and those that can affect radiological safety, including fire. Ordinary industrial hazards, chemical hazards, and occupational hazards are not included unless they have potential radiological consequences. A discussion of hazards in chemical processes is found in Reference 1.

Natural events, such as earthquakes, and external events, such as aircraft crashes, should be considered and may be screened out only if the risk is negligible.

Ideally, all hazards have been identified during the design of the process, and appropriate safety features have already been incorporated into the facility. However, new hazards may have been introduced along with process changes, enhancements, or improvements in the versatility of the process.

Examples of various techniques are presented in this document except where the examples are voluminous; then references to source documents are given.

3.1.4.1 Checklist

A checklist is a predetermined list of hazards that are generally present in a particular process or unit operation. The analyst needs only to identify and specify which items on the checklist are present and which are not.

The list of generic hazards is short. A simple example is given in Table 3.1-1. The left column in the table is the checklist in generic form. The middle column would be filled in by the analyst to identify the specific form of the hazard in the process in question. The right column is for information only; it identifies the concern (accident) should controls over the hazard fail and provides information later when the accidents are identified. This checklist can be copied by the analyst and expanded to include other hazards and/or examples applicable to the specific analysis.

Checklists are most useful for relatively simple systems where common cause effects are minimal. They are less effective for systems involving chemical reactions.

Table 3.1-1 Example Hazards Checklist

Hazard Type	Example	Potential Accident
1. Hazardous Material		
Fissile Material	Uranium	Criticality
Powdered RAM[a]	Uranium Oxide Powder	AA Release[b]
Liquid RAM	UF_6	AA Release, Liquid RAM Release
Dissolved RAM	Scrap Uranium Recovery	Criticality, Liquid RAM Release
Combustible Solids [c]	Recovery Trash	Fire
Combustible Liquids[c]	Recycle Extractant	Fire
Flammable Vapors[d]	Recycle Extractant Diluent	Fire
Flammable Gas	Hydrogen	Explosion, Fire
Unstable Chemicals[d]	Red Oil Ammonium Nitrate Nitric Acid	Explosion
2. Hazardous Operation	Welding Torch-Cutting Machining Zr Alloy	Fire
	High Pressure Vessels	Explosion
3. Hazardous Event	Earthquake Tornado	RAM Release, AA Release

---

[a]RAM = Radioactive Material
[b]AA = Airborne Activity
[c]Contaminated with RAM
[d]Inside process vessels

3.1.4.2 Matrix

The matrix used in this method is a representation of all possible combinations of hazard and operation that could produce radiological consequences. To the extent that this method uses a checklist as one starting point, it can be considered an extension of the method described in Section 3.1.4.1. The difference is that the matrix identifies where the hazards are located in the process as well as the number of locations.

From the descriptions of the process and equipment, a list of unit operations is prepared. These form one side of the matrix. The list of hazards forms the other side. An excellent source of input is the Process Hazards Review (or similar review) conducted for new projects and periodically updated for existing operations. At this point, a meeting should be held with the design engineers or operations engineers to fill in the details of the matrix. Once it is agreed that the lists (unit operations and hazards) are complete, the matrix is filled in to show where combinations of hazard and operation exist. Obviously, many of the matrix nodes will be left blank, because a given hazard will not occur in every unit operation.

Where matrix nodes identify a hazard and its location in the unit operations of the process, the potential for an accident exists. The product of the matrix method is a list of areas for further study, (e.g., "Flammable Solvent in Scrap Recovery-Solvent Extraction"). An example matrix is included in Appendix A.

A second type of matrix is the chemical interaction matrix that shows whether or not the chemicals used, stored, or produced in the facility will react. Such a reaction might release radioactive materials dissolved in the chemicals or in the release of toxic reaction products. An example chemical interaction matrix is shown in Appendix A.

3.1.4.3 Process Hazards Analysis

A process hazard is a hazard that is associated with (1) the facilities and functions needed to manufacture a product or (2) the byproducts of that manufacture, or (3) the wastes generated. These hazards are not associated with the construction of the facility, but are those associated with startup, operation, and shutdown.

The hazards are usually identified from lists of potentially hazardous materials, energy sources or equipment. Use the analyst's experience, expert opinions, facility walk-throughs and reviews of the accident histories of similar facilities. Include likely natural phenomena, such as high winds and low temperatures. In general, this is a "brainstorming" process to focus all available knowledge on the subject, so as to leave no hazard unidentified.

Such an approach will, in all likelihood, generate a list of hazards that should be screened before analysis. The objective of this screening is to eliminate unnecessary analyses. Some screening criteria that have been useful in the past are:

- Willful acts, such as sabotage, should be excluded.
- External events, such as aircraft crashes and meteorites, may be excluded if the risk is negligible. For example, aircraft crashes may be screened out if the facility is not located near an airport. Generally, beyond about five miles distance from an airport, aircraft crashes may be considered as random.

- Hazards addressed by other programs and regulations (e.g., OSHA, RCRA, DOT, EPA) should be included if loss of control may release radioactive materials to the environment.

- Unlikely natural phenomena, such as has never occurred in the history of the site, should be excluded, except for their possible contribution to the criticality analysis. Criticality is in a special category. It represents an accident unique to the fuel manufacturing industry. It is given special treatment because its consequences are not acceptable.

- Hazards routinely accepted by the public are not considered.

The potential consequences of a given hazard should be considered for both normal or abnormal operation. The resulting list of identified hazards is used as a starting point for the next step in the analysis, accident identification.

An example process hazards analysis can be found in: "Example Process Hazards Analysis of a Department of Energy Water Chlorination Process," DOE/EH-0340, September 1993, Reference 2. This method is very good where chemicals are used.

Section 3.1.4.4 Hazard Identification Technique (HIT)

This section explains and demonstrates by example a technique for analyzing systems and operations to identify hazards and needed controls. The HIT method, Reference 3, can be used both as a design tool and as a risk analysis tool. As a design tool, this method identifies requirements for design criteria. This method will define where the critical control points are and will allow the designer to determine under what conditions the controls and Engineered Safety Systems (ESSs) must function. As part of a risk analysis effort, HIT identifies potential accident sequences, which can become part of the safety analysis documentation. As a risk analysis tool, the technique will find the accident initiators, and weak links in the control of the operation. The HIT method can also be used in the design and review of standard/safe operating procedures. Normal, unusual, and maintenance operations can all be analyzed by using this technique.

This method is also known as the Hazard-Barrier-Technique or HBT.

All components of an operation are listed, and a complete set of initial condition interfaces is created to begin the process. Although tedious, it is important that this setup be done thoroughly. It defines and bounds the operation and determines the completeness of the subsequent analysis.

Interfaces, both initial condition and subsequent, are created by pairing each item on the component list with other items on the list. Every pairing that is physically possible is a viable interface.

The setup complete, the next steps of the method follow:

(1) Assign an "active" and a "passive" role to each component of an interface.

(2) Ask if the active component can cause the passive component to change state.

(3) Ask if the change of state results in new interfaces being created.

These three steps are repeated until some logical endpoint is reached. Any "yes" answer to questions in Steps (2) or (3) identifies a hazard and a potential accident.

The HIT method is described in detail in Appendix A with emphasis on application of the technique. Following the description is an example to illustrate this method. The HIT method is very good where interfaces among equipment, energy, and personnel can be readily defined.

3.1.5 Qualitative Accident Identification Techniques

Accidents are events that involve the loss of control over a hazard with resulting consequences. Without consequences, an event is considered only an unusual event or an operating incident.

Accidents generally fall into one of three categories. These are operational events (e.g., fires, spills), natural phenomena (e.g., earthquakes, high winds), and external events (e.g., aircraft crash). The latter two are not usually subject to preventive measures.

In this section, some methods of accident identification will be discussed, followed by a recommended format and content for each accident analysis. Guidance is provided on the threshold for considering rare and unlikely events in Section 3.6.

The methods below have been used successfully for a number of years. The identification of potential accidents is a task for a multi-disciplinary team. The use of more than one method can provide reassuring confirmation.

Some lists of accidents are given in Appendix B.

3.1.5.1 Brainstorming

After a list of hazards is identified by either the checklist or matrix methods above, conduct a brainstorming session to identify the potential accidents associated with each hazard.

A "What if. . .?" meeting is an excellent source of this kind of information. The structure of a "What If" meeting is as follows:

- The process operations and equipment are described so that all participants are prepared.
- A system for analysis is selected.
- The process operations and equipment are identified.
- The discussion leader selects a hazard from the working list.
- Causes of an accident are proposed and discussed.
- Ways to prevent the accident by avoiding its causes are proposed. (These are the safety features for prevention.)
- Potential consequences are explored to determine the effects of the accident under the assumption that the facility has no mitigating safety features.
- Safety features for mitigation are proposed until the expected consequences are considered acceptable or it is decided that additional research and development are required.
- Methods are suggested to detect the accident, either by detecting its causes or its consequences.

A written record of these proceedings is made to preserve the causes, consequences, safety features, and the consensus as to the efficiency of available safety features or the need for further research and development work. In the process of identifying causes and consequences, new accidents may be identified and accident sequences established which can be used in the construction of fault trees. Also, additional safety features for inclusion in the design are identified. See Appendix A.1 for an example for fuel fabrication.

The strengths of this method are:

- Covers a broad range of hazards
- Requires little prior training and is relatively easy to use
- Is effective as a learning tool
- Challenges design
- Recognizes effects of adjacent processes
- Compares process with previous experience

Limitations are:

- Shortcuts lead to weak review
- Limited depth of analysis
- Works only if the right questions are asked

3.1.5.2 Hazards and Operability Study (HAZOPS)

The Hazards and Operability Study (HAZOPS) is a structured analysis that uses a list of "guide words" to help focus on the effects of, detection of, and controls for all situations that are deviations from normal operation. It may be applied to any drawing, schematic, or model at any stage of facility design as a rigorous approach to the identification of potential problems. The procedure systematically questions every part of a process to discover how deviations from the intention of the design can occur and helps reviewers decide whether these deviations can result in accidents. HAZOPS are particularly valuable for determining instrumentation, fail-safe controls, and administrative controls that are needed in new facilities.

The HAZOPS procedure starts at the beginning of the process flow in a Piping and Instrumentation Diagram (P&ID), model, or other flow schematic. For each pipeline or vessel, the design intent is reviewed, and all of the guide words are used to identify deviations from each parameter that could have some effect on the system. A matrix is developed from applying the guide words to the different process parameters such as temperature, pressure, and flow. The use of the guide words ensures that the design is explored in every conceivable way. Example guide words are given in Table 3.1-2.

The guide words and deviations are charted, and the causes, consequences, existing protection, and Action Items or Recommendations are listed for each deviation. An example record is given in Figure 3.1-2.

The HAZOPS method works well for a continuous process. For a batch process, the guide words and parameters must be applied to each step in the process. The same is true for preparation of equipment for operation ("cold runs"), start-up, shutdown, and preparation for entry or maintenance. For these batch processes, an additional parameter, time, should be used to indicate such deviations as too long, too late, too short, too soon, missed actions or steps, extra actions or steps, steps taken out of order, and wrong time.

Unlike the "What-If" method, which relies on experience-based knowledge of a process, the HAZOPS method is a guide word stimulated brainstorming approach that focuses on previously unrecognized situations. The HAZOPS method is basically a structured "What-If" analysis that leads the reviewer systematically through the review. Overall, HAZOPS should be considered as the most versatile and applicable method of accident identification for most fuel cycle analyses. HAZOPS examples are presented in Appendix B.

The strengths of this method are:

- Provides a methodical assessment of all deviations from design intention
- Is good for unique situations and processes
- Is easy to document
- Is creative, flexible, free-ranging
- Is well adapted to chemical processes

Limitations are:

- Assumes design is correct for normal situations
- Requires an accurate model or diagram
- Needs a strong leader to keep the team on track

Table 3.1-2 HAZOPS Guide Words

Guide Word	Meaning	Example (Use)
NO or NOT	Negation of Intention	No flow of A (pump P2 stops); no cooling
MORE	Quantity Increased	Flow of A greater than design (control valve V2 fails open); high pressure; higher temperature
LESS	Quantity Decreased	Less of A (Flow sensor for valve V2 fails high); lower pressure; lower temperature
AS WELL AS	Qualitative Increase	B mixed with A (cross tie valve opened); impurities
PART OF	Qualitative Decrease	Failure to add all of C to A (Flow control valve sticks closed); missing component/reactant
REVERSE	Logical Opposite	Back flow of A (Check valve fails)
OTHER THAN/ SOONER/LATER/ INAPPROPRIATE	Substitution	Addition of C instead of A (Incorrect delivery of A - operator error); materials added in wrong order
BREACH	Structural Failure	Pipes, vessels

LINE OR VESSEL: Closed loop steam generator and piping header

DESIGN INTENTION: To generate steam and deliver to press steam header

GUIDE WORD/ DEVIATION	CONSEQUENCES	MAY EXCEED LIMITS/ WHICH CRITERIA	CAUSES	PROTECTION	ACTION ITEMS OR RECOMMENDATIONS
None	No flow	Loss of steam heat for process reactions.	No 260 psig supply steam from H Area.	Low pressure alarm 7680.	Locate PT 2220 next to steam generator (R).
		Loss of steam heat for process reactions.	Line blockage in 260 psig steam.	Low pressure alarm 2220.	Same as above.
		Loss of steam heat for process reactions. Steam generator may overheat.	No condensate return flow.	Low pressure alarm 2268, low level alarm 2220. Redundant automatic feed pump.	None identified.
More of	More flow	Process steam pressure rises.	Too much 260 psig steam.	High pressure alarm 2221.	None identified.
	More temperature	Overheat reactants. Overpressure generator. Fatality.	Steam generator tube failure.	High pressure alarm 2221.	None identified.
Less of	Less flow	Inadequate steam heat required for process reactions.	Line restriction in 260 psig steam.	Low pressure alarm 7680.	None identified.
		Inadequate steam heat required for process reactions.	Line restriction in 260 psig steam.	Low pressure alarm 2220.	None identified.
	Less temperature	Inadequate steam heat required for process reactions.	Header leak.	None.	Routine inspection. (R)

Figure 3.1-2 HAZOPS Examination Record

3.1.5.3 Event Tree Analysis

The event tree is an analytical tool which allows the analyst to organize and characterize potential accident sequences and provide a graphical logic model for quantifying outcomes of initiating events.

3.1.5.3.1 Introduction

The benefit of developing an event tree logic model is that it can provide a concise overview of all postulated accident scenarios considered in the ISA. Using it as a model can allow the analyst the means to describe in a comprehensive manner important aspects of the accident sequences, specifically:

- The mitigative system features which can be employed by an operator to safely shut down,
- The numerous alternative plant systems (and strategies for their use) available to the operator for achieving critical safety functions,
- The dependency among these systems and strategies relative to sequence progression (including describing their effects on the plant relative to the various initiating events postulated in the analysis), and
- The effects on the plant should these functions not be satisfied.

Consequently, the primary use of the event tree model is to aid the analyst in presenting the spectrum of significant accident sequences, including describing their effects on the plant relative to the various initiating events postulated in the analysis.

Based upon plant design information, potential accident initiating events are identified. Event trees are developed to depict the ability of the plant to mitigate or prevent the potential effects of these events. This comprehensive approach provides reasonable assurance that the significant causal factors affecting the safe operation of a plant have been accommodated in the analysis and that the results reflect a realistic bounding of potential accidents.

Once the initiating events have been described, functional event trees are developed. These event trees describe the functional relationships among safety and non-safety related systems, operator actions, and plant behavior into a binary event tree logic structure. When these functional relationships have been established, the events are expanded to depict the response of these various constituents which may mitigate the effects of a particular accident initiator. These detailed event trees define specific system and operator response requirements which are translated into top events. Event trees are developed to determine the probability of success or failure in achieving these requirements for mitigating the scenario.

It should be noted that the various analytical activities represent an interactive process. Information from each of the tasks is fed back to other on-going activities, and the individual analyses are refined and modified to reflect the acquisition and understanding of information as the overall analysis progresses. The following paragraphs provide detailed information on the event tree analysis technique.

3.1.5.3.2 Functional Event Tree Description

Evaluation of plant response using the event tree approach requires development of the event tree logic model where plant safety features (i.e., mitigative) are ordered and depicted according to the functional requirements for each initiator group. The functional event tree headings consist of statements of plant safety functions which can be translated into terms of associated systems and system logics for their use in emergency procedures. These provide the necessary information on plant response to allow the preparation of the more detailed system event trees that delineate the system accident sequences.

Functional event trees are developed for each initiator group because each group generates a distinctly different functional response. The functional event tree is not an end product, but an intermediate step which provides a baseline of information and permits a stepwise approach for describing the complex relationships between potential accident initiators and the response of mitigating features. It is the initial step in structuring plant responses to accident conditions in a time based format.

A functional event tree is developed for each class of initiating events based on the accident mitigative functions. The event tree headings consist of the initiating event group and the required functions. The event tree is constructed considering the functional relationships necessary to preclude the occurrence of a defined end state (e.g., explosion).

The functional event trees serve as guide for the development of system event trees. The determination of potential equipment damage consequences in the system trees must be consistent with the structure of the functional event trees. However, structural differences from the functional trees will occur in the system trees when accident sequence definitions include system hardware and operator performance considerations.

3.1.5.3.3 Event Success Criteria

Each function which is identified as an event tree heading is satisfied by the implementation of various systems. Some systems may perform more than one function or portions of several functions, depending on plant design. It is necessary to identify which systems are required to successfully perform each accident mitigative function for the definition of headings for the system event tree.

Some functions will be performed by different systems, depending on the nature of the accident. Information about the level of detail to which the systems are specified is fed iteratively back into the classification of accident. For example, purge to a tank is normally supplied by the vessel vent system, but is backed up by bottled nitrogen gas. In an accident that involves the loss of electrical power, the tank would then be purged by the bottled nitrogen gas.

The definition of functional success in terms of systems and operator response include primarily the engineered safety features of the plant. However, other systems may also provide necessary or backup mitigating actions. Systems that provide support functions, such as component cooling water and electric power, but do not directly perform the necessary safety functions are not explicitly included in event tree top event definitions.

Specific success criteria for each system which performs support or safety functions must be identified. Although success criteria for each system includes a functional definition (e.g., flow

rates, response time) they must also be stated in discrete hardware terms, such as the number of required pumps, flow paths, instrument trains, or power buses. This hardware definition will support fault tree analysis of the systems and construction of the system event trees.

Comprehensive definitions of success criteria will allow the analyst to identify the minimum complement of equipment necessary to achieve a function. Timing definitions will help determine the order of the event headings. The required complement of equipment for each system will identify when the failure of one mode of system operation may not result in the failure of a subsequent operational mode. This system success information, along with the functional relationships, will determine which sequences are to be included in the system event tree.

3.1.5.3.4 Systemic Event Tree Analysis

For the systemic event trees, the classes of accidents according to safety functions will serve as the starting point for classification according to mitigating systems. However, two main factors associated with system design and accident initiation will usually result in more classes being defined on a system basis than were identified for accidents when considering safety functions alone. These factors are:

- Design capability of systems: Although the same set of functions must be performed for two sets of initiating events, different systems may be employed to perform the same function due to the nature of the initiating event.

- Initiating event/system interaction: Some initiating events will occur in such a way as to impact either the function or the availability of potential mitigating systems. Therefore, the available set of mitigating systems for these events will be different from initiators that do not have interactions.

A system event tree will be developed for each class of accidents identified. Each event tree will identify the meaningful potential accident sequences consisting of the accident initiator type and various combinations of system success and failure states in response to the accident.

The system event trees will utilize the information on the effects of loss of various safety functions identified in the functional event trees. However, it is likely that the sequences on the event trees developed for the systems will differ somewhat from the functional event trees. This is due to the fact that in some cases, system faults may fail multiple functions. Even if its primary safety function may have failed due to other system failures, a system's operation may be of interest due to its impact on consequences.

Each system event tree will have a specific system or group of systems as event tree headings. The exact order of the headings is crucial to the presentation of the accident sequence model and the efficiency of the analysis. The number of sequences can be reduced by a judicious selection of the order of the headings: temporal, functional, and hardware relationships. Usually, phenomonological events are not explicitly included in an event tree.

Time sequence considerations are a good starting point for ordering the headings. This involves placing those systems on the event tree in the order in which they are expected to respond to an accident with those systems responding immediately (e.g., emergency power system) placed first and those responding later listed in order of response (e.g., emergency power then cooling water to cool a dissolver). Functional and hardware relationships between systems should also be considered when selecting the order of the event tree headings. Systems that depend on the

operation of other systems to perform their function should be listed after those systems. For example, pneumatic valves require the compressed air system. Since failure of one mode may imply failure to other modes, subsequent dependent modes should be listed later.

The event tree analysis proceeds by postulating the success or failure of each system in the context of all the previous system states. Only those unique combinations of success/failure states which have physical meaning (i.e., relative to achieving the functional success criteria) are included in the event tree. This understanding of the implications of each event tree sequence comes from the previous steps of the event tree development process. For each potential system success/failure state in the event tree a decision is made to postulate both states or to eliminate the choice and proceed to the next point. Only those system success/failure states which have potential significance in terms of accident sequence outcome or subsequent system operation are postulated.

Success/failure choices in the event tree can be eliminated based on a negative response to all of the following questions:

- Does the success or failure of the system impact the outcome (e.g., explosion)?
- Can the system hardware operate in this context?
- Does operation of this system contribute to a safety function in this context?
- Does operation of this system at this point impact the need for or operation of other systems?

If any of the responses are positive, the particular system success/failure state should be explicitly included in the event tree. It is important to examine each of these questions in the context of each potential accident sequence, for the importance or physical impact of a system success/failure can change depending upon the states of other systems. The convention used in drawing event tree models is that successful implementation of the top event is shown as the up branch of the binary nodal point; whereas failure to achieve the top event configuration is the down-branch path.

Table 3.1-3 describes various sources of information available to the analyst for developing event tree models.

TABLE 3.1-3 Specification of Desired Data for Event Tree Analysis

Analysis Task	Desired Data
System operation review	System descriptions System flow diagrams Operating instructions Procedures
Accident sequence timing	Plant-specific calculations Emergency Operating Procedures
System/functions interrelationships	System logic diagrams System flow diagrams Functional block diagrams Overall schematics and functional drawings showing interface areas Plant layout drawings

3.1.5.3.5 Example Event Tree

In the preparation of an event tree, the first step is to determine which systems are designed to mitigate the event. As an example (Figure 3.1-3), given the initiating low energetic event, the systems which affect the subsequent course of events are the vessel, the ventilation system, and the HEPA filter. Each of these barriers is ordered in its sequence across the top of Figure 3.1-3. The upper branch of the tree represents failure of the system to fulfill its confinement function. In the absence of other constraints, there are $2^{(n-1)}$ accident sequences where n is the number of headings (functions or systems) included on the tree. However, there are known relationships (constraints) between system functions. For example, if the vessel contains the solution, then no consequence will occur. Once these relationships are determined, some of the sequences can be eliminated because they represent success paths. These reduced event trees are used in the analysis. If the event sequences are independent, then the expected frequency of occurrence of a given sequence is the product of the initiating event frequency and the individual demand probabilities of the individual systems in that sequence. Because the failure demand probabilities are almost always 0.1 or less, it is common practice to approximate success (1-p) as 1. It should be noted that, as indicated in Figure 3.1-3, the study developed event trees in which each branch point provides only two options, system failure or success. No consideration is given to the fact that partial system success may occur within an accident sequence. Thus, an accident sequence is conservatively assumed to lead to the total release. The effects of partial system failure are accounted for by adjusting the release (in curies) to compensate for partial failure. A second example of a qualitative event tree is presented in Appendix B.

The strengths of this method are:

- Defines various damage states
- Quantifies probability of reaching various damage states

- Provides objective information for decision making
- Analyzes combinations of subevents
- Analyzes human errors
- Data readily available from incident data banks

Limitations are:

- Not readily understandable to reader; use without training is limited
- Focus is on initiating event versus the process; therefore, scope is limited
- Requires more training or practice than most of the other techniques
- Can be time-consuming

3.1.5.4 Failure Modes and Effects Analysis

A Failure Modes and Effects Analysis (FMEA) tabulates failure modes of equipment and their effects on a system or plant. The failure mode describes how a piece of equipment fails (open, closed, on, off, shorted, etc.). The effect of the failure mode is determined by the system's response to the equipment failure. An FMEA identifies single failure modes that either directly result in or contribute significantly to an accident. Human errors are not normally a part of an FMEA. However, misoperation as a result of an operator error is usually indicated as a part of the appropriate failure mode. An FMEA is not efficient for identifying an exhaustive list of combinations of equipment failure that lead to accidents. The knowledge gained in performing an FMEA (as a minimum it should include the major components of important systems) provides a detailed understanding of the function of each component and provides a solid basis for constructing event trees and fault trees.

A FMEA generates a qualitative, systematic reference list of equipment, failure modes, and effects. A worst-case estimate of consequences resulting from single failures is included. FMEA results are usually documented in a column-format table. Using the FMEA approach requires the following data and information sources: a system or plant equipment list or piping and instrumentation diagrams, knowledge of equipment function and failure modes, and knowledge of system responses to equipment failures. These studies can be performed by a single analyst, but needs detailed review by knowledgeable individuals to assure completeness.

Each accident description should include the following items.

- Initiators

  These are the proximate causes or root causes of the accident. They may be a human failure, an equipment failure, or a system failure.

- Enablers

  Usually, these are some combination of failures of preventive safety features, including human failures or failures in the administrative control systems.

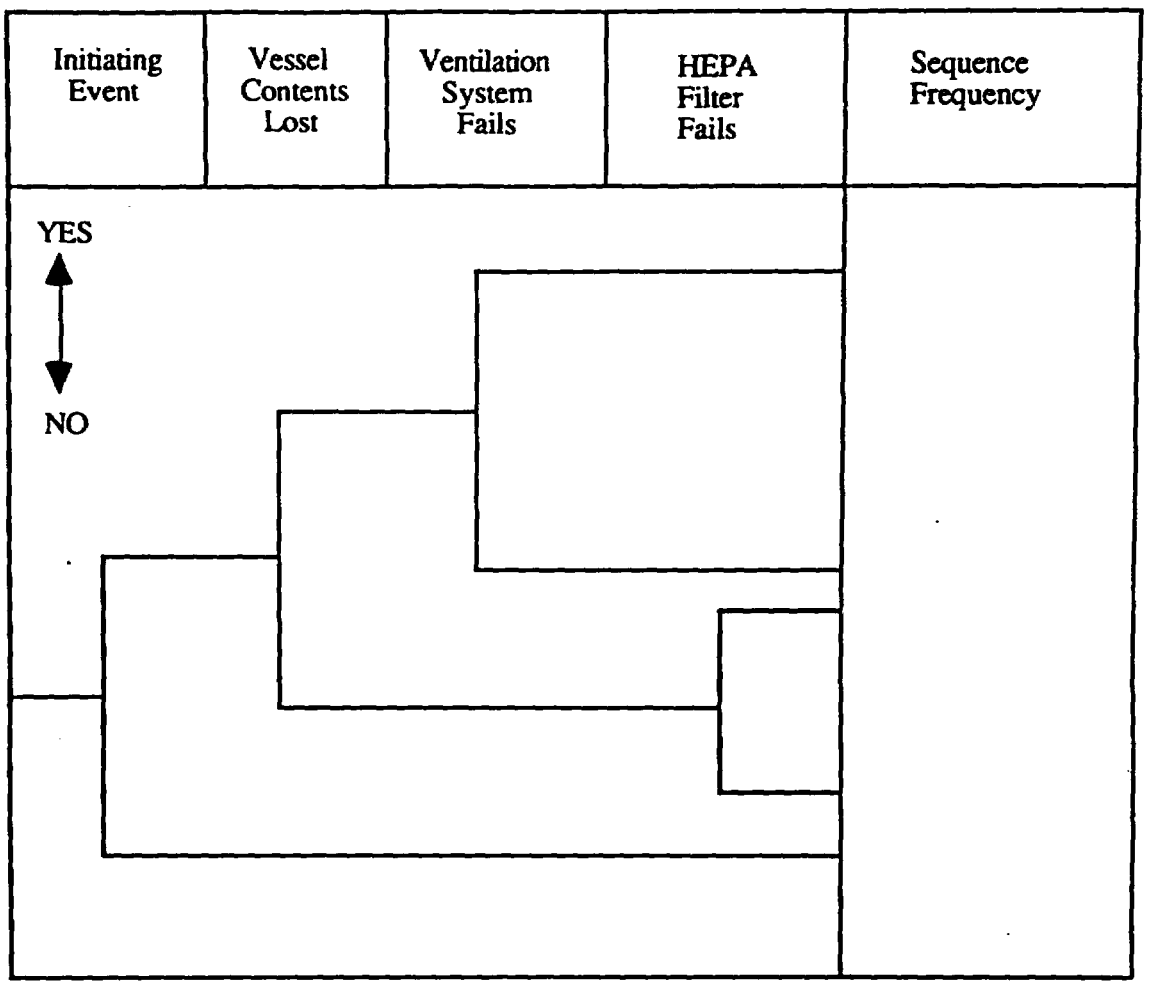


Figure 3.1-3 Example Event Tree for Airborne Releases

- Means for detection

  These are typically alarms or instruments that alert operating personnel that the event is in progress. They may or may not fail in the course of an accident.

- Qualitative potential consequences

  The perceived consequences of the accident should be described in detail.

- Means for mitigation

  These are typically those design features of a facility (or procedures) that reduce the consequences of accidents. passive mitigating features do not usually fail in an accident, but active features may or may not fail.

- Failure modes for each safety feature

  For each safety feature, the ways and conditions for failure should be described for information and for a basis for evaluation of the failure probability.

An example FMEA is presented in Appendix B.

The strengths of this method are:

- Provides a methodical approach to failure modes and consequences
- Segments unusual processes for fine, in-depth critical analysis
- Is easy to use and document for simple systems, with proper training

Limitations are:

- Very time consuming for complex systems
- Requires an accurate model or diagram
- Places focus on "Go - No Go" situations (e.g., instrument and equipment)
- Assumes design is correct

3.1.5.5 Fault Tree Analysis

For qualitative determination of the detailed combinations of events that can lead to an accident, fault tree analysis can be used. The fundamentals of fault tree analysis are abridged from the Fault Tree Handbook, Reference 4, and are presented below. Reviewers are referred to the Handbook for complete details. Examples are presented in Appendix B.

3.1.5.5.1 General Description

A fault tree analysis is an analytical technique by which an undesired state of the system is specified (usually a state that is critical from a safety standpoint). The system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. The fault tree itself is a graphic model of the logic representing various parallel and sequential combinations of faults that result in the occurrence of the predefined event. The faults can be events associated with component hardware failures, human errors, or any other pertinent events which can lead to the undesired event. A fault tree depicts the logical interrelationships of basic events that lead to the undesired event, which is the top event.

A fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive; they cover only the most credible faults assessed.

A fault tree is not, in itself, a quantitative model. It is a qualitative model that can be evaluated. This qualitative aspect is true of virtually all varieties of system models. The fact that a fault tree is particularly convenient to quantify does not change the qualitative nature of the model.

A fault tree is a complex of entities known as "gates" that serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a "higher" event. The "higher" event is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event. Thus, gates are somewhat analogous to switches in an electrical circuit or to valves in a piping layout.

3.1.5.5.2 Concepts

The concepts which are needed for the proper selection and definition of the fault tree events and, thus, for the construction of the fault tree are described in the following paragraphs.

3.1.5.5.2.1 Initiators

An accident begins with an initiator, that is, the failure to control a hazard as intended. Development of fault trees, therefore, must begin with identification of the possible initiators, those failures of the controls that prevent accidents. It should be pointed out that the word "initiator" is used differently in fault trees than in event trees. For event trees, the method typically implies time sequencing. The initiator refers to the first event to occur in the time sequence which results in an accident. For fault trees, the initiator is the event that actually starts the accident (essentially the end result of an event tree type series of events). A simplistic example of the difference in these two methods, is a leak in a tank, failure of the alarm, and ignition by a spark source. The leak in the tank would be seen as the initiator in an event tree

sequence. However, for a fault tree, the ignition source would be seen as the initiator of the explosion.

The controls that prevent accidents are usually ranked qualitatively as follows:

- Design
- Safety Systems
- Warning Systems
- Administrative

In the special case of the criticality analysis, the initiators may be called contingencies, if they meet these sufficiency tests:

- Independent - The violation or the cause of the violation of one contingency can in no way increase the probability of violation of any other event involved in the same scenario.
- Unlikely - The unlikely event is one whose violation is not expected, but may occur sometime during the operating life of the facility.
- Concurrent - In order to preserve these criteria, neither contingency may be in a failed state for an extended period of time. Otherwise, as soon as the contingency fails, "concurrency" results.

3.1.5.5.2.2 Enablers

Enablers, like initiators, are failures of controls, in this case, the controls that prevent the incident from proceeding to another, larger state or accident. Some examples are:

- Detection devices to warn of radioactive material escaping from primary containment
- Radiation monitors to warn of airborne radioactive material escaping from primary containment
- Procedural responses to alarms from monitors and detectors

Examples are presented in Table 3.1-4 to illustrate how hazards, initiators, and enablers are related.

TABLE 3.1-4 Typical Hazards, Initiators, and Enablers

Hazard	Initiator	Enabler
Fissile materials	Procedural violation	Neutron monitor failure
Powdered RAM[a]	Loss of ventilation/leak	Monitor failure
Dissolved RAM	Leak	Sump liquid-level detector failure
Combustible solids	Ignition source	Sprinkler system failure
Combustible liquids	Ignition source	Fire alarm failure
Flammable vapors	Loss of ventilation	Flow monitor failure
High pressure	Block valve failure	Relief valve fails closed

[a]RAM - Radioactive material

3.1.5.5.2.3 Mitigators

Mitigators are features that reduce the magnitude of the potential consequences of accidents. Most accident scenarios consist of an initiator and one or more enablers. For high-consequence accidents, more mitigator (failures) can be added to the scenarios.

3.1.5.5.2.4 Faults and Failures

A distinction is made between the rather specific word "failure" and the more general word "fault." Consider a relay. If the relay closes properly when a voltage is impressed across its terminals, this is called a relay "success." If, however, the relay fails to close under these circumstances, this is called a relay "failure." Another possibility is that the relay closes at the wrong time due to improper functioning of some upstream component. This is clearly not a relay failure; however, untimely relay operation may well cause the entire circuit to enter an unsatisfactory state. An occurrence like this is called a "fault" so that, generally speaking, all failures are faults but not all faults are failures. Failures are basic abnormal occurrences, whereas faults are "higher order" events.

The proper definition of a fault requires a specification of not only what the undesirable component state is, but also when it occurs. These "what" and "when" specifications should be part of the event descriptions which are entered into the fault tree.

A fault may be repairable or not, depending on the nature of the system. Under conditions of no repair, a fault that occurs continues to exist. In a repairable system, a distinction must be made between the occurrence of a fault and its existence. Actually, this distinction is of importance only in fault tree quantification. From the standpoint of constructing a fault tree, one is concerned only with the phenomenon of occurrence. This is tantamount to considering all systems as nonrepairable.

3.1.5.5.2.5 Active and Passive Components

In most cases, it is convenient to separate components into two types: passive and active (also called quasi-static and dynamic). A passive component contributes in a more or less static manner to the functioning of the system. Such a component may act as a transmitter of energy from place to place (e.g., a wire or bus-bar carrying current or a steam line transmitting heat energy), or it may act as a transmitter of loads (e.g., a structural member). Additional examples of passive components are pipes, bearings, journals, and welds.

An active component contributes to the functioning of its parent system by modifying system behavior in some way. A valve which opens and closes, for example, modifies the system's fluid flow, and a switch has a similar effect on the current in an electrical circuit. To assess the operation of an active component, parametric studies of operating characteristics and studies of functional interrelationships are performed. Examples of active components are relays, resistors, and pumps.

A passive component can be considered the transmitter of a "signal." The physical nature of this "signal" may exhibit considerable variety; for example, it may be a current or force. A passive component may also be thought of as the "mechanism" (e.g., a wire) whereby the output of one active component becomes the input to a second active component. The failure of a passive component results in the non-transmission (or, perhaps, partial transmission) of its "signal."

In contrast, an active component originates or modifies a signal. Generally, such a component requires an input signal or trigger for its output signal. In such cases the active component acts as a "transfer function," a term widely used in electrical and mathematical studies. If an active component fails, there may be no output signal or there may be an incorrect output signal.

From a numerical reliability standpoint, the important difference between failures of active components and failures of passive components is the difference in failure rate values. As shown in WASH-1400, Reference 5, active component failures in general have failure rates greater than that of passive components. In fact, the difference in reliability between the two types of components is often two to three orders of magnitude.

In the fault tree discussion, definitions of active and passive components apply to the main functions performed by the components; and failures of the active component (or failures of the passive component) apply to the failure of that main function. (There are, for example, "passive" failure modes of active components, e.g., valve rupture, if there is an attempt to classify specific failure modes according to the "active" or "passive" definition.)

3.1.5.5.2.6 Fault Classification

It is also useful for the fault tree analyst to classify faults into three categories: primary, secondary, and command. A primary fault is any fault of a component that occurs in an environment for which the component is qualified (e.g., a pressure tank designed to withstand pressures up to and including a pressure PO, ruptures at some pressure P<PO because of a defective weld).

A secondary fault is any fault of a component that occurs in an environment for which it has not been qualified. In other words, the component fails in a situation which exceeds the conditions for which it was designed (e.g., a pressure tank designed to withstand pressure up to and including a pressure PO, ruptures under a pressure P>PO).

Because primary and secondary faults are generally component failures, they are usually called primary and secondary failures. A command fault, in contrast, involves the proper operation of a component but at the wrong time or in the wrong place (e.g., an arming device in a warhead train closes too soon because of a premature or otherwise erroneous signal origination from some upstream device).

3.1.5.5.2.7 System Definition

The definitions of system, subsystem, and component are relative, and depend upon the context of the analysis. A "system" is the overall structure being considered, which, in turn, consists of subordinate structures called "subsystems," which, in turn, are made up of basic building blocks called "components."

For example, a dissolver cooling water system may consist of two redundant pumping subsystems which pump water to the cooling coils of the dissolver. Each of these subsystems in turn may consist of an arrangement of valves, pumps, piping, etc., which are components. In a particular analysis, definitions of system, subsystem, and components are generally made for convenience in order to give hierarchy and boundaries to the problem.

In constructing a fault tree, the basic concepts of failure effects, failure modes, and failure mechanisms are important in determining the proper interrelationships among the events. When speaking of failure effects, the concern is for why the particular failure is of interest (i.e., what

are its effects (if any) on the system). When detailing failure modes, aspects of component failures are exactly specified. When listing failure mechanisms, the concern is for how a particular failure mode can occur and also, perhaps, what are the corresponding likelihoods of occurrence. Thus, failure mechanisms produce failure modes which, in turn, have certain effects on system operation.

The system analyst defines the system (i.e., determines its boundary) and then selects a particular system failure mode for further analysis. The latter constitutes the top event of the fault tree. He next determines the immediate, necessary, and sufficient causes for the occurrence of this top event. It should be noted that these are not the basic causes of the event but the immediate causes or immediate mechanisms for the event. This is an extremely important point which is clarified and illustrated in later examples.

The immediate, necessary, and sufficient causes of the top event are now treated as sub-top events and the analyst proceeds to determine their immediate, necessary, and sufficient causes. In so doing, the analyst is placed in the position of the subsystems person for whom the failure mechanisms are the failure modes; that is, the sub-top events correspond to the top events in the subsystem fault tree.

In this way, proceeding down the tree, the point of view is continually transferred from mechanism to mode, and the mechanisms and modes are more finely resolved, until ultimately the limit of resolution of the tree is reached. This limit consists of basic component failures of one sort or another. The tree is now complete.

3.1.5.5.2.8 Common Cause Analysis

Dependent failures are an extremely important aspect of risk quantification and must be given adequate treatment to avoid gross underestimation of risk. Risk estimates can be in error by many orders of magnitude if the possibilities for the so-called common-cause failures and systems interactions are overlooked. These common-cause events can be categorized into three types:

Type 1. Common-cause initiating events (external events)

Type 2. Intersystem dependencies (including human interaction)

Type 3. Intercomponent dependencies

3.1.5.5.3 Fault Tree Construction Rules

Successful fault trees are drawn in accordance with a set of basic rules. Observance of these rules helps to ensure successful fault trees so that the process is now less of an art and more of a science. The basic rules for successful fault tree analysis are presented as follows:

- Write the statements that are entered in the event boxes as faults; state precisely what the fault is and when it occurs.

The "what condition" describes the relevant failed (or operating) state of the component. The "when condition" describes the condition of the system, with respect to the component of interest, which makes that particular state of the existence of the component a fault.

- If the answer to the question, "Can this fault consist of a component failure?" is "Yes," classify the event as a "state-of-component fault." If the answer is "No," classify the event as a "state-of-system fault."

If the fault event is classified as state-of-component, add an OR-gate below the event and look for primary, secondary, and command modes. If the fault event is classified as state-of-system, look for minimum necessary and sufficient cause or causes. A state-of-system fault event may require an AND-gate, or an OR-gate, an INHIBIT-gate, or possibly no gate at all. As a general rule, when an event originates from a point outside the component, the event may be classified as state-of-system.

- If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.

In the course of a system analysis, the propagation of a particular fault sequence can be blocked by the totally unexpected failure of some component. The correct assumption is that the component functions normally, thus allowing the passage of the fault sequence in question. If the normal functioning of a component acts to block the propagation of a fault sequence, then the normal functioning must be defeated by faults if the fault sequence is to continue up the tree. Another way of stating this is to say that if an AND situation exists in the system, the model must take it into account.

- All inputs to a particular gate should be completely defined before further analysis of any one of them is undertaken.

- Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates.

The Complete-the-Gate Rule states that the fault tree should be developed in levels, and each level should be completed before any consideration is given to a lower level.

3.1.5.5.4 Computer Code for Fault Tree Analysis

Application of the preceding theory can be made by manual effort; however, as a matter of practicality, the analyses of complex fault trees should be performed using fault tree evaluation computer programs. The CAFTA program developed by Science Applications International Corporation Inc., the FTAP/Importance programs developed by Howard Lambert, BRAVO by JBF Associates Inc., and IRRAS by the Idaho National Engineering Laboratory are but a few of the programs available.

CAFTA, for example, is a microcomputer-based program designed to meet the many needs of reliability analysts performing fault tree analysis on a system or group of systems. The program includes a fault tree editor for building and updating fault tree models, and a reliability data base for storing all of the basic events used in the models. The reliability data base is really two data bases. One contains the basic events for all the fault tree models and a second contains the failure rate data for each type of basic event. Once a fault tree model is built and failure probability data obtained, CAFTA provides a versatile formatting package to support many large mainframe fault tree evaluation codes. In addition, CAFTA's fault tree evaluating processor can be used to obtain the model cut sets.

The strengths of this method are:

- Identifies various causes for an accident
- Quantifies frequency/probability of various accidents
- Provides objective information for decision making
- Analyzes combinations of equipment failures
- Analyzes human errors
- Data readily available from incident data banks

Limitations are:

- Not readily understandable to reader; use without training is limited
- Focus is on an accident versus the various outcomes of a single event; therefore, tends to obscure dependencies between accidents
- Requires more training or practice than most of the other techniques
- Can be time-consuming

3.1.6 Quantitative Accident Frequency Analysis Techniques

3.1.6.1 High-frequency events

When data on events are available, it is usually preferable to use the data, rather than the methods described below in Section 3.1.6.2

For those process-related events that occur frequently, an abundance of data usually exists on both component and system failures. Site-specific data for the Savannah River Site can be obtained from the data bank, discussed in Reference 6. Statistical analysis of events sorted from the data bank can be performed using a statistical analysis the computer code such as SAS, Reference 7, to determine the frequency and other statistical parameters.

Data on the failure rates of components and systems can also be obtained from safety analyses for similar facilities or from generic sources, such as:

- Arthur H. Dexter and William C. Perkins, Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant, DP-1633, July 1982.
- Reactor Safety Study, WASH-1400 (NUREG-75/014) Appendix III, October 1975.
- A. D. Swain, and H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, August 1983.
- Alan D. Swain, A Shortened Version of the Therp/Handbook Approach to Human Reliability Assessment for Probabilistic Analysis. Proceedings of the ANS/ENS International Topical Meeting on "Advances in Human Factors in Nuclear Power Systems," Knoxville, TN, April 1986, Conf-860415.
- Barbara Jean Bell and Alan D. Swain, A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants, NUREG/CR-2254, Mary 1983.
- Alan D. Swain, Accident Sequence Evaluation Program, Human Reliability Analysis Procedure, NUREG/CR-4772, February 1987.

3.1.6.2 Low Frequency Events

Low-frequency events are treated somewhat differently from high-frequency events. For example, they tend to be more complicated, their data are harder to develop empirically, and system failure data becomes more important. The two most popular methods of developing frequencies and probabilities for this category are fault trees and event trees, as discussed below.

3.1.6.2.1 Event Tree Analysis

The event tree is an analytical tool for organizing and characterizing potential accidents so as to provide a logic model that can be used to quantify the outcomes of accident-initiating events. This analysis uses a logic diagram (the tree) to identify the ways the initiating event can lead to major accidents (i.e., it identifies the other events that are necessary and sufficient). The fundamentals of event tree construction were presented earlier in Section 3.1.5.3 with further details.

3.1.6.2.1.1 Event Tree Quantification

An event tree is constructed to show graphically the possible outcomes of the chosen initiating event. The tree is composed of the responses of safety systems and operators to the initiating event. Each end point represents a combination of successes and failure with a corresponding outcome. To determine the probability/frequency of each outcome, the probability of each branch point (equipment failure or human error) must be determined. If these branch point probabilities are high, their value can be obtained from the sources described in Section 3.1.6.1. If they are low probability events, a fault tree can be constructed whose top event is the failure of the system of interest. Fault tree methodology is described in Section 3.1.6.2.2.

Once all of the initiator and branch point data are obtained, the frequency of any single outcome can be determined by multiplying the initiator frequency times the probability of each success or failure in the sequence which resulted in the outcome. Normally, the outcomes can be grouped or put in to bins (i.e. a number of different sequences result in the same outcome). The frequency for this bin can be found by adding the frequencies of all the sequences that were combined into these bins. The results are then reported as the frequency for each accident bin. An example of a quantified event tree is presented in Appendix C.

3.1.6.2.1.2 Determination of relevant failure experience

There are a number of references to relevant failure experience available to the risk analyst. Although developed primarily for power reactors, NUREG/CR-4639 provides a Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Reference 8, much of which can be applied to non-reactor facilities. The Savannah River Site Generic Data Base Development, WSRC-TR-93-262, Reference 9, contains failure rates and error factors for a variety of components associated with waste management activities. Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant, DP-1633, Reference 10, contains failure rates for valves, instruments, pumps, electrical components, and ventilation systems derived primarily from the chemical industry literature. The Idaho Chemical Processing Plant Failure Rate Database, WIN-330, Reference 11, contains pedigree failure rate data on components for the Idaho facility, much of which would be of general utility.

Other sources of failure rate data include References 12-20. NPRDS, Reference 12, data are largely for nuclear power plants, but has utility for non-reactor facilities. Cramer, References 12, 14, published data on valve and check valve reliability, Rossi's, Reference 15, data is for nonelectronic parts, Cadwallader, References 16, 17, 18, published generic data on tritium system failure rates generally associated with fusion studies, Wykoff's data· Reference 19, is for emergency diesel generators, and Derdiger, Reference 20, discusses component failure and repair data for coal-fired power plants.

Preanalyzed data for many non-reactor facilities may be found in References 21-27. Daling's, Reference 21, work is primarily associated with waste repositories, irradiated fuel storage, and transportation and includes frequencies, consequences, and risks of a wide variety of accidents. Cohen and Dance, Reference 22, published frequency and dose calculations for milling, conversion, enrichment, fuel fabrication, and reprocessing. Erdmann's, Reference 23, data is associated with mixed-oxide (MOX) fuel refabrication, irradiated fuel storage, reprocessing, waste disposal, and transportation.

Fullwood and Jackson, Reference 24, present accident frequency and dose data for MOX fuel refabrication, reprocessing, transportation, and waste handling. Cooperstein, Reference 25, published a limited amount of data on the frequency and dose of accidents for reprocessing. Karn-Bransle-Sakerhat, Reference 26, shows a small amount of data for irradiated fuel storage accidents. Smith and Kastenberg, Reference 27, published data on frequency and doses associated with solidified high level waste storage. Much of the material contained in References 21-27 may be found in the Regulatory Analysis Technical Evaluation Handbook, Reference 28.

The Savannah River Technology Center maintains data banks, Reference 29, containing chronological abstracts of equipment failure, process upsets, contamination events, environmental releases, injuries, etc. for a large number of non-reactor facilities including reprocessing, fuel fabrication, analytical laboratories, research and development laboratories, and waste management facilities. These data banks contain approximately 400,000 events which are available through the Savannah River Operations Office of the U.S. Department of Energy, Aiken, SC.

3.1.6.2.1.3 Other Means of Obtaining Quantitative Data

- Rare Event Theory

For events that have not occurred in a facility and do not lend themselves to fault/event tree analysis, a method based on Rare Event Theory may be used. This method is useful only if a very conservative estimate of frequency is appropriate, because this method usually overstates the frequency of an event in order to provide a high-confidence estimate.

In simple form, if an event has not occurred in t years, a conservative upper limit of the failure frequency (at the 95% confidence level) is given by:

$$\text{Upper Limit Frequency} = 3/t$$

It should be noted that the value of t should be very large for practical application of this method. Otherwise, the upper limit value may be overly conservative, i.e. too large to be useful, Reference 30.

- Human Reliability Analysis

Human errors can act as accident initiators, propagators, and mitigators. Often, human errors are more important in accident analyses than equipment failures. A useful method of evaluating the human factors for an analysis is the Technique for Human Error Rate Prediction (THERP). The method, models, and human error probability values are contained in a handbook of human reliability prepared for the US Nuclear Regulatory Commission, Reference 31.

Additional resources on human reliability, human error probabilities, and analytical procedures include the following:

- Barbara Jean Bell and Alan D. Swain, A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants, NUREG/CR-2254, May 1983.
- Alan D. Swain, "A Shortened Version of the THERP/Handbook Approach to Human Reliability Assessment for Probabilistic Analysis", Proceedings of the ANS/ENS International Topical Meeting on "Advances in Human Factors in Nuclear Power Systems," Knoxville, TN, April 1986, CONF-860415.
- William C. Perkins, "The Probability of Process Laboratory Errors Affecting Reprocessing Operations," Proceedings of the ANS/ENS International Topical Meeting on "Advances in Human Factors in Nuclear Power Systems," Knoxville, TN, April 1986, CONF-860415.
- William C. Perkins and William S. Durant, "The Human Factor in First-Year Operations," Transactions of the American Nuclear Society, Volume 57, Washington, DC, October 1988.
- Alan D. Swain, Accident Sequence Evaluation Program, Human Reliability Analysis Procedure, NUREG/CR-4772, February 1987.

- Delphi

Where little or no data exists, it is possible to generate acceptable data by utilizing the opinions of experts or personnel highly experienced in the area of interest. Frequently, these individuals have knowledge of qualitative or quantitative information that has never been formally documented. Basically, a group of these people can be solicited to assess the question and to reach a consensus regarding the appropriate information. A consensus of experts is more highly regarded than the opinion of an individual. The Delphi method, Reference 32, is a simple method that can be performed with a number of variations. The process is iterative and can involve the following steps:

- A group of three or more experts is selected.
- In isolation from one another, the independent estimates of the value in question is solicited along with the reason for the choice.
- All experts are supplied the initial results and revisions that might ensue.
- The average of the final estimated provides the best estimate of the value in question and the standard deviation provides a measure of uncertainty.

It is acceptable to assemble the experts to discuss their choices in order to reach a consensus. Weighting of opinions is also acceptable depending on the experience of the individuals. Also, the highest and lowest values may be discarded before averaging if a sufficient number of opinions have been solicited, Reference 1.

3.1.6.2.2. Fault Tree Analysis

For process-related events for which no data (or insufficient data) exist, a popular method of frequency determination is fault tree analysis. Basically, this method uses the frequencies and probabilities of the more-frequent proximate causes of major events, such as fire and criticality, to construct the frequencies of rare and very rare events.

This analysis also uses a logic diagram (the tree) to identify the ways the cause event can lead to the major event, (i.e., it identifies the other events that are necessary and sufficient for the "top" event. The fundamentals of fault tree construction are found in the Fault Tree Handbook , Reference 4, and were presented earlier in Section 3.1.5.5.

Some worked examples of fault tree analysis are presented in Appendix C.

3.1.6.2.3 System Failure Analysis

If a system failure is to be analyzed, it must first be determined what type of analysis should be used for the system. For complex systems, a detailed fault tree and/or event tree is required to understand and appropriately predict system failures. These techniques are discussed in the following sections. Care should be taken in the decision to create a fault/event tree. No analysis should be driven below the level of the data. For example, if an analysis is required for transfer errors in a given process, it would be possible to construct a fault/event tree which would delineate all of the cause of transfer. Data could be obtained for each of the components/branches and an overall transfer error rate estimated. However, if data is available on this specific process, it should include all of the pathways for transfer errors, as well as reflect the human performance of the operators involved. The subtleties of human performance, effectiveness of human engineering, and clarity of procedures are difficult to model in an event tree, but readily reflected in site specific data.

If a fault tree/event tree is not required, the next step is to search for failure data. The search should begin with any site specific data which exists. If data is not available on the specific system of interest, failure information of similar systems could be used. If known differences exist between the two systems, an adjustment (either up or down) could be made in order to account for these differences. These adjustments should be made carefully to assure that conservatism is retained.

If site specific data is not available, it is necessary to resort to generic sources of data. These range from data on similar equipment at other sites to generic component type data (e.g., IEEE-500 for electrical equipment). It is often necessary to settle for information that is not a perfect match for the system being analyzed. As stated above, if sufficient information exists, adjustments can be made to these failure frequencies to account for their differences.

3.1.6.3 Non-Credible Accidents

Credibility of a potential accident is based on the annual frequency at which the accident is expected to occur. Credibility limits in the range of 10^{-8} to 3×10^{-5} occurrences per year have been used, References 33, 34, 35, 36, 37. Reference 38 suggests an annual frequency of 10^{-6} be used to establish the credibility of potential accidents. The selection of 10^{-6}/yr is based primarily on a consensus among risk analysts for non-reactor nuclear facilities to consider a frequency of 10^{-5}/yr as a frequency which should cause concern if the accident consequence is high; conversely, a frequency lower than 10^{-7}/yr is considered so low as to be almost indeterminate or nonsensical. Therefore, any postulated major accident which has an estimated annual frequency approaching 10^{-6}/yr should be considered credible.

In reporting of events with an annual frequency of less that 10^{-6}/yr, it is appropriate to acknowledge their existence for completeness and to provide the estimated frequency; however, consequences of these events should not be specifically analyzed.

3.1.7 Quantitative Accident Consequence Analysis Techniques

An ISA should contain a risk determination, where risk is a function of event frequency and the consequences at the points of interest. Thus, assessment of the consequences of accidents is an integral part of risk determination and ISA. The objective in carrying out this assessment should be to keep the process simple by not trying to be too rigorous in subdividing consequences. The level of detail should be consistent with the risk and with the chosen method of the analysis. Qualitative estimates based on expert opinion may be appropriate or quantitative calculations may be required.

Consequence assessment in the context of nuclear fuel cycle facilities may be defined as the evaluation and interpretation of postulated radiological (or other hazardous material) releases to provide a basis for decision making.

Consequence assessment for safety analysis differs from consequence assessment for emergencies. As described in the DOE Emergency Management Guide for Consequence Assessment , Reference 39, consequence assessment for emergencies includes planning, preparedness, and response.

Planning involves development of postulated scenarios and consequence projections for hazards assessment; developing procedures for consequence assessment during an emergency; and identifying resources to provide an effective response.

Preparedness includes personnel training; acquisition and maintenance of resources; exercises; and essential procedures, personnel, and resources for consequence assessment.

Response represents the results of planning and preparedness during an emergency.

Consequence assessment for safety analysis, on the other hand, identifies credible accident scenarios which can lead to the onsite or offsite exposure of people (or can cause significant property damage), followed by identification and quantification of the source terms associated with each scenario and estimation of the magnitude of the exposures at the different receptor points (or the magnitude of the property damage).

Each scenario can then be associated with a qualitative severity rank, which enables a determination of acceptability to be made. This then becomes the basis upon which further decisions (e.g., introduce administrative controls, restrict inventory, upgrade design, change process, etc.) are made.

For quantitative assessment, this estimation of the magnitude of the exposures at the different receptor points (or the magnitude of the property damage), is coupled with its projected frequency of occurrence to give a risk estimate for each accident scenario. This risk is then compared with fixed criteria to guide protective action decisions.

3.1.7.1 Accident Selection

There are several well-known techniques in routine use in industry for developing a comprehensive list of events or accidents that could result in the release of radioactive hazardous materials to the environment, or could result in significant property damage. These have been described in Sections 3.1.4 and 3.1.5, and include techniques such as Failure Modes and Effects Analysis (FMEA), Hazards and Operability Study (HAZOPS), "What If" sessions, checklists,

and Event Tree analysis. These are not mutually exclusive, and the choice as to which method to use may well depend upon the severity of the perceived consequence of the facility being evaluated.

3.1.7.2 Source Term Determination

The total quantities and types of material that can be released, their physicochemical form, the pathways (e.g., air, surface or ground water), and the rates at which they are released to the environment, must be determined for each of the identified accident scenarios. Typically, if the total inventory of radionuclides and/or hazardous material is known, some reasonable default assumptions are used to determine the fractions that are likely to be released to the air, surface water, or ground water, based upon their physical state (gas, vapor, liquid, finely divided or bulk solid), and characteristics such as solubility, stability, and volatility. For example, it is usually assumed that 100% (release fraction RF = 1) of a non-reactive gas will be released to the air and be transported to the downwind receptor point, compared with only 50% (RF = 0.5) of a volatile or combustible liquid. Some other assumed release fractions are an RF = 0.01 for semi-volatile liquids, and an RF = 0.0001 for nonvolatile solids. U and Pu metal are assumed to have an RF = 0.001, Reference 40. Methods for consequence analysis in the chemical industry are discussed in Reference 1.

Some examples of source term determination in specific cases follow.

3.1.7.2.1 Masses of Materials Involved in an Accident

Amounts of materials involved in specific accidents are typically determined from available inventory data, process information, material balance data, routine monitoring or observation (e.g., of storage tanks), etc. These quantities are then applied categorically to the event being analyzed as a whole rather than attempting to estimate the fractions of the totals that might be involved in any particular operation involved in the event. The values may be grouped primarily according to activity level (e.g., natural or enriched uranium compounds), contaminated process chemicals, cold chemicals (e.g., ammonium hydroxide, hydrogen fluoride, nitric acid, tributyl phosphate), and water.

Three statistical functions are calculated for each group of accidents: the mean and median mass of material, and the 90% error bounds of material released beyond the confines of the facility.

In the absence of more specific data, one-half of the maximum content (capacity) of the vessel involved in the accident may be used as the mean mass in the evaluation. Maximum credible masses are assumed to be the masses contained in the largest vessels in the applicable operation.

3.1.7.2.2 Curies of Material Involved in an Accident

Curies of materials involved in a process accident are based on the measured concentrations in process solutions, and on the masses.

Appropriate computer codes may be used to calculate the quantity of radioactive material released to the environment following an accident which results in the spillage of liquid. The evaporated mass will depend upon the rate of evaporation of the pool of liquid, which in turn depends upon (1) the surface area of the pool, (2) its temperature (both absolute and differential with respect to the air), (3) the vapor pressure of the spilled liquid, and (4) the time that elapses before recovery or sequestration of the liquid. All of these parameters would be expected to change with time after the initial spillage occurs, because the temperature differential between

the air and the liquid, the vapor pressure of the liquid, and the size of the spill may all decrease with time. The amount of material reaching the environment also depends on other factors such as mechanical dispersion from splashing, plateout, and resuspension.

If the evaporating liquid contains dissolved uranium compounds, the residue would comprise uranium compound sludge or powder, so consideration would have to be given to possible dispersion mechanisms. Usually, an energy source (e.g., a fire or an explosion) would be necessary to create a credible airborne source term in this way. NUREG-1140, Reference 40, recommends use of 1 E-3 as the release fraction for nonvolatile powders of this nature.

Scrap recovery processes should be examined for possible source terms for accidental radioactive release source terms. The total quantity of uranium involved can be estimated from a material balance calculation: The quantity of uranium input (e.g., from UF_6 cylinders) is known, and the total quantity of uranium loaded into fuel tubes (as UO_2 pellets) is known by calculation or measurement. The difference represents the quantity of material somewhere in the process lines, vessels, filters, columns, etc. The distribution and chemical form of this uranium will be a function of the process.

To be conservative, the total inventory is assumed to be available for dispersion in the event of an accident. The only mitigation (apart from physics, i.e., the physicochemical characteristics of the source material) that can be considered in calculating the consequences are those items (barriers) that have been put there for the purpose, and are qualified to remain operable for the scenario (e.g., tornado or earthquake) being analyzed.

3.1.7.3 Consequence Calculation

This section discusses techniques that are useful for determining the consequences of credible accidents at the points of interest. This has to be done for both qualitative and quantitative analysis. For fuel fabrication facilities, the only radionuclides of interest as source terms for most accident scenarios will be the uranium isotopes. One exception is a criticality accident where fission products will be present. (See Reg. Guide 3.34.)

Consequence calculations for airborne release resulting from postulated accident scenarios involve atmospheric transport and radiological dosimetry calculations. This section provides technical guidance for dose calculations using conservative analysis techniques.

Calculation of radiological dose, in terms of 50-year Committed Effective Dose Equivalent (CEDE), has to be performed for each accident scenario. For materials of greatest interest for fuel cycle, the dose from inhalation pathway normally dominate the dose, and therefore, dose contributors from other exposure pathways can be dismissed. However, for situations in which the dose contribution from ground contamination and cloudshine exposure pathways is relatively significant, special considerations should be given.

Radiation doses resulting from inhalation of radionuclides in air depend on the amount of radionuclides released, the dispersion characteristics, the physical and chemical nature of the radionuclides, and various biological parameters. Inhalation dose can be calculated using the general equation:

$$CEDE = \sum_i Q_i \times (X/Q) \times BR \times DCF_i$$

where

CEDE	=	Committed effective dose equivalent (rem) from inhaling radioisotope i
Q_i	=	Source term (Ci) for radioisotope i
X/Q	=	Expression accounting for dilution of release at a point under given meteorological conditions (sec/m^3)
BR	=	Breathing rate (m^3/sec)
DCF_i	=	50-year inhalation dose commitment factor (rem/Ci) for radioisotope i

For the sake of conservatism, X/Q should be determined using adverse meteorological conditions (e.g., F stability class and 1 m/sec windspeed). Dispersion models for ground-level and stack releases, as presented in NRC Regulatory Guide 1.145, Reference 41, are recommended: Gaussian plume models with the adaptations of the straight-line trajectory. These models are provided to calculate relative concentration from stack releases and from releases through vents or building penetrations.

Breathing rate is dependent on age and physical activity. To ensure reasonable and consistent inhalation dose calculations, a breathing rate of 3.5E-4 m^3/sec is recommended.

To ensure reasonable and consistent inhalation dose calculations, the inhalation dose conversion factors as presented in DOE/EH-0071, Reference 42, or ICRP 56, Reference 43, are recommended. The inhalation dose factors were generated using ICRP Publication 30, Reference 44, methodology and the associated dose commitment is extended over a 50-year period from initial intake. In this model, radioactivity is fractionated between various organs immediately after inhalation, and eliminated using effective biological clearance half-times. Inhalation dose factors account for daughter ingrowth once the nuclide has been inhaled. To account for skin absorption of tritium oxide, the inhalation dose factor for tritium oxide should be increased by 50% over the value given in DOE/EH-0071, Reference 42.

Airborne releases into high-velocity winds must be given special treatment. Dispersion modeling of straight-wind or tornado-caused release can be quite complicated. However, if the straight-wind or tornado-caused release involves only solution spills, upper-bound approximation of air radionuclide concentration can be made by considering that air entrainment of the spilled solution and the dispersion of airborne radionuclides are under normal meteorological conditions (i.e., after high wind or tornado passes). Under normal meteorological considerations, the entrainment (and evaporation) rate thus estimated may be too low because of low wind speed. However, such underestimate of the source term is overly compensated by the conservatism in the dispersion modeling (normal meteorology vs. straight-wind or tornado).

If the straight-wind or tornado-caused releases involve radionuclides in gaseous or powder form, then an appropriate dispersion models of straight wind or tornado with some conservative assumptions must be made.

3.1.7.4 Consequence Severity Determination

Having determined the consequences of each accident scenario, one should evaluate them qualitatively. This may be accomplished by comparing the consequence with an approved set of criteria. NRC policies or regulations will determine both the criteria and the required mitigative action associated with each accident consequence level (rank).

3.1.7.5 Identification of Potential for Propagation of Accidents

It is possible that the consequences of an accident could stretch beyond the originally assumed accident scenario. For instance, if a tank were to explode it could release its contents, but shrapnel from the tank could breach a nearby tank. The second tank could leak, catch fire, or explode releasing at least some portion of its contents. Thus the original explosion accident could propagate to a second tank.

It is important to remember that the propagation does not have to take place in a direct manner. Frequently it takes the form of loss of support systems. An accident could result in a nearby transformer being damaged or destroyed. The resulting loss of power could cause another vessel to overheat or explode (due to loss of cooling or ventilation).

It is also possible for accidents such as fires to propagate through the ventilation system.

When determining the consequences of an accident, the potential for propagation by all possible pathways should be examined and the consequences of the propagation included as part of the consequences for the accident.

3.1.8 Determination of the Risks of Accidents

After evaluating the consequences of each key accident scenario and estimating the likelihood of its occurrence (i.e., the expected frequency), the user must establish defensible criteria against which to judge the acceptability of those consequences. In general, the smaller the expected frequency of occurrence of an accident the larger the acceptable consequence. The classical approach is to consider events that are expected to occur with a frequency greater the once every ten years to be routine (normal) and, therefore, covered by occupational exposure guidelines.

3.1.8.1 Risk Identification (Qualitative Method)

This section brings together the qualitative safety evaluations discussed above and summarizes the results in terms of the potential accidents categorized largely by frequency and consequence estimates.

Figures 3.1-4 and 3.1-5 and Tables 3.1-5 to 3.1-7 provide examples of risk evaluation and ranking methods. More than one example is provided to indicate that there are more than one correct approach. These are based on adaptations of methods in Military Standard 882B (March 1984).

The approach used at any specific facility should be based on the detail appropriate for the accident, the facility, and the expertise of the analysis team.

Figures 3.1-4 and 3.1-5 are graphic examples of typical frequency- and consequence-ranking matrices. The logic behind Figure 3.1-4 is explained in Tables 3.1-5 to 3.1-7.

In other cases of facility-accident combinations a four-by-four matrix may be more appropriate. Elsewhere, a nonsymmetrical matrix could be used, such as a four-by-five or other arrangement.

Although they differ in appearance, the philosophical basis and objectives are the same. The ranking method is designed to eliminate the majority of the low-risk accidents, indicate high-risk accidents for further attention. The moderate-risk accidents between the two extremes are also identified for further analysis and attention.

The tables provide typical definitions of frequency and consequences for the rankings. Although this process is essentially subjective and qualitative, a numerical basis for the judgments has been used to provide consistency in the analysis. For example, a simple method for frequency estimations would be to begin with an initiator frequency and assign a probability of 1.0 to nonindependent events, 0.1 to human errors, and 0.01 to independent failures.

TABLE 3.1-5 Qualitative Consequence Severity Classification

Severity Level	Descriptive Word	Description
0	No	Negligible onsite and offsite impact on people or the environs.
1	Low	Minor onsite and negligible offsite impact on people or the environs.
2	Moderate	Major onsite impact on people or the environs; only minor offsite impact.
3	High	Major onsite and offsite impacts on people or the environs.

TABLE 3.1-6 Qualitative Frequency Classification

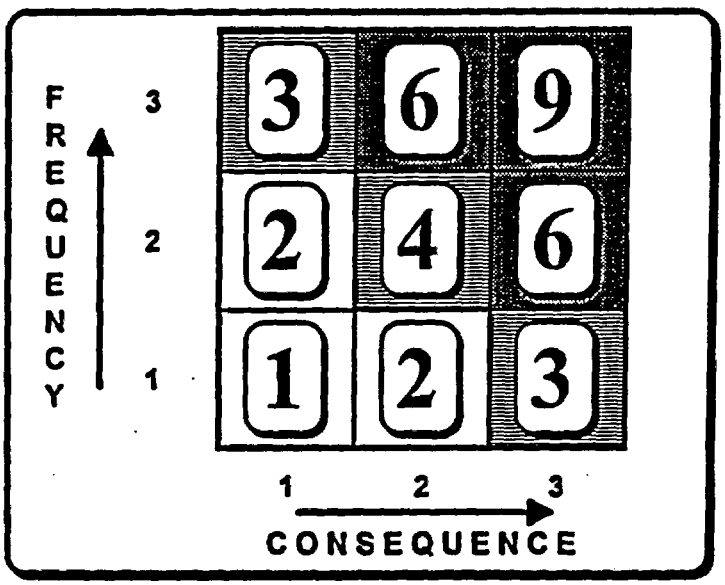
Level	Descriptive Word	Estimated Annual Probability of Occurrence	Description
3	Anticipated	1≥p>1E-2	Incidents that may occur several times during the lifetime of the facility. (Incidents that commonly occur.)
2	Unlikely	1E-2≥p>1E-4	Accidents that may occur sometime during the lifetime of the facility. Natural phenomena of this probability class include: UBC-level earthquake, 100-year flood, maximum wind gust.
1	Extremely Unlikely	1E-4≥p>1E-6	Accidents that will probably not occur during the life cycle of the facility. This class includes the Design Basis accidents.
0	Incredible	1E-6≥p	Accidents that are not credible.

TABLE 3.1-7 Qualitative Risk

Risk Level*	Description	Risk Evaluation
0	No impact or incredible	
1	Low severity and extremely unlikely	Acceptable
2	Moderate severity and extremely unlikely or low severity and unlikely	
3	High severity and extremely unlikely or low severity and anticipated	Marginal
4	Moderate severity and unlikely	
6	Moderate severity and anticipated or high severity and unlikely	Unacceptable
9	High severity and anticipated	

*Risk level = severity level x frequency level.

RISK ZONES



RISK = FREQUENCY X CONSEQUENCE

RISK ZONE	ACTION REQUIRED
6 & 9	Risks require prompt mitigation with comprehensive demonstration
3 & 4	Risks require management attention and a rational degree of mitigation with the engineering basis documented
1 & 2	Risks do not require further formal treatment

Figure 3.1-4

Risk Zone Assignment

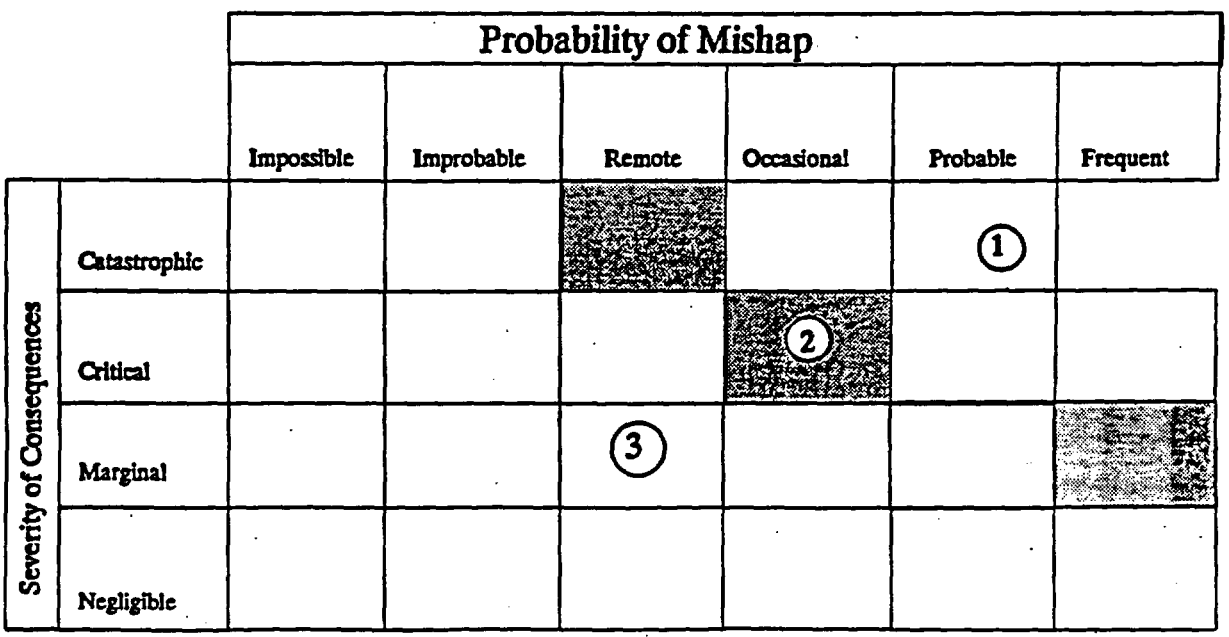


Figure 3.1-5

3.1.8.2 Risk-Based Analysis (Quantitative Method)

Section 4.2 discusses quantitative methods used to determine accident frequencies and Section 4.3 discusses quantitative methods used to determine the probable consequences of accidents. In this section, methods to combine these frequencies and consequences to give a measure of risk are reviewed and discussed. Several methods of presenting risk estimates are discussed and guidelines for choice depending on the expected use of the results. Large uncertainties are associated with risk estimates and methods for treating these are discussed in Section 3.1.8.3.

Traditionally, risk has been estimated in four basic ways:

- The judgmental, or qualitative, approach (Section 3.1.8.1) involves a subjective comparison of risk. If used by an experienced analyst it can give adequate results. If it is based on public perception, the results can be highly erroneous.

- The cost/benefit approach compares the cost of risk mitigation to the cost of risk acceptance. Although it is an effective risk management tool, this approach does not provide information that can be used to compare the risk of one facility to another and is not discussed in this manual.

- In a deterministic approach, consequences are postulated and compared to an upper limit, but the accident mechanism is not identified and the likelihood of the accident is not estimated. The deterministic risk approach does not actually provide a measure of total expected risk and is not discussed in this manual.

- In the probabilistic approach, accident mechanisms are postulated and both the likelihood and consequences of the accident are estimated. This is the approach most suitable for the ISA of complex facilities because it provides information on the relative contributions of different types of accidents to the total risk.

3.1.8.2.1 Formats for Presentation of Risk Results

In general, risk of an operation in terms of either economic loss or human injury or both is desired to be known. This manual discusses methods for estimating human injury. Economic risks and their determination are a matter of internal policy for individual companies. There are many different ways to present similar information, some of which are more appropriate than others, depending upon the intended message. In some instances, there are multiple ways to interpret the same information.

Typically, risk is calculated as the product of frequency (Section 3.1.6) and some measure of the consequences (Section 3.1.7) of an accident. The frequency of the outcome will be expressed in expected events per unit time. A number of outcomes may be feasible as a result of the initial event and event/fault tree sequence analysis can be used to establish likely sequences. The event outcome is itself the combination of the frequency of the event occurring and a particular final outcome. The frequency analysis may be simple estimates or the result of sophisticated fault and event tree analyses. Consequences may be evaluated as facility damage, individual uptake of a chemical or radiological material, injury or fatality depending on the desired measures and the intended use. Consequences may be determined using simple estimates from empirical models or more complex mechanistic models to evaluate phenomenological behavior of source, dispersion and effects. For complex facilities multiple incidents may be analyzed to fully characterize the safety envelope of the facility (i.e., an Integrated Safety Analysis).

The level of detail and effort spent to determine the event frequencies and consequences, and as will be seen later the uncertainty analysis, establishes the level of detail upon which the risk estimates are made and the credibility and usefulness of the analysis. Simple broad brush treatments are appropriate for simple facilities with low hazard potential. For more complex facilities with numerous interactive systems and with the potential for catastrophic consequences, detailed analyses to produce a complete Probabilistic Risk Analysis are most appropriate. A PRA provides a better picture of the risk of operation to the public rather than a deterministic estimate which significantly overestimates the risk. The PRA also provides the basis for selecting operations and systems that may require additional measures to lower the overall risk of operation. A full analysis including uncertainty is termed a Probabilistic Risk Analysis PRA or a Probabilistic Safety Analysis (PSA).

The outputs of the analysis include a wide variety of risk measures, of which a selected subset may be presented. These risk measures, such as onsite and offsite prompt or latent fatality risks, can be made available in different formats depending upon what information is to be conveyed. Special calculations are performed with specific sets of assumptions to produce results for direct comparisons to such measures as the NRC safety goals.

Typical presentations of risk estimates are simple point estimates, individual risk measures and population or societal risk measures. These will be elaborated on below.

3.1.8.2.2 Complementary Cumulative Distribution Functions

The risk of operation is determined by comparing the frequencies of accidents to their consequences. However, a gross total of the frequency and consequence products (i.e., a point estimate) can be misleading. Risk is expressed in terms of separate frequency and consequence numbers; therefore, high-consequence, low-frequency events are not easily compared with low-consequence, high-frequency events. The risk should be presented to show both the overall risk and the distribution of the risk. This is usually done with a graphic presentation.

A risk curve is a graphic representation with frequency plotted versus consequence for the set of accident sequences developed by the fault tree/event tree analysis. There are several variations to the risk curve involving uncertainty bands, comparison to other risk curves and comparison to acceptable limits.

The Complementary Cumulative Distribution Function (CCDF) is the most complete description of a measure of risk. A CCDF plot , Figure 3.1-6, is essentially a family of curves, with each curve representing one complete quantification of the full PSA, from accident initiator through consequences. The abscissa of the plot describes the magnitude of the risk measure, and the ordinate describes the frequency with which the risk magnitude will be exceeded. One curve is produced for each sample member and thus a complete family of CCDFs for a particular risk measure could require the plotting of multiple separate curves. The number of curves is determined by the number of statistical samples required in the sampling analysis to determine uncertainty. Monte Carlo sampling routines can be used to develop a family of curves that represent the spectrum of events with a high degree of confidence. However, a large number of curves plotted together would impart very little useful information. Therefore, the next most complete representation of risk would be to present "typical" and "bounding" curves to represent the expected range of the risk as well as the predicted mean. This is accomplished by analyzing the family of curves at many points along the risk measure axis. At any one risk level, there will be many estimates of the frequency of exceedance of that level of risk; one from each of the

CCDF curves. Statistics can be calculated from this multi-point sample, and the 5th, 95th, and median percentiles calculated, as well as the sample mean. When this is done at many points along the risk axis, many estimates of the 5th, 95th, etc. statistics are generated at many values of the risk, and can then be plotted as just a few curves. These curves can be taken as a summary description of the full set of curves in which only a small amount of information is lost.

In the CCDF plots there are two different types of variation, along a curve in the direction of the consequence measure, and vertically between curves along the exceedance frequency axis. These two types of variation have different sources. For the raw CCDFs, the variation along a curve is typically caused by meteorological variation only for offsite consequences. For the statistical measure CCDFs (mean, 95th, etc.), however, variation along the curve is produced by variability in the weather status at the time of the accident, as well as the frequency of different types of accidents. Thus, the different types of accidents which may occur, coupled with the consequence analysis use of probabilistic models of the weather over a year's time produce the variation along the summary curve. Variation between the curves vertically, however, is produced only by variation in the input parameters for the accident, accident progression, and source term analyses. The parameters in these analyses which have been assigned probability distributions and have been propagated throughout the full PSA model cause this curve-to-curve variability. The two forms of variation also have different interpretations. The variation along a raw CCDF represents stochastic variability with respect to the effect that weather patterns characteristic to a site have on the consequences from a given source term. Variation along a summary CCDF, however, is a mixture of stochastic and model uncertainty since points along each summary curve may be derived from raw CCDFs produced by different sample members. The curve-to-curve variability for both raw and summary CCDFs is caused by variation in parameters which is caused, for the most part, by imprecisely known data or models. This variation is, therefore, mainly non-stochastic in nature. Thus, more accurate models and data would decrease the spread between the curves, but would do little to decrease the variation along the curve.

3.1.8.2.3 Annual Risk

It is often desired to obtain a single estimate of a measure of risk for comparison or other purposes. A CCDF plot does not accomplish this. It is possible, however, to utilize the CCDF curves to derive multi estimates of mean or "annual" risk. This is accomplished by integrating each of the CCDF curves and reducing it to a single value; i.e., the mean risk for each curve. This, then, will produce a complete sample size of mean risk values, one for each curve. In performing this operation, however, all information relating the frequencies of the various risk levels is lost and all that is left is the average of the risk over a year's time period. Statistics can then be formed on the samples of annual risk, and a mean value formed to represent a "point-estimate" of risk. Note that there is really very little information contained in this point-estimate; it is essentially the mean of the mean (annual) risk.

Results may be presented in two forms: as societal risks, which will be the predicted levels of consequence within a population at risk (Figure 3.1-6), and individual risk, which can be interpreted as the frequency of the analyzed consequence happening to an "average" individual within the zone of interest for the accident (Figure 3.1-7). The societal risk implicitly includes the distribution of the population within the zone of interest for the accident. The individual risk, however, has "averaged out" this population distribution, and cannot actually be thought to apply to any single individual within the zone of influence.

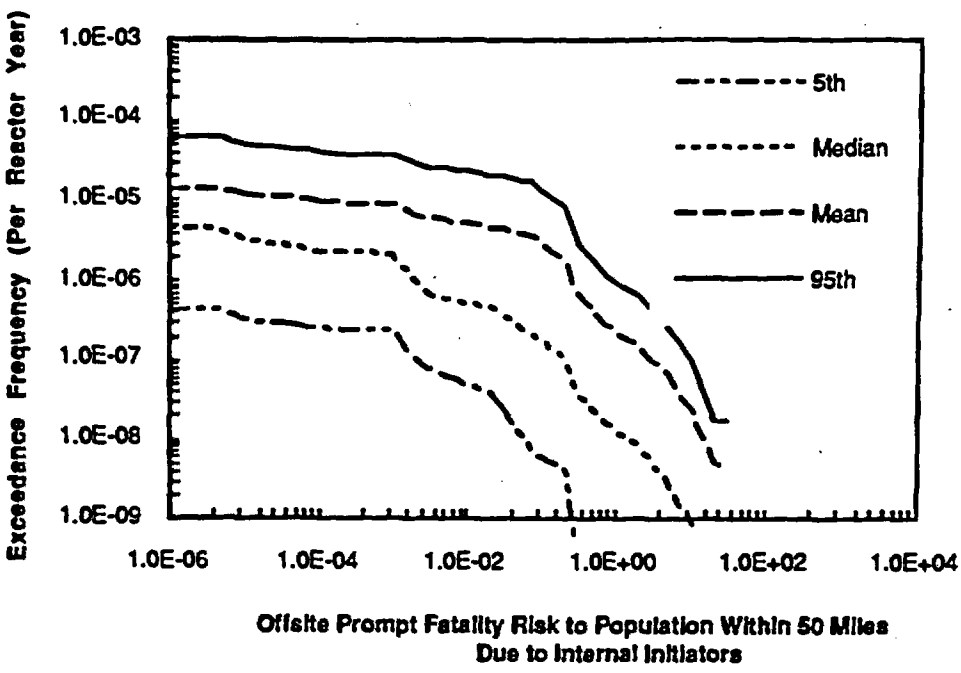
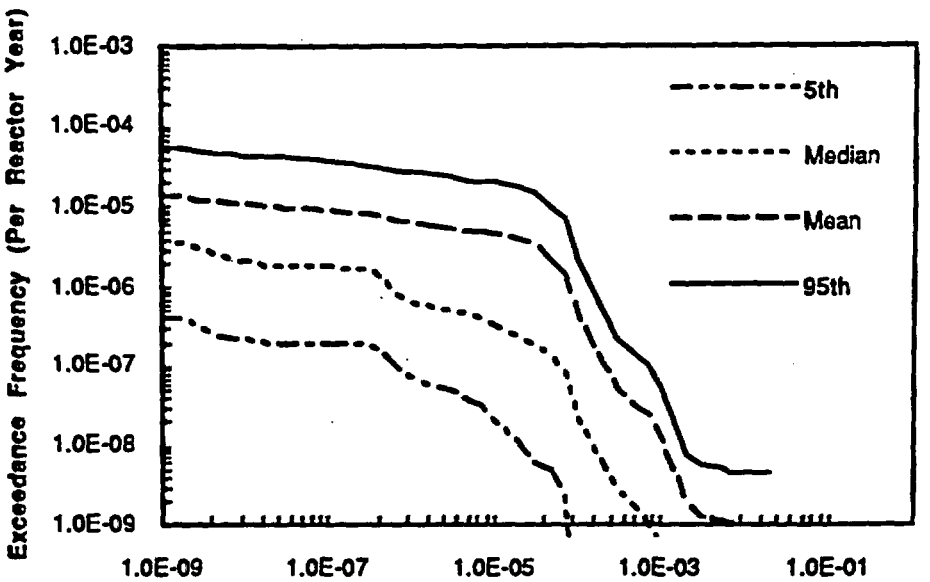


Figure 3.1-6. Societal CCDF



Offsite Prompt Fatality Risk to an Individual Within 1 Mile of the Site Boundary Due to Internal Initiators

Figure 3.1-7. Individual Risk

3.1.8.3 Uncertainty Analysis (Quantitative Method)

In Section 3.1.8.2, the method for obtaining an estimate of the risk of plant operation was described. The initial value of risk obtained will be referred to as a point estimate with no additional qualifiers. It is preferable not to characterize this as a "best-estimate" (mean or otherwise) value of risk, unless significant effort is spent by the analysts to assure that all the inputs to the various codes, and the models themselves, are truly the best available estimates. Whether mean, median, or mode is used is a judgment for the analyst. The most conservative result is easiest to defend.

Whether the risk estimate is thought of as merely a point estimate or as a best-estimate value, the single value has little real meaning. As with any engineering analysis, some representation of the uncertainty associated with the value obtained is essential. Since PRA results may well be used in making decisions relative to overall plant safety and the need for design improvements, the importance of putting the point-estimate result in the context of the associated uncertainty is crucial. Considering the sparseness of the data and the incompleteness of knowledge regarding some of the phenomena that are modeled, the uncertainty can be significant. Both the analysts and decision-makers would like to know which of the various uncertain aspects of the PRA models contribute most to the uncertainty in risk. This information can then be used to guide data-gathering programs and research into severe accident phenomena so that they focus on issues for which added knowledge will reduce uncertainty with regard to plant risk. In the course of performing a uncertainty analysis, sensitivity studies are usually performed to determine the effect of various input parameters on the risk results which yield important insights on the relative importance of operational parameters on the risk.

Uncertainty that stems from both incomplete knowledge of phenomena and the stochastic nature of some of the physical processes involved requires that the accident analysis be probabilistic. Incomplete knowledge of the phenomena leads to what will be referred to herein as model uncertainty. For a given context (i.e., series of events leading up to the point in time under consideration), the particular outcome of a single event in the accident progression may not be known. A number of possible outcomes can often be defined for each event considered. For example, an accident mitigating system, such as the carbon filters, can (1) operate as designed and retain all absorbed halogens; (2) overheat and release part of the adsorbed halogens; or (3) burn and release all deposited radionuclides. With a given aerosol loading and airflow, the expected filter response can be determined with reasonable accuracy using available engineering models and the uncertainty is relatively small. However, it is frequently the case that more than one model can be applied to predict the outcome for a particular event. For models that represent more complex severe accident phenomena, it is not uncommon for different models to predict different outcomes. Sufficient data to validate these models is typically not available for many severe accident phenomena.

The extent of damage resulting from a steam explosion is an example of a phenomenological event which is treated with large model uncertainty. In the context of evaluating accident progressions, a steam explosion can be sufficiently energetic to (1) permanently breach the confinement structure; (2) cause a momentary bypass of confinement; or (3) do no significant damage. Even if the conditions associated with the steam explosion are well characterized, a specific outcome cannot usually be assigned. Since there is uncertainty associated with the outcome of the event, there are multiple paths along which the accident can proceed, given a situation in which a steam explosion can occur. In an accident progression event tree (APET), each event outcome or branch is assigned a branching ratio. Where model uncertainty causes the specification of multiple possible outcomes, the branching ratio (in the point estimate) represents

the analyst's level of confidence that the indicated outcome would actually occur based on their knowledge of the phenomena.

APET branch points may also represent events for which uncertainty in the outcome is due to processes best modeled as random events. Examples include events that depend on hardware performance or human action. This type of variability in the outcome of an event is referred to as stochastic uncertainty. These events are treated using traditional reliability analysis techniques. Fault tree analysis is applied to determine the branching ratios that characterize the failure frequency of active system components, which are considered in the APET. Human error frequencies are evaluated for human actions that are modeled in the APET. The frequencies thus determined are used as the APET branching ratios for this type of event. Where the phenomena are governed by processes that are too complex to be reasonably modeled (i.e., no amount of research or data collection would allow resolution of which outcome occurred for a particular condition), they are represented as stochastic uncertainties. Weather and the probability of a steam explosion occurring are examples. Empirical evidence or data collection are combined with subjective judgments to evaluate branch points representing these uncertainties.

3.1.8.3.1 Method

In a simple engineering analysis, uncertainty can be propagated analytically. For instance, if the specific heat of a substance is measured using a calorimeter, an expression for this property would be written as a function of measured temperatures and the properties of materials used in the apparatus. Assuming that the dominant source of uncertainty was the thermocouple measurements, the uncertainty in the measured value of specific heat would be expressed as a function of the partial derivatives of the specific-heat expression with respect to the measured temperatures. Using this expression, combined with the known error in the thermocouple readings, an estimate of the uncertainty in specific heat is obtained.

The concepts used to estimate uncertainty in a PRA results differ little from those introduced by the above simple example. However, the risk model to which these concepts are applied is immensely more complex than the simple expression for the specific heat of a substance in terms of calorimeter measurements. The model for risk that is developed to obtain the point estimate is the basis for the uncertainty evaluation. This model actually consists of the ensemble of models for each module in the PRA (the accident initiation, the APET, the Source Term Algorithm, and the Consequence Model). Each module has a number of inputs that are uncertain. In some cases, most notably for the accident progression assessment (i.e., the APET), these inputs reflect uncertainty with respect to the most appropriate model to use for a certain phenomena. Because of the complexity of the risk model, numerical methods must be applied to characterize uncertainty and obtain the equivalent of the model's partial derivatives with respect to the uncertain inputs.

Monte Carlo Sampling techniques are usually used to evaluate the response of the model to variations in the uncertain inputs. The sampling process randomly selects sets of values for the model-input parameters that are considered to be uncertain. The model, and the module assembly process, is then exercised with each set of values in the sample to propagate the uncertainties through the entire calculational process. The mapping from input value combinations to risk estimates can be investigated using statistical techniques to obtain estimates of the relative importance of the various uncertainties considered.

To summarize how the uncertainty evaluation is accomplished, each module in the risk model ensemble should be viewed as a model with inputs that have some associated uncertainty. Each

module can be thought of as a function of its parameters; i.e., for output Y of the module, and inputs X_1—X_n, the response may be formulated as:

$$Y = f(X_1, X_2, \ldots, X_n),$$

where the analytic form of the function *f* is indeterminate but can be numerically approximated. The process of evaluating uncertainty involves three steps: identification of important parameters, assignment of probability distributions to those parameters, and propagation of these distributions through the function (computer code) to arrive at a distribution for the output variable. The final step amounts to an empirical characterization of *f* by constructing the partial (due to the finite number of parameter combinations evaluated) mapping from its inputs (X_i) to its output (Y). This process is similar to the generation of a response surface.

3.1.8.3.2 Sources of uncertainty

Uncertainty is inherent to the models that constitute the PRA, and is considered only within each module. The interfaces between the modules are not considered as sources of uncertainty. The grouping of results is required in order to reduce the size of the problem to a manageable level. In reality, errors in the assessed risk could be introduced at each interface. This would occur if a result from a module were placed in an inappropriate group for consideration in subsequent modules. Quality assurance procedures are used to minimize the likelihood of such errors.

Typical sources of uncertainty are:

- Plant damage state frequency
- Plant damage state uncertainty
- APET uncertainties
- Source Term Calculation Uncertainty
- Consequence Calculation Uncertainty

3.1.8.4 User-Established Criteria

Several organizations and/or agencies have proposed risk-based guidelines to assist the user in evaluating the acceptability of accident consequences. These include, inter alia, the U. S. Department of Energy Office of Defense Programs (DP), the U.S. Army (MIL), the Westinghouse M&O Nuclear Facility Safety Committee (NFSC), the Westinghouse Hanford Company (WHC), the Westinghouse Savannah River Company (WSRC), E.G.&G. Rocky Flats, and Martin Marietta (ORNL). The NFSC has recommended comprehensive risk acceptance guidelines for both radiological and nonradiological hazards. The latter are of interest to NRC only if the chemical hazards can cause or exacerbate a radiological accident scenario.

The user may choose to evaluate the accident scenario consequences against one of these existing sets of risk acceptance guidelines.

3.2 Assurance that Controls are in Place and Capable of Controlling Hazards or Accidents

Operating facilities must provide assurance that the hazards and accidents identified in Sections 3.1.4 and 3.1.5 are accompanied by controls that are in place and capable of functioning as intended. A system is presented to illustrate a method that can used effectively in the nuclear industry.

3.2.1 Operational Safety Requirements

Operational Safety Requirements (OSRs) are derived from the analyses and evaluations presented in License Aplications, Safety Analysis Reports, Integrated Safety Analyses, or other formal evaluations of the facility safety. The OSRs define the envelop of authorized operation of the nonreactor nuclear facility and formally documents the requirements in the following categories:

- Safety Limits and Limiting Control Settings
- Limiting Conditions for Operation
- Surveillance Requirements
- Design Features
- Administrative Controls

3.2.1.1 Safety Limits and Limiting Control Settings

Operation outside of a Safety Limit results in immediate shutdown of the affected portion of the facility, notification to the licensing authority, and approval of the licensing authority to restart. Safety Limits are specified only for those conditions that if exceeded could pose a serious risk to operating personnel or to the general public. For operation outside of an OSR other than a Safety Limit, operations within Technical Specifications are restored and the incident investigated and reported.

Limiting Control Settings are those numerical values (e.g., pressure, temperature, concentration) chosen such that if exceeded corrective action can be accomplished before the Safety Limit is exceeded. Failure to conform to these value should result in immediate shutdown or in restoration of operations to less than the Limiting Control Setting.

3.2.1.2 Limiting Conditions for Operation

Limiting Conditions for Operation defines those instruments, monitors, controls, and equipment that must be operable to ensure that the Safety Limits are not exceeded. All facility standards, tests, manuals, or operating procedures must be within the limits of the OSR. Also specified are the applicable actions and completion times required should failure to comply with a limiting condition for operation occur.

3.2.1.3 Surveillance Requirements

Surveillance and testing requirements are imposed on those instruments, monitors, controls and equipment required to be operable under Limiting Conditions for Operation. Numerical values for the maximum interval allowable between surveillance and/or testing are documented in this section.

3.2.1.4 Design Features

Design features to be included are those features of the facility such as materials of construction and geometric arrangement, which, if altered or modified, would have a significant effect on safety, and are not covered in the sections above.

3.2.1.5 Administrative Controls

Administrative Controls are the provisions relating to organization and management, procedures, record keeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner.

3.2.1.6 Bases

This should be an appendix to the OSR requirements. The appendix should provide summary statements of the reasons for the operating limits and associated surveillance requirements. The bases show how the numeric value, the condition, or the surveillance fulfill the purpose derived from the ISA.

Examples of portions of OSRs for a nonreactor nuclear facility are presented in Appendix D.

3.3 Assurance that Controls are Maintained

The accident analyses in the ISA should furnish the logical basis to derive comprehensive Operational Safety Requirements for the facility and its operations. In turn then, the most important role of the Operational Safety requirements is to ensure that the ISA is applicable to the process authorized. The Operational Safety Requirements require that those safety systems (for which credit is taken in the ISA) must be available to the process. Otherwise, the ISA is not available, and the facility is operating outside the ISA envelope.

Therefore, the ISA must conspicuously highlight the commitments (e.g. limits, parameters, assumptions on which the ISA conclusions depend) to clearly identify those items that are important to the safety of the facility.

3.3.1 Availability of Safety Systems

In order to ensure that the ISA is properly in effect, the availability of the safety systems to the extent required must be ensured by the combination of administrative controls, inspections, preventive maintenance, periodic calibrations, and testing. A safety system that is not available when needed is of no use in protecting the workers, general public, or the facility. The percentage availabilities of these functional systems depend on their importance to the analysis. If the system has adequate backup, a 90% availability may be adequate for those events for which the consequences are acceptable. However, other systems may have to be available at a much higher percentage to mitigate serious hazards.

The ISA should identify the organizational structure and controls that are in place to ensure adequate availability of important safety functions.

3.3.2 Preventive Maintenance

In order to provide the reliability assessed in the ISA, certain instruments, equipment, and systems must be given preventive maintenance. Preventive maintenance consists of regular

servicing of instrumentation and equipment (such as lubrication, recalibration, set point rechecks, and flow tests) so that the failure frequencies of vital equipment are effectively minimized so that the risks of operation are reduced in the ISA to acceptable levels.

The ISA delineates the provisions for preventive maintenance, the scope, and the frequency and timing of it. Sufficient information should be included to demonstrate a commitment to preventive maintenance as a tool for safety assurance. This information should include:

- A general description of the maintenance organization, objectives and philosophy.
- Responsibilities for maintenance functions.
- Structures, systems, components, and equipment included in the formal maintenance program.
- The management systems used to control maintenance activities and a description of the interfaces between the maintenance department and other organizations.

3.3.3 Testing

Testing may be done in place or on a bench. The purpose is to determine that the response to the input produces a result that is within the parameters described by the ISA. The ISA and Operational Safety Requirements delineate the provisions for testing, the scope of the tests, and the frequency and timing of the tests. The ISA furnishes the technical basis and describes the program for testing.

Thus the ISA should identify the plan for testing (and calibration of the test equipment) to determine that the safety-related items are acceptable for their intended use.

3.3.4 Administrative Controls

Administrative and procedural controls for a facility should be documented to delineate (1) clear lines of responsibility and methods for safe operation under normal and emergency conditions, and (2) a system of configuration control that requires internal and independent safety review, at a level of independence commensurate with risk, of all changes to components, equipment, procedures, and systems required for nuclear facility safety. Such an administrative and procedural control system ensures that basic and important decisions are made after review throughout appropriate elements of the organization and that decisions which could significantly affect nuclear safety are reviewed by at least one organization not directly responsible for operations.

Types of information that should be considered in formal policy include:

- Company organization. This delineates overall authority, responsibility, and accountability.
- Management policy. The overall facility activity should be considered as a system involving interaction of process, people, facilities, and procedures.
- Organizational responsibility. This clearly details the responsibilities of each suborganization in the hierarchy and the interactions among them.
- Authorization basis documentation. These controls, such as Operational Safety Requirements, provide the bounding condition for operation of the facility within the licensing requirements.

- Operating procedures. These controls prescribe detailed actions that are prescribed for normal, abnormal, and emergency conditions for the facility.

3.3.5 Emergency Preparedness

One of the elements of assurance that controls are maintained is an adequate emergency preparedness program. Presented is an overview of a typical emergency preparedness plan consisting of fourteen sections that can be used as a model.

3.3.5.1 Introduction

This section defines the purpose and scope of an emergency plan and provisions to identify hazards. The plan should be applicable to the following:

- Events (operational, transportation, etc.) with the potential to cause releases above allowable limits of hazardous materials to the environment.
- Events such as fires, explosions, tornadoes, hurricanes, earthquakes, dam failure, etc., that affect or may effect safety systems designed to protect site and offsite populations and the environment.
- Events such as bomb threats, hostage situations, etc., that reduce the security posture of the site.
- Events created by close proximity to the facility with a significant hazards potential.

The emergency plan should identify measures that are intended to provide maximum protection for onsite and offsite person, limit damage to facilities and equipment, limit adverse impacts on the environment and minimize impact on site operations and security.

3.3.5.2 Emergency Response Organization (Internal)

This section identifies the positions, responsibilities and operations of the onsite emergency organization. Included are directions on the declaration of an emergency, activation of emergency response facilities, and specific duties of emergency management personnel.

3.3.5.3 Offsite Response Interfaces

This section addresses the role of offsite organizations and expected assistance and response. Included are specific contacts that need to be made.

3.3.5.4 Operational Emergency Event Classes

This section addresses classification of operational emergencies at the facility. The objective is to promptly classify an emergency condition using Emergency Action Level criteria into levels commonly understood by on and offsite officials to provide for a graded response. Figure 3.3-1 shows an example of a prompt classification matrix.

3.3.5.5 Notification and Communication

This section provides information on the notification processes and the communications systems used if there is an emergency at the facility. The notification/communication process includes the following:

- The facility emergency response organization
- Site populations who may be required to take protective actions
- Appropriate offsite authorities including other agencies that may assist in the response upon request
- Appropriate offsite regulatory agencies as required by law (e.g., Comprehensive Environmental Recovery, Compensation and Liability Act (CERCLA), Emergency Planning and Community Right-to-Know Act (EPCRA), etc.
- Members of the general public

ATTACHMENT 1- PROMPT CLASSIFICATION MATRIX		
Category ⇒ Classification ⇓	**1-RADIOACTIVE RELEASE**	**2-TOXIC CHEMICAL RELEASE**
General Emergency (GE)	Radiation Dose (actual or projected) beyond the site boundary is ≥ 1 rem TEDE ≥ 5 rem CDE Thyroid ≥ 50 rem EDE Skin Dose	Chemical Exposure (actual or projected) beyond the site boundary is ≥ ERPG-2
Site Area Emergency (SAE)	Radiation Dose (actual or projected) between the facility boundary and the site boundary is ≥ 1 rem TEDE ≥ 5 rem CDE Thyroid ≥ 50 rem EDE Skin Dose	Chemical Exposure (actual or projected) between the facility boundary and the site boundary is ≥ ERPG-2
Alert	Radiation Dose (actual or projected) 30 meters (100 ft) from the point of release and the facility boundary is ≥ 1 rem TEDE ≥ 5 rem CDE Thyroid ≥ 50 rem EDE Skin Dose	Chemical Exposure (actual or projected) 30 meters (100 ft) from the point of release and the facility boundary is ≥ ERPG-2
Notification of Unusual Event (NOUE)	Radiation Dose (actual or projected) at the site boundary is ≥ 0.1 mrem TEDE	*NONE*

FIGURE 3.3-1

ATTACHMENT 1- PROMPT CLASSIFICATION MATRIX		
Category ⇨ Classification ⇓	3-OPERATIONAL EVENTS	4-NATURAL DISASTERS
General Emergency (GE)	*NONE*	*NONE*
Site Area Emergency (SAE)	• Loss of Essential Cooling Water - and - • High Range Radiation Monitor >10 rem/hr	Damage to facility safety systems by tornado or high winds ---------- Earthquake ≥ 5.3 on Richter Scale (DBE)
Alert	Loss of all AC and DC power for ≥ 15 minutes ---------- A confirmed criticality occurs	Hurricane forecasted to arrive at SRS in less than 1 hour ---------- Tornado touches down within limited area fence resulting in any facility structural damage ---------- Earthquake ≥ 3.5 but < 5.3 on Richter Scale
Notification of Unusual Event (NOUE)	Any radiological Technical Specification or Technical Standard limit is exceeded which requires a process shutdown	*NONE*

FIGURE 3.3-1 (Cont.)

3.3.5.6 Consequence Assessment

This section describes the methods, systems and equipment available for assessing the actual or potential emergency conditions and the impact of an emergency on the facility. This includes the initial assessments made in the early stages of an emergency, the extended assessments that may continue for several days and the post-accident assessments that may continue for several years.

3.3.5.7 Protective Actions

This section deals with equipment, procedures and response actions at the facility necessary to provide maximum protection for onsite and offsite populations. For hazardous material emergencies, protective actions are designed to keep onsite and offsite exposures As Low As Reasonably Achievable (ALARA). This is accomplished by minimizing time spent in the vicinity of the hazard, keeping as far from the hazard as possible and taking advantage of available shielding. For emergencies based on safeguards and security events, protective actions are designed to provide maximum physical safety on onsite personnel while maintaining operational and security integrity of the facility.

3.3.5.8 Medical Support

This section identifies the medical resources available onsite and interactions that occur with offsite sources of assistance.

3.3.5.9 Recovery and Reentry

This section describes the planning, stipulations, roles, and responsibilities related to entry into and conduct of operations during the recovery phrase of an emergency.

3.3.5.10 Public Information

This section discusses the organization and facilities used to provide accurate and timely information to the public for facility emergencies. This section also discusses the requirements for providing pre-emergency information to the public, offsite authorities and local media.

3.3.5.11 Facilities and Equipment

This section describes the emergency response facilities and equipment identified for use in an emergency to support the activities of members of the emergency response organization.

3.3.5.12 Training

The purpose of this section is to define the emergency management training program and administration requirements for all personnel at the facility It encompasses the following major training plan elements: emergency management training goals, organization, responsibilities, methodology; courses for planners and hazards assessment personnel, training requirements, examination, record keeping; offsite programs for personnel, training support, and training; and instructor training and qualification.

3.3.5.13 Drills and Exercises

This section identifies the process whereby drills and exercises are conducted to develop, maintain and test response capabilities of the emergency response organization members, and validate adequacy of emergency facilities, equipment, procedures, and training.

3.3.5.14 Emergency Management Program Administration

This section delineates responsibilities related to management of specific elements of the facility's emergency management program. It addresses plan and procedure development and administration of the emergency response organization.

3.4 Assurance that Integrated Safety Analysis is Adequate

3.4.1 Training of Analysts

Adequate training of analysts is a prerequisite of an effective integrated safety analysis. Experience has shown that untrained or inadequately trained personnel will not produce a quality product primarily due to errors of omission in identifying hazards and in a lack of accounting for common mode effects. For quantitative assessments, a novice will generally underestimate the frequency of an accident by two orders of magnitude.

Formal training courses are available through professional societies, such as the American Institute of Chemical Engineers, and through a number of private engineering firms specializing in hazards and risk assessment. Ideally, those personnel who will be performing the assessments should receive both text book training and on-the-job training by qualified instructors. Formal training of personnel that will not be directly involved in assessments is usually not cost effective nor should there be a significant delay between the training and the assessments.

Core competency can be maintained by bringing on new personnel in the actual assessments. Failure to do so can result in loss of corporate memory and a return to square one on the ISA updates.

3.4.2 Management Support

Effective integrated safety programs must be vertically integrated from the working teams through the site manager. This may be accomplished either by direct line organization or by recognized sponsorship. No program will be more effective than the interest and resources supplied from the top. Management must recognize that the safety effort is not a one-shot proposition but a continuing effort in which the integrated safety analysis becomes a living document to be reflected throughout the lifetime of the facility.

3.4.3 Lessons Learned from Accidents

To protect against recurrence, it is vital that lessons are learned from accidents that occur, the basic reason that they occurred, and that corrective measure be implemented. Two methods are presented that may be used for this purpose, Management Oversight and Risk Tree and root cause analysis.

3.4.3.1 Management Oversight and Risk Tree

MORT is a comprehensive analytical procedure that provides a disciplined method for determining the causes and contributing factors of major accidents, Reference 45. Alternatively, it serves as a tool to evaluate the quality of an existing system. While similar in many respects to fault tree analysis, MORT is more generalized and presents many specific elements of an ideal "universal" management program for optimizing environment, safety and health, and other programs.

The MORT principle has two meanings:

1. A total safety program concept (viewed as a specialized management subsystem) focused upon programmatic control of industrial safety hazards

2. The actual logic diagram which displays the structured set of interrelated safety program elements and concepts comprising the ideal management program model called MORT. This universal logic diagram becomes a master "work sheet" for use in analyzing a specific accident or alternatively for use in the evaluation and appraisal of an existing safety program for accident potential

As an ideal management program, MORT is designed to include the following:

1. Prevent management oversights, errors, and omissions.

2. Result in identification, assessment, and referral of residual risks to proper management levels for appropriate action.

3. Optimize allocation of resources available to the program and to individual hazard control effort.

Integrated into the MORT program model are the best features of exemplary safety programs found in the U.S. (i.e., management implementation, hazards analysis, human factors analysis, work processes, monitoring, information systems, and organizational systems and services).

Innovative concepts, such as the sequential role of unwanted energy flow, barriers to energy transfer, error, change, and risk are systematically related along with the most current concepts of the behavioral, organizational, and analytical sciences.

Translated to "analytical MORT" (the MORT logic diagram), these features of "programmatic MORT" accumulate to over 1,500 "basic events" (i.e., causative problems or preventive measures related to an ideal safety system). These, in turn, underlie nearly 100 different generic problems identified in successively broader areas of management and accident prevention. Incorporated into the above listed concepts are some 50-70 "new ideas". (The actual number is highly subjective, depending upon a person's background and experience.) The way in which the MORT concept (programmatic MORT) is schematically represented by a logic diagram (analytical MORT) is shown in Figure 3.4-1.

Fundamental to a successful accident investigation or safety program evaluation is the assignment by higher management of technically qualified, competent, safety motivated personnel to participate in the investigation. More details of the MORT process are presented in Appendix E.

The strengths of this method are:

- Widely accepted
- Thorough
- Depicts idealized safety system
- Works well in conjunction with HAZOPs

Limitations are:

- Considerable training required
- Trees are cumbersome
- Always leads to management problem
- Not equipment oriented

3.4.3.2 Root Cause Analysis

The Root Cause Analysis system, Reference 46, is designed for use in investigating and categorizing the root causes of occurrences or accidents. Root Cause Analysis is simply a tool to help investigators describe what happened during a particular occurrence, to determine how it happened, and to understand why it happened. Only when investigators are able to determine why a failure occurred will they be able to specify workable corrective measures.

Most incident investigation systems allow investigators to answer questions about what happened during an accident and about how the accident occurred, but often they are not encouraged to determine why the failure occurred. Assume an occurrence during which an operator is instructed to close Valve A; instead, he closes Valve B. The typical investigation would probably result in the conclusion that "operator error" was the cause of the occurrence. This is an accurate description of what happened. An operator committed an error by manipulating the wrong valve. If the investigators stopped at this level of analysis' however, they have not probed deeply enough to understand the reason for the mistake. Generally, mistakes do not "just happen." They can be traced to some well defined causes. In the case of

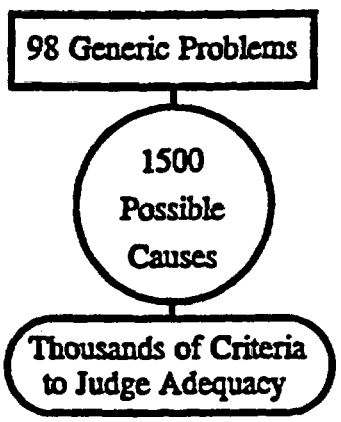
MORT is simply a diagram which arranges safety program elements in an orderly and logical manner. It presents a schematic representation of a dynamic, idealized (universal) safety system model using Fault Tree Analysis methodology.

MORT structures the largely unstructured safety literature and current best safety practices into three levels of relationships:

a. Generic Events (Problems)

b. Basic Events (Causes)

c. Criteria (Judgment rationale from the MORT text)

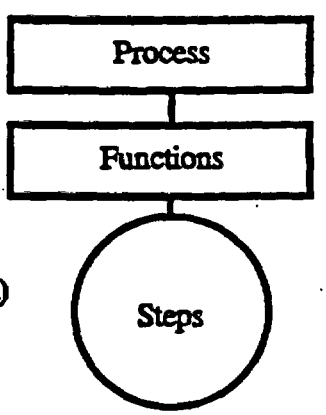


MORT makes explicit:

a. The functions necessary to complete a process.

b. The steps to fulfill a function.

c. Judgment criteria (from the MORT text) by which to judge when a step is well done or is "less than adequate" (LTA).



It provides relatively simple decision points in an accident analysis or safety system evaluation and enables an analyst or evaluator to detect omissions, oversights, or defects.

FIGURE 3.4-1 MORT Logic Diagram

the valving error, we might ask if the procedure is confusing. Were the valves clearly labeled? Was the operator who made the mistake familiar with this particular task? These are all questions that should be asked to determine why the error took place.

When the investigation stops at the point of answering what and how the recommendations for preventing recurrence of the accident may be deficient. In the case of the operator who turned the wrong valve, we are likely to see recommendations like "Remind all operators to be alert when manipulating valves" or "Emphasize to all personnel that careful attention to the job should be maintained at all times. Such recommendations do little to prevention of future occurrences. Investigations that probe more deeply into why the operator error occurred are able to provide more specific, concrete recommendations. In the case of the valving error, examples might include, "Revise procedures so that references to valves match the valve labels found in the field" or " Require trainees to have a training procedure in hand when manipulating the valves."

The Root Cause Analysis system provides a structured approach for investigators trying to discover the whys surrounding a particular occurrence. Identifying these root causes is the key to preventing similar occurrences in the future. The added benefit of Root Cause Analysis is that, over time, the root causes identified across the population of occurrences can be used to pinpoint major opportunities for improvement. For example, if a significant number of investigations point to procedure inadequacies as root causes, then resources can be focused on procedure improvement programs. Trending of root causes allows tracking causes of occurrences, development of systematic improvements, and assessment of the impact of corrective programs.

Further information on Root Cause Analysis is presented in Appendix E.

The strengths of this method are:

- Simple to use
- Structured
- Minimal training required
- Built-in verification
- Relatively fast
- Identifies all causes

Limitations are:

- Some subjectivity required
- Finite number of root caused defined
- Not widely known system

3.4.4 Good Practices

This section contains a number of practices used by seasoned risk analysis organizations that have proven to be effective. Recognize that these practices are by no means the only acceptable methods and presented only to provide some ideas for further thought.

3.4.4.1 Team Approach

If possible a team approach should be used in conducting the procedures outlined in this manual. Generally, individuals do not have all of the qualifications necessary to ensure that a comprehensive and accurate analysis will be done. In an idealized environment, a team leader should be appointed that has been trained in the various techniques to be used. Otherwise, the analyses will tend to drift away from the ultimate goal of the ISA. In addition to a team leader, the following personnel should be considered.

- Process engineer. This person should be thoroughly familiar with the design of the process and how it should respond to process transients.
- Facility operator. This person should be thoroughly familiar with how the process and equipment realistically behaves, the reactions that personnel can accomplish under various event scenarios, and the history of the past events. Maintenance and electrical mechanics also can provide a perspective valuable for an ISA assessment.
- Safety specialist. This person should be familiar with mandated requirements imposed on the facility and the various safety features available should the ISA indicate the necessity for changes to the design.

3.4.4.2 Employee Buy-In

Facility employees, especially operating personnel, must have buy-in to the contents of an ISA if the analysis is to be highly effective in controlling safe operation of the facility. This requires participation in the preparation wherever possible, training on what the document contains, ready access for reference, and rapid response to suggested improvements. The most effective safety programs are those in which the employees feel that they are truly a part of the program. This culture must stem from top management in a committed fashion.

3.4.4.3 Incident Records

Corporate memory has historically been short where accidents are concerned. Retirement, changing job assignments, and time contribute to this loss of memory. As a result, many accidents tend to repeat themselves. One very effective method of maintaining this memory is through the use of a computer data base containing process upsets, accidents, injuries, releases of hazardous materials, and equipment failures. Such a data base has many uses far beyond direct ISA application as shown in Table 3.4-1. Reference to one such system is presented in Reference 47.

Although such a data base must be protected to prevent inadvertent altering or erasure, employees should be allowed read-only access and encouraged to use the information. One direct application is in accident investigations in which the history of similar occurrences are resurrected both as a reminder and as training for new employees.

TABLE 3.4-1 Uses for an Incident Data Base

- Failure rate data
- Equipment breakdown histories
- Generic incident histories
- Data for Integrated Safety Analyses
- Dates of specific incidents
- Consequences of incidents
- Data for design studies
- Data for quality assurance studies
- Trend analyses
- Data for project justification
- Data for process hazards analyses
- Training
- Process problem solving
- Management decision data
- Studies of effectiveness of administrative controls
- Incident audit information
- Data for reliability studies
- References to source documents

3.4.4.4 Unreviewed Safety Question Determination

The Unreviewed Safety Question process is an effective method of ensuring that the proper authorization basis for an existing facility has been properly identified and validated. It is especially useful for an existing facility in which changes are proposed or in which discoveries are made for situations that have not been previously analyzed. The process is detailed in DOE Order 5480.21, Reference 48.

3.5 References

1. Guidelines for Chemical Process Quantitative Risk Analysis, Center for Chemcial Process Safety, American Institute of Chemcial Engineers, 1989.

2. Example Process Hazards Analysis of a Department of Energy Water Chlorination Process, DOE/EH-0340, September 1993.

3. H. H. Howard and C. L. Faust, The HIT Method: A Hazards Identification Technique, LA!-11507-MS/CV-7078, March 1989.

4. Fault Tree Handbook. NUREG-0492, Office of Nuclear Regulatory Research. U.S. Nuclear Regulatory Commission, Washington, DC, January 1981.

5. Reactor Safety Study, WASH-1400 (NUREG/CR-75/014, August 1975.

6. W.S. Durant, C.R. Lux, and D.F. Baughman, Data Banks for Risk Assessment at the Savannah River Site, WSRC-RP-89-1298, Westinghouse Savannah River Company, Aiken, SC, April 1990.

7. SAS User's Guide: Basics, SAS Institute, Inc., Cary, NC

8. D. I. Gertman et al., Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), NUREG/CR-4639, June 1989.

9. C. H. Blanton and S. A. Eide, Savannah River Site Generic Data Base Development, WSRC-TR-93-262, June 30, 1993.

10. A. H. Dexter and W. C. Perkins, Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant, DP-1633, July 1982.

11. J. N. Wilkinson et al., Idaho Chemical Processing Plant Failure Rate Database, WIN-330, October 1991.

12. Nuclear Plant Reliability Data System (NPRDS), Southwest Research Institute, San Antonio, TX.

13. D. S. Cramer, Valve Reliability for the Level 1 PRA, WSRC-RP-89-776, 1991.

14. D. S. Cramer, Check Valve Reliability for the Level 1 PRA, WSRC-RP-90-1258, 1991.

15. M. J. Rossi, Nonelectronic Parts Reliability Data, NPRD-3, 1985.

16. L. C. Cadwallader and M. A. Stolpe Gavett, Tritium Waste Treatment System Component Failure Data Analysis from June 18, 1984 to December 31, 1989, EGG-FSP-8973, Rev. 1, November 1990.

17. L. C. Cadwallader et al., Tritium Room Air Monitor Component Failure Data Analysis from January 1, 1984 to December 31, 1990, EGG-FSP-9450, May 1991.

18. L. C. Cadwallader and D. P. Sanchez, Secondary Containment System Component Failure Data Analysis from 1984 to 1991, EGG-FSP-10323, August 1992.

19. H. Wykoff, The Reliability of Emergency Diesel Generators at U.S. Nuclear Power Plants, NSAC/108, September 1986.

20. J. A. Derdiger et al., Component Failure and Repair Data for Coal-Fired Power Units, Topical Report AP-2071, Research Project 239-2, October 1981.

21. P. Daling et al., Preliminary Characterization of Risks in the Nuclear Waste Management System Based on Information in the Open Literature, PNL-6099, 1990.

22. S. Cohen and R. Dance, Scoping Assessment of the Environmental Health Risk Associated with Accidents in the LWR Supporting Fuel Cycle, Contract No. 68-01-2237, Teknekron, Inc., 1975.

23. R. Erdmann et al., Status Report on the EPRI Fuel Cycle Accident Accident Risk Assessment, EPRI NP -1128, 1979.

24. R. Fullwood and R. Jackson, Actinide Partitioning-Transmutation Program Final Report VI. Short-Term Risk Analysis of Reprocessing, Refabrication, and Transportation, SAI-099-78-PA, 1980.

25. R. Cooperstein et al., Hazards Analysis of a Generic Fuel Reprocessing Facility, SAI/SR-113-PA.

26. Karn-Bransle-Sakerhat, "Handling of Spent Nuclear Fuel and Final Storage of Vitrified High Level Reprocessing Waste", Safety Analysis, Vol. IV, 1977.

27. Smith and Kastenberg, "On Risk Assessment of High Level Radioactive Waste Disposal.", Nuclear Engineering and Design, 39, 293-333, 1976.

28. Regulatory Analysis Technical Evaluation Handbook, Prepared for the Division of Regulatory Applications, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1993 (Draft).

29. W. S. Durant et al., "Data Bank for Probabilistic Risk-Assessment of Nuclear-Fuel Reprocessing Plants." IEEE Transactions on Reliability, Vol. 37, No. 2, June 1988.

30. L. M. Arnett, Quantitative Analysis of Reactor Safety. DP-1168, 1968.

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

32. H.A. Linstone and M. Turoff, The Delphi Method: Techniques and Applications, Addison-Wesley, Reading, MA (1975).

33. D. E. Lucas, "Safety Analysis Guide for Nonreactor Nuclear Facilities", Hanford Engineering Development Laboratory, Report HEDL MG-153 (1981).

34. P. L. Clemens, "A Method of Combinatorial Failure Probability Analysis Using MIL-STD-882A", Sverdrup Technology, Inc., Report (April 1982).

35. "Safety Analysis and Review System for AL Operations", DOE Albuquerque Operations Office Order AL 5481.1A (September 15, 1982).

36. "Criteria for the Design of Plants for the Manufacture of Mixed Oxide (U-Pu) Fuels", ANSI N46.1, American National Standards Institute, Inc., New York, NY (1976).

37. A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", US Nuclear Regulatory Commission Report NUREG/CR-2300 (1983).

38. J. C. Elder, et al, "A Guide to Radiological Accident Considerations for Siting and Design of DOE Nonreactor Nuclear Facilities", Los Alamos National Laboratory Report LA-10294-MS (1986).

39. "Guidance for Consequence Assessment," DOE Emergency Management Guide, USDOE, July 28, 1992. Established by DOE Order 5500.3a, "Planning and Preparedness for Occupational Emergencies", April 30, 1991.

40. S. A. McGuire, A Regulatory Analysis on Emergency Preparedness for Fuel Cycle and Other Radioactive Material Licensees, NUREG-1140, USNRC, January 1988.

41. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.145: Atmospheric Dispersion Models for Potential Accident Consequence Assessments at Nuclear Power Plants, Washington, DC, 1979.

42. U.S. Department of Energy, Internal Dose Conversion Factors for Calculation of Dose to the Pulic, DOE/EH-0071, Washington, DC, July 1988.

43. International Commission on Radiological Protection, "Age-dependent Doses to Members of Public from Intakes of Radionuclides," Annuls of the ICRP, Publication 56, Part 1, Pergamon Press, Vol. 20, No. 2, 1989.

44. International Commission on Radiological Protection, "limit for Intake of Radionuclides by Workers," Annuls of the ICRP, Publication 30, Part 1, Pergamon Press, Vol. 2, No. 3, 1979.

45. MORT User's Manual, U.S. Department of Energy, DOE-76-45/4, February 1992.

46. Root Cause Analysis Handbook, WSRC-IM-91-3, Westinghouse Savannah River Company, Aiken, SC, January 2, 1991.

47. W.S. Durant, et al, Data Bank for Probabilistic Risk-Assessment of Nuclear-Fuel Reprocessing Plant," IEEE Transactions on Reliability, Vol 37, No 2, June 1988.

48. Unreviewed Safety Questions, DOE Order 5480.21, U.S. Department of Energy, December 24, 1991.

4.0 DOCUMENTATION

Elements of good practice in safety documentation are presented and discussed here.

4.1 Purpose

Proper and complete documentation is important to:

- Record the details and the results of the analysis for:
  - review and comment
  - approval
  - use in license applications or renewals
  - future reference
  - a baseline for comparison to future changes in safety-related process equipment
- Identify the detailed assumptions in the analysis:
  - as a basis for operational safety requirements
  - for future reference
  - for use in revising the analysis

The assumptions made in an analysis are the foundation for the scope and breadth of an integrated safety analysis.

4.2 Quality Assurance

Most successful organizations in nuclear operations have a Quality Assurance (QA) program that specifies requirements for recording the details that comprise their compliance documentation. Through implementation of these requirements, the organization will successfully implement and maintain a prevention oriented QA Program ensuring that their products and services met requirements, are suitable for use, and satisfy the customers' expectations. Barring such an existing program, this manual presents a proven method to achieve these goals. Included are a description of requirements, responsibilities, and controls necessary for systematic implementation of sound QA program for documentation of an ISA.

Basically, three individuals or groups of individuals must assume these responsibilities; the originator, the reviewer, and the management.

The originator:

1. Prepares the formal documentation in accordance with this procedure.
2. Responds to the reviewer's questions and comments, and take necessary action to resolve them.
3. Obtains management review and approval for any deviations from the procedures.
4. Ensures that the completed analysis is filed in a control system and issued to the requestor.

The reviewer:

1. Reviews the adequacy of the analysis.
2. Signs and dates the analysis to document the review and the resolution of review comments.

The responsible manager (or designee):

1. Assigns qualified personnel as Originators and Reviewers.
2 Ensures that preparation and review, as described in this procedure, is implemented.
3. Resolves any comments on which the Originator and Reviewer cannot agree.
4. Reviews and approves, when appropriate, deviations from standard methodology.
5. Approves the completed analysis.

APPENDICES

APPENDIX A.1 URANIUM FUEL FABRICATION CHECKLIST

In this example, the checklist method is used to study criticality hazards in a Uranium Fuel Fabrication operation. The process, shown in Figure A.1-1, begins with a roll-type compaction unit that takes UO_2 powder and binder-lubricant and combines it before feeding to the pellet presses where pellets are formed. The pellets are transferred in boats to the sintering furnace, where the pellets are sintered in a hydrogen atmosphere to 95% theoretical density. The pellets are then ground to precise dimensions, and dried. Dried and inspected pellets are loaded into empty fuel tubes which are pressurized and sealed. Finished fuel rods are loaded into and stored.

It has been shown that there are safe if no excess moderator material is present and if analyzed geometries of SNM is maintained.

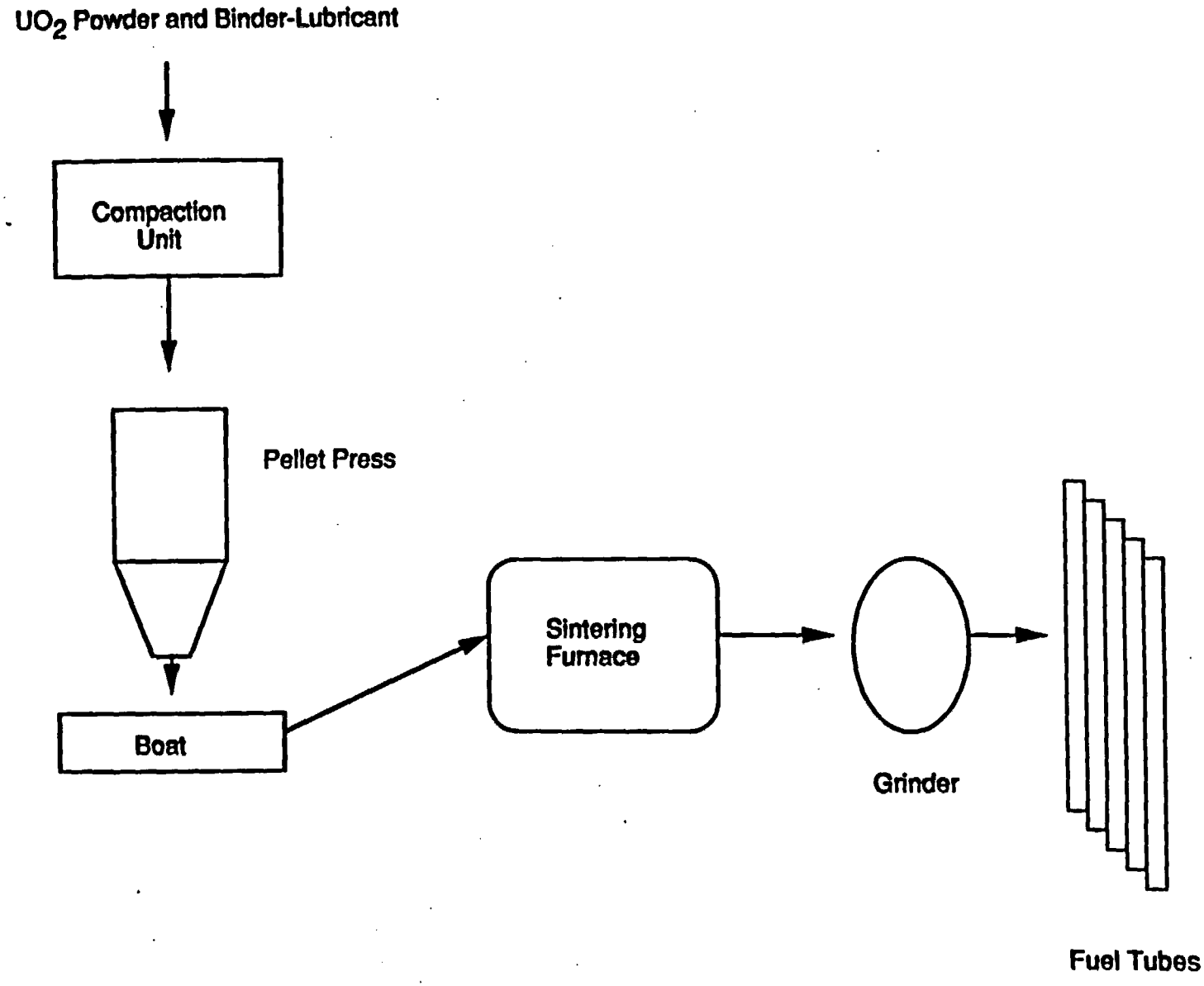


Figure A.1-1
Uranium Fuel Fabrication

APPENDIX A.1

Example "What-If" Analysis of Uranium Fuel Fabrication

Process Section: Pelleting

Subject: Criticality

What-If/Cause	Consequence/Hazard	Safeguards
Moderation Control Fails Because:		
-hydraulic fluid leaks	moderator reaches powder/ criticality	all hydraulic fluid systems are shielded from powder
-powder is not dry enough	moderator reaches powder/ criticality	multiple qulaity control steps for analytical results
-room floods	moderator reaches powder/ criticality	no piped water systems in bulk powder handling areas
-bulk powder storage container collects and holds liquid	moderator reaches powder/ criticality	bulk containers are moved with sealed opening facing down
Geometry Control Fails Because:		
-cart tips over	safe geometry exceeded/ criticality	passive stops welded to bottom of carts
-powder builds up in pelletizing equipment	safe geometry exceeded/ criticality	buildup prevention devises within equipment
-small powder storage container breaks	safe geometry exceeded/ criticality	containers are of rugged construction, containers are administratively protected
-sintering boats are stacked too high	safe geometry exceeded/ criticality	training, administrative controls

APPENDIX A.1

Example "What-If" Analysis of Uranium Fuel Fabrication (Cont.)

Process Section: Fuel Rod Loading and Bundle Assembly

Subject: Criticality

What-If	Consequence/Hazard	Safeguards
Moderation Control Fails Because:		
-assembly shroud collects moderator	moderator reaches rods/ criticality	shrouds are split to prevent accumulation
-room floods	moderator reaches rods/ criticality	no piped water systems in bulk powder handling areas
Geometry Control Fails Because:		
-stored fuel rods are stacked	safe geometry exceeded/ criticality	storage and transport containers have controlled thickness, only one channel of rods may be transported at a time, adminsistrative controls and training
-assemblies are stored too close	safe geometry exceeded/ criticality	storage racks control spacing
-assemblies are spaced too closely during cleaning	safe geometry exceeded/ criticality	wash tanks have spacers to control distance
-rods dissolve during cleaning step	safe geometry exceeded/ criticality	wash tank contents are strictly controlled
-poison inserted to supplement geometry is removed	safe geometry exceeded/ criticality	boral shelves are fixed inside carts

NOTES TO EXAMPLE PROCESS MATRIX:

A. UF_6 is a radioactive, toxic, unstable, and reactive compound.
B. Flammable solvents are fire hazards.
C. Fire is a hazard where it is part of the process.
D. Represents a list of additional hazards. This list of hazards is typical, but incomplete. The analyst should complete it from other sources, such as HAZOPS or "What if...?" meetings.

Node 3.3B, for example, is translated as "Flammable Solvent (Fire) Hazard in Solvent Extraction." Node 1.2A is "UF_6 Hazards during Vaporization."

APPENDIX A.3

Example Chemical Matrix for ADU Process

	UF_6	UNH	UO_2F_2	ADU	HF	HNO_3	NH_4OH	NH_3	H_2O	STEAM	N_2
UF_6		X				X			X	X	
UNH	X										
UO_2F_2											
ADU											
HF							X	X			
HNO_3	X						X	X			
NH_4OH					X	X					
NH_3					X	X					
H_2O	X										
STEAM	X										
N_2											

X - Indicates Incompatability, Potential Worker Hazard

Table A.3-2 List of Chemicals for which Limit Parameters were Analyzed

No.	CHEMICAL NAME	Chemical formula	CAS No.	State	MP °C	BP °C	Units	MW
1	Ammonia	NH_3	7664-41-7	G	-77.7	-33.35	ppm	17.0
2	Ammonium Hydroxide	NH_4OH	1336-21-6	L	-77			35.06
3	Hydrogen Fluoride	HF	7664-39-3	G	-83.1	19.54	ppm	20.1
4	Nitric Acid	HNO_3	7697-37-2	L	-42	86	ppm	63.0
5	Uranium Hexafluoride	UF_6	7783-81-5	S < 64°C	64.5 [1]		mg/m^3	352.0
6	Uranyl Nitrate (UNH)	$UO_2(NO_3)_2.6H_2O$	13520-83-7	S < 60.2°C	60.2	118	mg/m^3	502.1
7	Steam	H_2O		G > 100°C				18
8	Water	H_2O		L < 100°C	0	100		18

Table A.3-3 Concentration Limit Parameters found for Chemicals listed in Table A.3-2

No	A			B				C					D		
	PEL-TWA	TLV-TWA	CEGL CE90	ERPG E1	PEL-STEL	TLV-STEL	3TLV TWA	ERPG E2	EEGL EE60	EPA LOC	PEL-C/ TLV-C	3TLV TWA	ERPG E3	EEGL EE30	NIOSH IDLH
	(1)	(2)	(3)	(4)	(5)	(6)	3x (2)	(7)	(8)	(9)	10/11	5x (2)	(12)	(13)	(14)
1	50	25	50	25	35[1]	35		200	100	50			1000		500
2											50[1]/-				
3	3			5	6[1]			20		2	-/3		50		30
4	2	2		2	4[1]	4	6	15		10			30		100
5	0.05[2] 0.2[1,3]	0.2		1		0.6		10					20		20[2] 30[3]
6	0.05[2]	0.2		1		0.6		10					20		20[2]
7															
8															

Notes:
1. Values vacated by court order
2. Soluble compounds
3. Insoluble compounds

- PEL-TWA, PEL-STEL, and PEL-C values are OSHA workplace rgulatory limits (29 CFR 1910.1000)
- TLV-TWA, TLV-STEL, and TLV-C values are workplace guidelines published annually by the American Conference of Governmental Industrial Hygienists (ACGIH), headquartered in Cincinnati, Ohio.
- EEGL (Emergency Exposure Guidance Levels for 30 or 60 minute exposures) and CEGL (Continuous Exposure Guidance Levels for 90 day exposures) were developed by National Academy of Sciences committee for military use.
- ERPG (Emergency Response Planning Guidelines) values are being developed by a technical committee of the American Industrial Hygiene Association (AIHA) for use in emergencies for increasingly severe exposure situations.
- LOC (Levels of Concern) were published by the EPA , DOT and FEMA as part of their Technical Guidance for Hazards Analysis: Emergency Planning for Extremely Hazardous Substances (1987).
- IDLH (Immediately Hazardous to Life or Health) values were developed by NIOSH for use in the event of respirator failure in the workplace.

Table A.3-4 Handbook of Reactive Chemical Hazards

No	CHEMICAL NAME	Hazard Information	Bretherick 3rd e
			Reference page
1	Ammonia	Potentially violent or explosive reactions on contact with nitric acid. A jet of ammonia will ignite in nitric acid vapor (ambient temperature). Incompatable with HF, HNO_3, and UF_6. Emits toxic fumes of NO_2 when heated.	1177
2	Ammonium Hydroxide	Incompatable with HF, HNO_3, and UF_6.	1205
3	Hydrogen Fluoride	Violent reaction with NH_4OH Reacts with steam or water to produce toxic and corrosive fumes	1044
4	Nitric Acid	The common chemical most frequently involved in reactive incidents, reactions do not generally require addition of heat. Ignition on contact with HF. Incompatible with NH_4OH Will react with steam or water to produce heat and toxic and corrosive fumes The oxidising power and hazard potential of HNO_3 increases with concentration.	1100
5	Uranium Hexafluoride	Violent reaction with water.	1078
6	Uranyl Nitrate (UNH)	Decomposes at 100°C	1302
7	Steam		
8	Water		

Notes: 1. MP at 2 atmospheres. Volatile crystals sublime. Triple point - 64.0°C.

Chemical reactions:

1. $UF_6 + UO_2(NO_3)_2.6H_2O$ + water --> UO_2F_2 + 4HF + $UO_2(NO_3)_2.6H_2O$ + heat

   or, in the absence of water, UF_6 could strip some water from UNH, e.g.,
   $3UF_6 + 2UO_2(NO_3)_2.6H_2O \rightarrow 3UO_2F_2 + 6HF + UO_2(NO_3)_2.3H_2O$
   (Other similar reactions are also possible).

2. $UF_6 + HNO_3$ + water --> UO_2F_2 + 4HF + HNO_3 + heat

3. $UF_6 + 2H_2O \rightarrow UO_2F_2 + 4HF$

4. UF_6 + Steam --> UO_2F_2 + 4HF

5. $HF + NH_4OH \rightarrow NH_4F + H_2O$

6. $HF + NH_3 \rightarrow NH_4F$

7. $HNO_3 + NH_4OH \rightarrow NH_4NO_3 + H_2O$

8. $HNO_3 + NH_3 \rightarrow NH_4NO_3$

None of the above reactions require elevated temperatures or pressures.

Ammonium fluoride (CAS No. 12125-01-8) has MW = 37.1 and decomposes on heating. It is corrosive to tissue. Ammonium nitrate (CAS No. 6484-52-2) has MW = 80.1 and MP = 169.6°C and decomposes above 210°C, evolving nitrogen oxides. A powerful oxidizer, it may explode under confinement and high temperatures.Uranium oxyfluoride (CAS No. 13536-84-0) has MW = 308.0 and emits toxic F^- fumes when heated to decomposition. Its regulatory limits are measured as uranium.

Table A.3-4 Handbook of Reactive Chemical Hazards

No	CHEMICAL NAME	Hazard Information	Bretherick 3rd e
			Reference page
1	Ammonia	Potentially violent or explosive reactions on contact with nitric acid. A jet of ammonia will ignite in nitric acid vapor (ambient temperature). Incompatable with HF, HNO_3, and UF_6. Emits toxic fumes of NO_2 when heated.	1177
2	Ammonium Hydroxide	Incompatable with HF, HNO_3, and UF_6.	1205
3	Hydrogen Fluoride	Violent reaction with NH_4OH Reacts with steam or water to produce toxic and corrosive fumes	1044
4	Nitric Acid	The common chemical most frequently involved in reactive incidents, reactions do not generally require addition of heat. Ignition on contact with HF. Incompatible with NH_4OH Will react with steam or water to produce heat and toxic and corrosive fumes The oxidising power and hazard potential of HNO_3 increases with concentration.	1100
5	Uranium Hexafluoride	Violent reaction with water.	1078
6	Uranyl Nitrate (UNH)	Decomposes at 100°C	1302
7	Steam		
8	Water		

Notes: 1. MP at 2 atmospheres. Volatile crystals sublime. Triple point - 64.0°C.

Chemical reactions:

1. $UF_6 + UO_2(NO_3)_2.6H_2O$ + water --> $UO_2F_2 + 4HF + UO_2(NO_3)_2.6H_2O$ + heat

   or, in the absence of water, UF_6 could strip some water from UNH, e.g.,.
   $3UF_6 + 2UO_2(NO_3)_2.6H_2O \rightarrow 3UO_2F_2 + 6HF + UO_2(NO_3)_2.3H_2O$
   (Other similar reactions are also possible).

2. $UF_6 + HNO_3$ + water --> $UO_2F_2 + 4HF + HNO_3$ + heat

3. $UF_6 + 2H_2O \rightarrow UO_2F_2 + 4HF$

4. UF_6 + Steam --> $UO_2F_2 + 4HF$

5. $HF + NH_4OH \rightarrow NH_4F + H_2O$

6. $HF + NH_3 \rightarrow NH_4F$

7. $HNO_3 + NH_4OH \rightarrow NH_4NO_3 + H_2O$

8. $HNO_3 + NH_3 \rightarrow NH_4NO_3$

None of the above reactions require elevated temperatures or pressures.

Ammonium fluoride (CAS No. 12125-01-8) has MW = 37.1 and decomposes on heating. It is corrosive to tissue. Ammonium nitrate (CAS No. 6484-52-2) has MW = 80.1 and MP = 169.6°C and decomposes above 210°C, evolving nitrogen oxides. A powerful oxidizer, it may explode under confinement and high temperatures.Uranium oxyfluoride (CAS No. 13536-84-0) has MW = 308.0 and emits toxic F^- fumes when heated to decomposition. Its regulatory limits are measured as uranium.

APPENDIX A.4

THE HIT METHOD

SETUP

Before beginning the HIT method, set up the problem by defining initial conditions. Figuratively, a dotted line is drawn around the operation to indicate explicitly what facilities, components, and functions are being considered.

Frequently, an operation that is normally considered a unit should be divided into several phases. If an operation has several steps, each unique in some way, the various steps might best be analyzed as separate operations. Uniqueness might be found in materials, procedures, or level of personnel involvement.

A step that brings in a new component or a new set of conditions should be analyzed separately. For instance, if a technician sets up a piece of equipment which then functions automatically to do a job, the operation may best be divided into two or more phases. Many maintenance activities clearly involve different equipment, energy, and personnel from normal operations. A storage operation may involve accumulation of larger quantities of materials than are normally present during an operation, Some of the phases that might be considered for separate analysis are setup, normal operation, shutdown, storage, decontamination, and maintenance activities.

Once the functional extent of the operation has been decided, the physical limit should be agreed upon. A physical boundary may be an ESS, a physical barrier, or an administrative line. The boundary may be as small as a reaction vessel or as large as a room. However, it must be defined.

Finally, after the operation has been divided into reasonable and manageable phases and the physical extent of the operation has been delineated, the initial conditions must be set.

PROCEDURE

Step 1: List all components of the operation

Even with relatively small systems, the list quickly becomes long and not readily manageable. A useful tool is to arrange the components into four categories forming fundamental lists of material, equipment, energy, and personnel (Figure A.4-1). The categories accomplish two tasks. First, the categories lend some structure to the list. Second, the categories direct thoughts along specific channels, forcing more completeness. However, categories should be seen as tools, not restrictions. Whether an item is material or equipment is not important. As will be seen in the next step, all categories are treated equally.

Compiling the material and equipment lists is relatively straightforward. Whether an item is equipment or material may not be clear, but in which category an item is placed is not critical. Generally, items that are intended to perform some mechanical functions are equipment, and items that have a critical chemical or physical property would best be listed as materials.

A possible question with the equipment lists regards the degree to which items should be resolved into their constituent parts. Usually, if an item is intended to function as a unit, consider should be named separately. As the analysis proceeds, additional resolution may be necessary. The list may be supplemented at that point.

In the energy category, consider both the energy required as input to operate the equipment or perform the operation, and energy produced within the operation, either intentionally or as a by-product. Some examples of energy types to be included are electrical, thermal, chemical, nuclear, kinetic, and potential.

In the personnel category, the list should include personnel who interact directly with and could be considered part of the operation being analyzed. Personnel who may simply be "in the room" are of interest in evaluating the magnitude of the consequences of an accident, but unless those persons have some sort of effect on the operation, they can be left off the list.

As the material, equipment, energy, and personnel lists are being generated, it is useful to annotate the lists with information that may be pertinent to later analysis. Some useful pieces of information are quantity, physical form (gas, solid, liquid), chemical form, (e.g., oxide nitrate, metal), and material characteristics e.g., flammable, corrosive, acid, caustic).

However, as the analysis proceeds, ask more situation-specific questions about the properties of the items on the lists. For example, if a beaker is being heated, some of the beaker properties one may eventually have to know are:

- Is the beaker heat resistant? To what temperature?
- Will it become brittle at elevated temperatures?
- Is it inspected for embrittlement?

In this fashion, the list will be annotated with information needed to complete the analysis.

Step 2: Form all potential interfaces

Now the list of all potential interfaces between items on the list should be formed. For convenience, these interfaces are divided into ten sets:

- material - material
- material - equipment
- material - energy
- material - personnel
- equipment - equipment
- equipment - energy
- equipment - personnel
- energy - energy
- energy - personnel
- personnel - personnel

To begin, match every item on one list of the set with every item on the other list of the set (Figures A.4-2 and A.4-3). If the pairing is an interface that occurs as a normal part of the operation, add it to the list. If, however, the pairing represents an interface that is not physically possible with the operation being considered, do not add it to the list.

"Not physically possible" means that significant changes from the expected initial conditions must occur for the interface to exist. That is, if an intermediate reaction, or failure of a physical barrier, or sabotage must occur for the interface to exist, the interface is not included on the list. Finally, if the pairing is an interface that is not a part of the normal initial conditions, but physical barriers are not preventing it, the interface and the circumstances should be considered. Generally, the interface should be added to the list, but some judgment should be used here.

A word of caution before proceeding to Step 3: at this stage, the analyst should only be cataloging, not screening. All potential interfaces should be listed, even the intentional and obviously innocuous ones. The next step will eliminate the uninteresting interfaces systematically and, for the most part, fairly quickly. However, if the final analysis is to be complete, it is critical for the initial component and interface lists to be complete.

Step 3: Examine the interfaces

The real analysis begins by examining the first interface. One component of the interface is labeled "active" and the other component is labeled "passive." Ask "Can the active component cause the passive component to change state?" Figure A.4-4 illustrates this assignment of roles and subsequent questions. A change in state is defined for the purpose of this exercise as a change of any physical parameter. These parameters may include material properties such as strength or ductility; physical conditions such as temperature or pressure; chemical state or form; or physical state such as solid, liquid, or gas.

If the answer is no, the active and passive roles should be reversed and the question repeated: "Can the active component cause the passive component to change state?" If the answer is again no, the analysis for this interface is complete. However, if one component can cause a change of state in the other component, the analysis continues with the next question: "Can the change of state lead to new interfaces?" These new interfaces generally result from new interactions or reactions that can take place as a result of the state change. New materials may be formed or materials already present may undergo a change of physical state. If no new interfaces are created, then analysis is complete for that interface. If, however, new interfaces can exist because of the change of state, these new interfaces are listed and analyzed. The new interface list is made by pairing new materials or new physical states of materials with each other and with items on the original material, equipment, energy, and personnel lists, thus creating second-generation interfaces.

If while working through a sequence of interfaces, an initial condition interface (first-generation interface) that had previously been overlooked is noticed, add it to the original list. This interface should then be treated like all other interfaces. When or in what order an interface is considered does not matter, only that all interfaces are considered.

Analysis of second-generation interfaces proceeds just as with the first generation by asking "Can one component cause a change of state in the other component of the interface?" and "Does the change result in new interfaces?" If the interface itself is benign, and the answer to either question is no, the analysis for that interface is complete. If the interface is interesting or if both questions have been answered yes, the analysis proceeds. If one of the components of the interface is an ESS, or if either of the components might be considered a "target" (that is, it has the capacity to sustain damage), the interface is interesting provided that the other component has the capacity to cause damage. How to proceed from here is a function of the purpose of the analysis.

Step 4: Complete the analysis.

The degree of completeness and the extent of the analytical process are based on the objective of the exercise. If the objective is to stimulate the thought process to find potential accidents that are not immediately obvious, then continue the process until thoughts are so stimulated. If, however, HIT is being used as a design tool or to perform a risk analysis, the method should be carried through more thoroughly.

If the method is being used as a design tool, then one is looking for criteria for components of the system and one wants to know the critical control points. If one is using the method as a risk

analysis tool, one wants to find potential accident sequences and weak links in the control of the operation. If one is doing either design or risk analysis, one wants to know the conditions under which controls and ESSs must function. Analysis is continued, keeping in mind the sort of information sought.

Returning to the last decision made in Step 3, if the interface itself is interesting or if it leads to other interfaces, refer to the previous generation interface and ask "Area there controls over the original interface to prevent the second interface from occurring?" The control may be active, such as a thermostat, or it may be passive, as with material properties. The passive controls give the designer material selection criteria.

If an ESS or an endpoint target has not been reached, continue to cycle through generations of interfaces until reaching one of those two unless the sequence fails to produce an interesting consequence.

A good idea is to follow an interface sequence to the end, even when controls are present, because the ultimate consequence of control failure determines the importance of a control or set of controls. We are more interested in control effectiveness and reliability if the event sequence ends in a catastrophic accident than if the sequence has trivial consequences. Thus, the method finds the critical control points and the weak links in the operation.

NOTE: When the original active component is the (H)azard and the final passive component is the (T)arget, with the two being linked by a series of (I)nterfaces, then the reason for the name, the HIT Method, is clear.

EXAMPLE

To illustrate the use of the HIT Method, a simple example is presented. The example is a simplification of an operation performed in chemical research and development facilities at Los Alamos. The number of components involved has been reduced to a small number to allow a full discussion of the example. Even with this simplification, there are a large number of possible combinations of components, which are quickly reduced by the knowledgeable analyst. The knowledge needed is not that of sophisticated systems analysis techniques, but rather that knowledge possessed by the experienced operator/ designer of a system. The knowledge associated with the operation of the system is quickly applied to eliminate from further consideration those interfaces that lead to triviality or are benign in nature.

Consider the example illustrated by Figure A.4-5. The example is used to illustrate the usefulness of the HIT Method as a design tool and as a hazard/safety analysis tool. The contrast in applications of this tool for these two tasks will be clear.

The first effort is to define the boundary conditions and initial conditions of the operation. It is important to do this to limit the scope of subsequent considerations. Because HIT works best and proceeds quickly as a group activity, all participants must be thinking about the same process. By clearly stating the boundary conditions and initial conditions, everyone involved can focus on a finite set of components within a clearly defined physical boundary at an agreed-upon stage within an operation. In the example, define the boundary to be the glove box and its high-efficiency-particulate-air (HEPA) filter placed in the exhaust connection to the building exhaust system. This defines the boundary conditions-a physical enclosure and the items enclosed (Figure A.4-5).

As initial conditions, assume that the person in charge of this operation has set up the operation and has physically left the area of the glove box. Thus, human interactions with the operation

will not be part of our example analysis. (Note that for maintenance, setup, shutdown, and decontamination operations, include the personnel interfaces.)

As the first step, list all of the components within the physical boundary that are present at the start of the operation. This list is divided into four categories for convenience (Figure A.4-6). At this point, two comments should be made. First, it is not important to which category a component is assigned as long as the component appears in one category. If a computer is used to form the interfaces, dividing the list of components into categories is not useful, but rather let the computer form all possible combinations of components. [The appearance of self-interfaces (e.g., Pu-Pu) are of no real concern here.] The categories, however, also aid in forming interfaces.

The second comment is that when making the list of components, use judgment in how detailed the component list should be. Some components may be whole systems. For example, the hot plate includes many internal components that may not be of interest at the moment, but if the details of how the hot plate functions are needed later, a new problem can be defined that includes these internal components. In this example, the power cord is a separate component because it acts as an independent system for the purposes of this analysis.

Now that all of the components are listed, proceed with Step 2, the formation of the interfaces. Figure A.4-7 shows those potential interfaces that satisfy the boundary conditions and the initial conditions. Judgment and experience with the process being analyzed are important here. Many theoretical combinations were eliminated from the interface list because they are not physically possible under the initial conditions, e.g., beaker-glove box. If doubtful as to whether to include an interface, include it. Notice that many interfaces listed are intentional, e.g., Pu-HNO_3. It is as important to consider these interfaces as it is to consider the unintentional interfaces, e.g., hot plate-glove.

To demonstrate this importance, select a few interfaces and follow through with the HIT Method. From the material-material interfaces, refer to Pu-HNO_3. This is an intentional interface, but the quantities of material may be important as seen from later steps in the method. Assign the active role to PU and the passive role to HNO_3. Can the Pu act on the HNO_3 to change its state? The answer is yes because of the chemical reaction:

$$2\,Pu + 6\,HNO_3 = 2[Pu(NO_3)_3] + 3\,H_2$$

Does this change of state cause new interfaces? Yes, hydrogen, which may stay in solution (new ion species in solution) or escape as a gas (gas interfaces), is now present.

The new interfaces associated with the gas are formed by pairing H_2 with all of the components it may come in contact with, such as the beaker, hot plate, power cord, glove box, gloves, and HEPA filter. In addition, H_2-air, H_2-electrical, and H_2-thermal interfaces should be considered. The importance of quantity now becomes apparent. If a sufficient amount of hydrogen is

evolved to form an explosive mixture with air (H_2.air), an interesting interface is created. Likewise, H_2-electrical poses an explosive or fire potential. Now there is an air/hydrogen mixture (a new component). A possible interface is air/hydrogen-electrical. Certainly electrical energy could ignite an explosive mixture of air/hydrogen. Such an explosion would result in a rapid rise of temperature and pressure in the glovebox. These conditions (temperature and pressure) are challenges to the glove box and its gloves' ability to continue providing containment.

The boundary of our problem is now reached in that the last set of interfaces, high-pressure gas-gloves, high-pressure gas-glove box, and high-pressure gas-HEPA filter, have ESSs as their passive components.

Identified along the way was a "new" hazard, hydrogen, not originally on our list of components. As mentioned, the amounts of HNO_3 and H_2 involved are important. If the amounts are not sufficient and the reaction rate is not great enough, an explosive mixture cannot be formed, and the hazard (hydrogen) is controlled by the amounts of materials (Pu, HNO_3). For the purpose of hazard identification and control in design considerations, prepare a list of items that must be considered in starting this operation. Also consider the compatibility of materials with hydrogen; there needs to be an inspection/maintenance program that ensures the electrical insulation integrity of the electrical cord and its connections to the hot plate and the electrical feed through at the glovebox surface.

For the purpose of safety analysis, a different application of this tool, there was identified a sequence of events that can lead to an explosion within the glove box. If the amount of hydrogen formed and the potential concentration is known, one can calculate the explosive forces that would challenge the glove box containment ability. Once these challenges are characterizes, the glove box and its associated systems can be analyzed to see if they provide adequate containment. Once the level of containment is known, an estimate of the amount of Pu that could be released is easily calculated.

Controls were identified that need to be provided to prevent the hazard from proceeding to an accident that damages the target (glove box): quantities of materials, concentration of air/hydrogen mixture, proper electrical insulation, and nonsparking electrical connections. To prevent deterioration, use hydrogen-resistive materials to the extent possible. A new control was identified - some means to exhaust the hydrogen before an explosive mixture can occur.

Now examine an unintentional interface: hot plate-glove. Here the hot plate as the active component supplies thermal energy that could act on the glove causing the glove to melt and to become porous or have a large hole. Already identified is a hazard, hot plate (or thermal energy supplied by the hot plate), and a target that is an ESS, glove. Depending on the ability of the exhaust system to maintain a negative pressure (challenge to an ESS), new interfaces could now exist outside the glove box. Thus, it would be important to ensure that the gloves would not be inadvertently drawn onto the hot plate by a negative pressure or by gravity. Notice that HIT has identified a sequence of events that can lead to a leak in the glove box system. This puts some constraints on the capabilities of the exhaust system to maintain negative pressure and hence inward flow of air.

In the example, the HIT Method identified hazards, their targets, and controls over these hazards much as one would when preparing safe operating procedures, operating requirements, etc. Also demonstrated was how HIT identifies sequences of events that can lead to potential accidents. If the consequences of these accidents warrant the effort, then more formal analysis may be performed by experts as is often done for safety analysis reports.

Again in the safety analysis mode of application, the HIT Method can be used to identify the controls that are critical in preventing a sequence of events from continuing to a set of unacceptable consequences. Once these critical controls are identified, then the more formal systems analysis techniques (fault trees, event trees, cause/consequence, etc.) can be used to provide more quantitative information on the likelihood that these controls will function as intended, given the challenges they face. Remember that the controls may be hardware, procedures, or administrative limits. The HIT Method treats all controls the same. Experience

with HIT shows how much dependency there is upon administrative controls. HIT also identifies the number of levels of control that exist between the hazard and the target.

SUMMARY

The HIT Method is a simple analysis tool that can be used to find hazards and their targets, find potential accidents and their initiating events, and determine design criteria and critical control points. Areas where this sort of information might be useful are in facility or system design, in risk analysis, and in preparation of standard operating procedures.

The HIT Method should be used as a means to obtain an end. It is a very flexible tool that can be modified by the used to fit his needs (the end). Modify the details of the technique using the structure of the fundamental idea to fit the problem to be addressed. HIT is not intended to be a rigid procedure; it is a way of organizing thinking to achieve a systematic identification of hazards and their controls. As the example illustrated, there are different applications of the basic technique resulting in a variety of final products. The technique is simple and flexible, hence powerful.

In the application of the HIT Method, some steps should be performed thoroughly and conscientiously, regardless of the user's needs. Other steps should be modified to fit the situation. The first two steps of the method have to be done thoroughly if the technique is to work at all. The material, equipment, energy, and personnel lists and the first-order interfaces must be complete to define the operation and to stimulate thinking about all aspects of an operation.

However, the interface analysis should be done to the extent needed for the analysis being conducted. When only trying to see if a particular type of accident is possible, stop when that accident is found. When trying to prove that such an accident is not possible, follow every interface through every step.

HIT proceeds quickly and works best in an informal setting. A small group of operating people can easily interact to determine which interfaces lead to "interesting" sequences and outcomes and which interfaces are trivial and should not be followed in great depth.. The value of the group is that interfaces that might be dismissed by one person may appear important to another. Experience shows that if an atmosphere of "what if" play can be created, then the human trait of "one-upmanship" can be a positive contribution. If possible, the group should comprise equals and not be dominated by a single participant.

One potential difficulty with applying the HIT Method is the number of interfaces. Because of the large increase in the number of possible combinations forming potential interfaces as the number of components increases, complex systems should be subdivided into smaller, manageable units. And remember that a large number of interfaces usually are quickly eliminated as uninteresting.

Another suggestion is to avoid becoming bogged down in details. If the point of discussion requires more detail or expertise than is available at the gathering, document the question, refer it to the experts, and come back to it when more information is available. Also, the group should stop their development of a sequence of events when the group reaches the limits of their expertise. For example, if a major fire is possible, but no one in the group has experience with the development and propagation of industrial fires, it is appropriate for the group to document that a fire is possible and would involve estimated amounts of combustible loadings in a well-confined space. Fire protection engineers can then characterize the fire and predict the consequences.

Finally, think creatively and consider all of the possibilities. Be open to, new thoughts and ideas so as to let this method work. Just because an event is not supposed to happen, or has not happened yet, does not mean it cannot or will not. Let your imagination run with unfamiliar ideas. Be prepared to think about an operation in ways not yet considered.

Reference: Hilliard H. Howard and Cheryll L. Faust, "The HIT Method: A Hazard Identification Technique," LA-11507-MS/UC-707, March 1989.

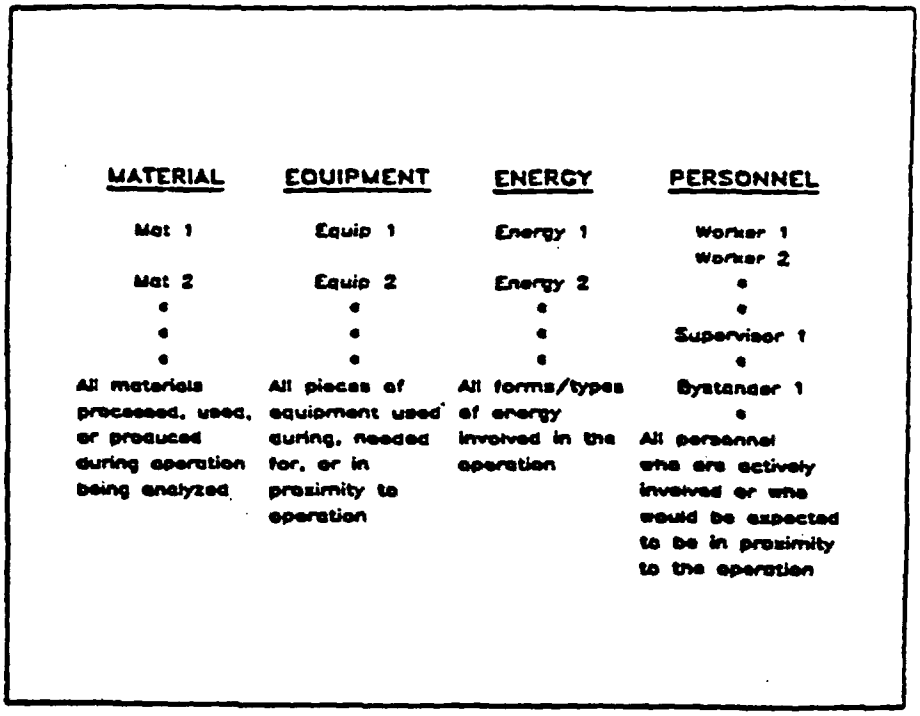


Figure A.4-1. Fundamental lists.

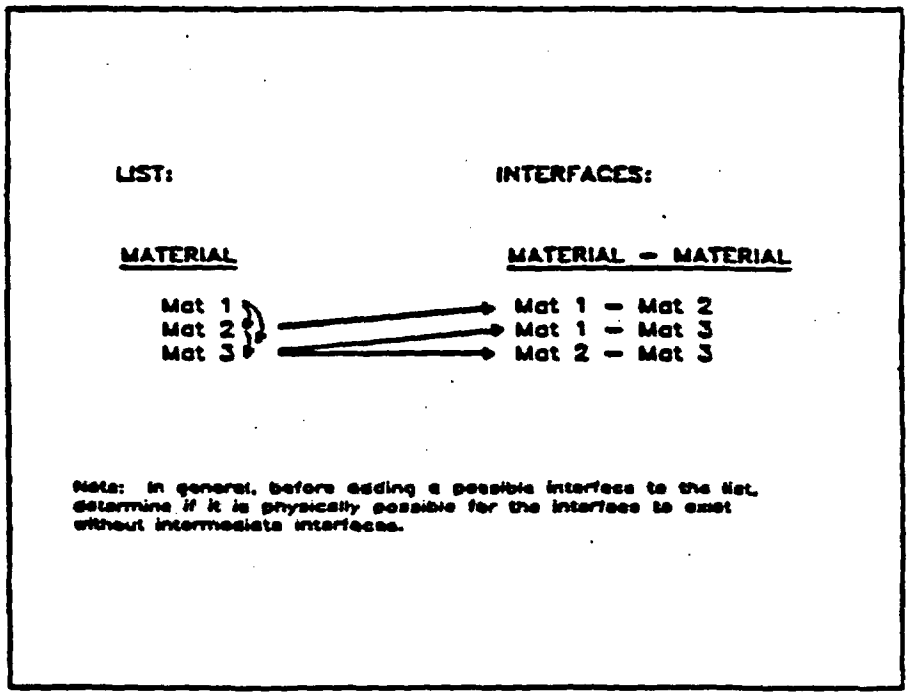


Figure A.4-2. Formation of possible interfaces from within lists.

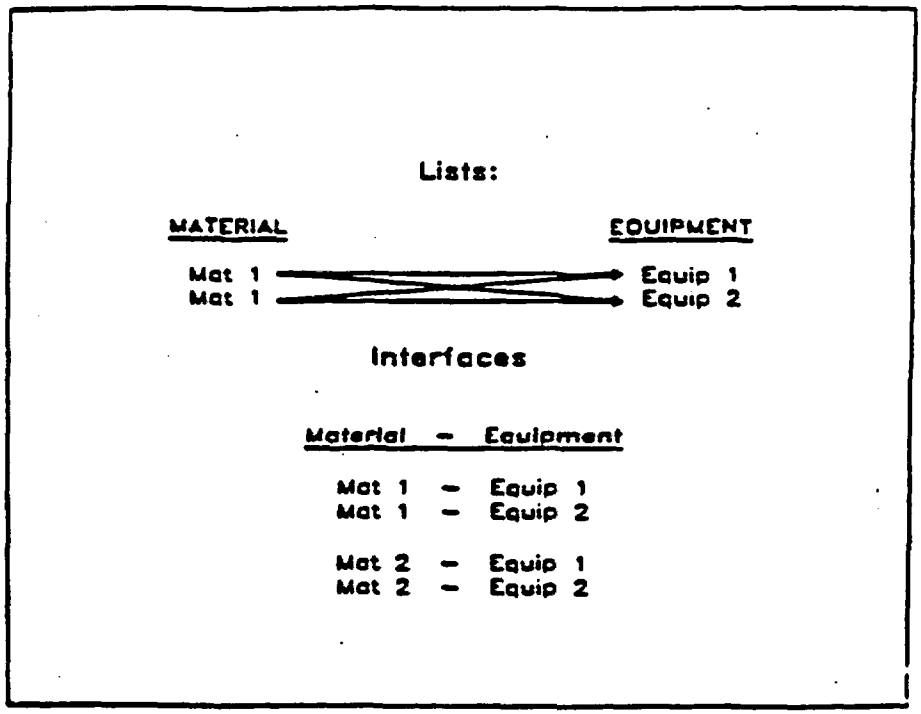


Figure A.4-3. Formation of possible interfaces between lists.

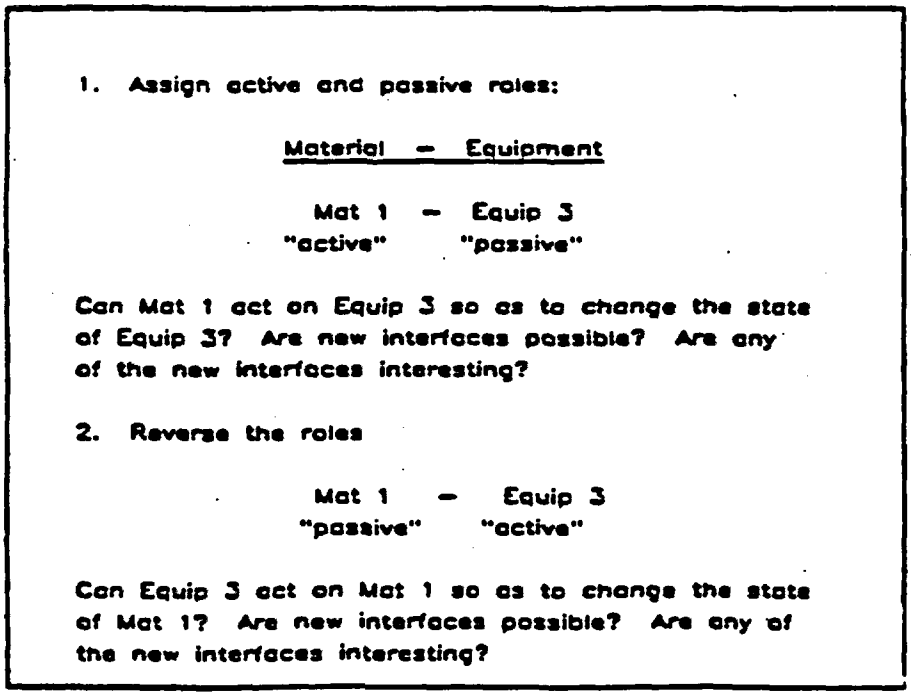


Figure A.4-4. Assignment of roles.

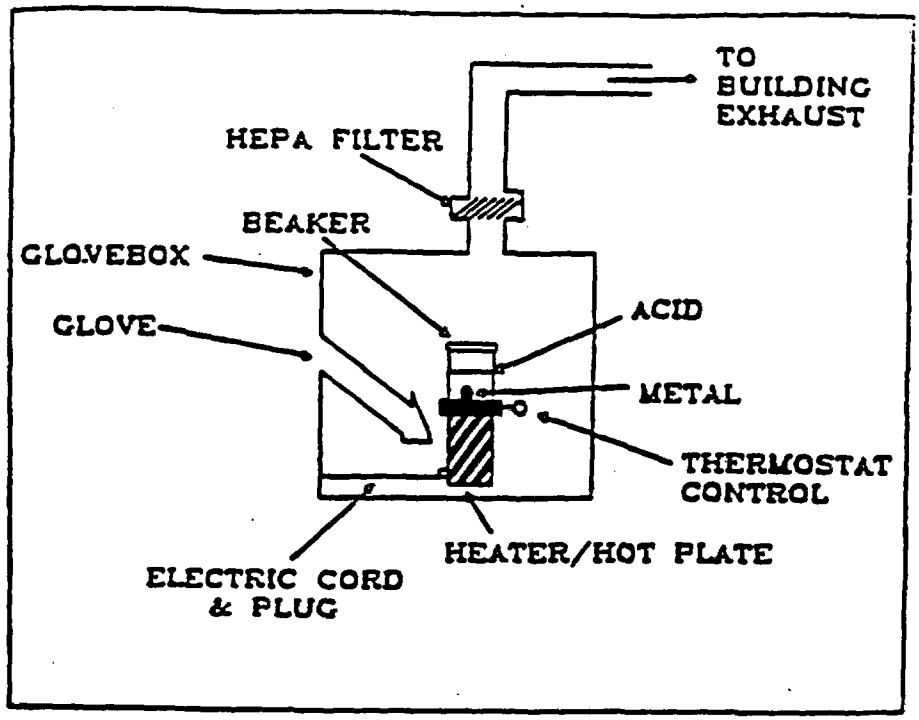


Figure A.4-5. Example operation.

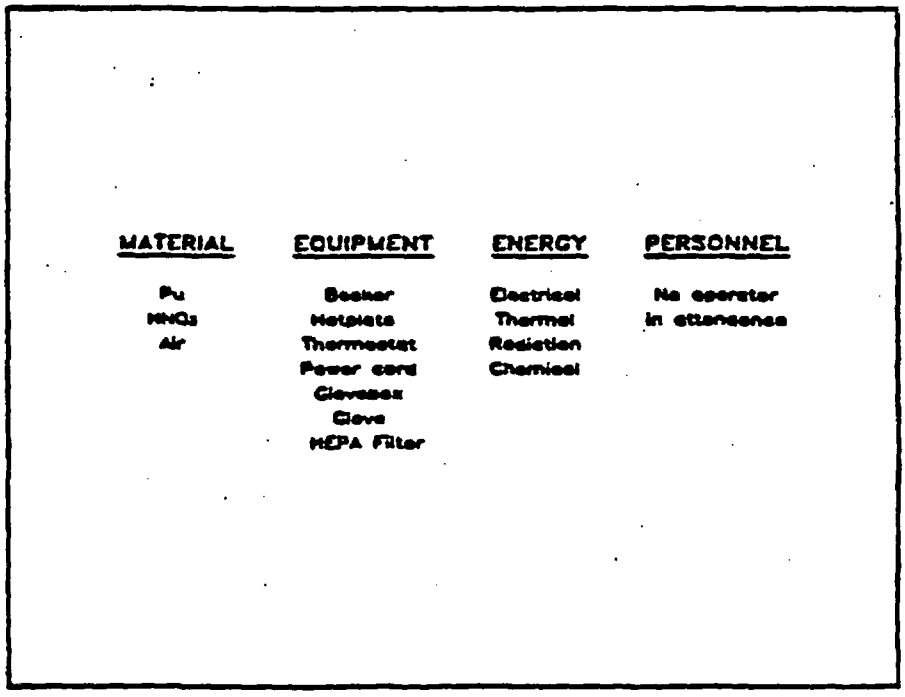
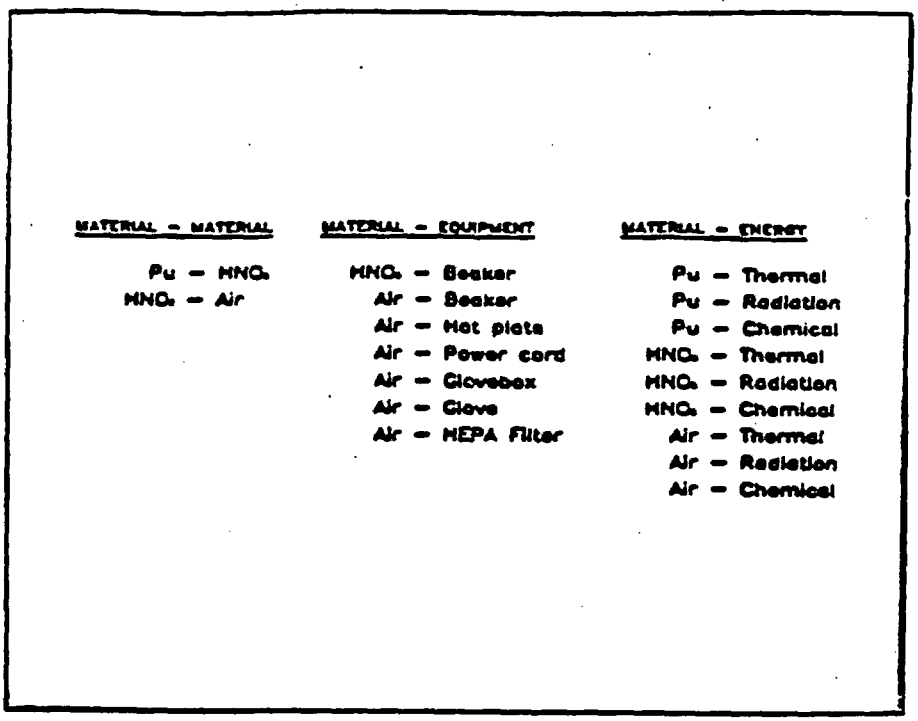
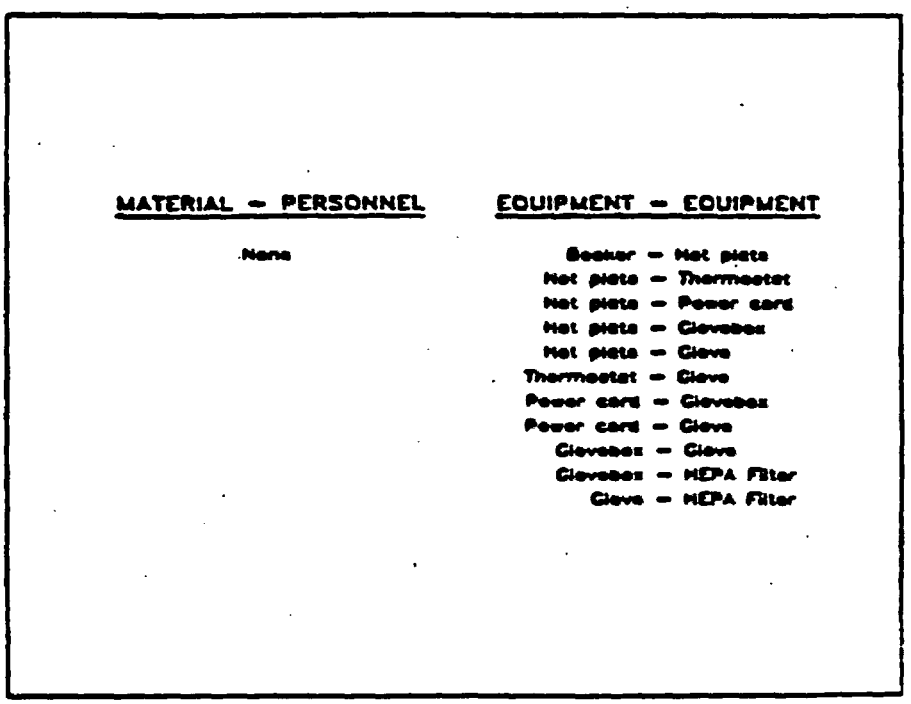


Figure A.4-6. Component list.



MATERIAL – MATERIAL	MATERIAL – EQUIPMENT	MATERIAL – ENERGY
Pu – HNO_3	HNO_3 – Beaker	Pu – Thermal
HNO_3 – Air	Air – Beaker	Pu – Radiation
	Air – Hot plate	Pu – Chemical
	Air – Power cord	HNO_3 – Thermal
	Air – Glovebox	HNO_3 – Radiation
	Air – Glove	HNO_3 – Chemical
	Air – HEPA Filter	Air – Thermal
		Air – Radiation
		Air – Chemical

Figure A.4-7. Interfaces.



MATERIAL – PERSONNEL	EQUIPMENT – EQUIPMENT
None	Beaker – Hot plate
	Hot plate – Thermostat
	Hot plate – Power cord
	Hot plate – Glovebox
	Hot plate – Glove
	Thermostat – Glove
	Power cord – Glovebox
	Power cord – Glove
	Glovebox – Glove
	Glovebox – HEPA Filter
	Glove – HEPA Filter

Figure A.4-7. (cont.)

APPENDIX B.1

ACCIDENT LISTS

Table B.1-1 GENERIC ACCIDENT LIST

DESIGN BASIS ACCIDENTS	1. Fire 2. Explosion 3. Criticality 4. Power Failure
TYPICAL ACCIDENTS	1. Pipe Leaks 2. Breaching of a tank

TABLE B.1-2. SPECIFIC ACCIDENTS LIST

UNIT OPERATIONS	ACCIDENTS/INCIDENTS	
1. Conversion		
1.1 UF6 Receipt, Handling, and Storage	1.1A.1	Overweight Cylinder
	1.1A.2	UF6 Release
	1.1D.1	Fire in Cylinder Storage Area
1.2 Vaporization	1.2A.1	UF6 Leak
	1.2A.2	UF6 Line Pluggage
	1.2D.1	Pluggage of condensate line
	1.2D.2	Vaporizer low or hi steam pressure
	1.2D.3	Vaporizer high condensate level
	1.2D.4	Vaporizer Instrument Failure
	1.2D.5	Vaporizer-to-Hydrolysis-Tower line Plugged
	1.2D.6	Vaporizer Tower Liquid Siphoning into UF6 Feed line
1.3 Hydrolysis	1.3D.1	Tower low water level
	1.3D.2	Tower high uranium concentration
	1.3D.3	Tower high temperature
	1.3D.4	Tower power failure
1.4 Precipitation		
1.5 Centrifuging	1.5D.1	Ammonium nitrate explosion in a filtrate pump during cleanout
1.6 Drying	1.6C.1	Excess Furnace Temperature
	1.6C.2	Air in a Furnace
	1.6C.3	Flame-Curtain Pilot Light Failure
	1.6C.4	Kiln High-Pressure Interlock Fails
	1.6C.5	Furnace T-control fails; High-T setpoint limit exceeded
1.7 Calcining	1.7C.1	Loss of Combustion Air
	1.7C.2	Air in a Calciner
	1.7C.3	High Pressure in a Calciner
1.8 Interim Storage		
1.9 Blending	1.9D.2	A human-error-caused powder spill in a hood

TABLE B.1-2. SPECIFIC ACCIDENTS LIST (Continued)

UNIT OPERATIONS	ACCIDENTS/INCIDENTS	
2. Fabrication		
2.1 UO2 Receipt, Handling, and Storage	2.1D.1	Airborne Activity in Work area
2.2 Powder Preparation and Pelleting		
2.3 Pellet Sintering	2.3C.1	Excess Furnace Temperature
	2.3C.2	Air in a Furnace
	2.3C.3	Failure of Flame-Curtain Pilot
2.4 Pellet Grinding		
2.5 Fuel Rod Loading	2.5D.1	Pellet cart overturned into water
2.6 Inspection and Storage		
2.7 Final Fuel Assembly		
2.8 Storage		
3. Scrap Recovery		
3.1 Cylinder Washing		
3.2 Batch Processing	3.2D.1	Zircalloy fire in plastic bottle
	3.2D.2	Dissolver High Uranyl Nitrate Level
	3.2D.3	Dissolver Batch Boil-Over
	3.2D.4	Level controller failure causes concentrator overflow
	3.2D.5	Detection system fails to detect high U in evap. steam condensate
	3.2D.6	UN Storage Tank High Level
	3.2D.7	UN Bulk Storage Tank Rupture
3.3 Solvent Extraction	3.3B.1	Solvent Spill
3.4 Powder Blending		
3.5 HF Recovery	3.5D.1	HF Reaction with Contaminants
	3.5D.2	HF Storage Tank Overflow/Leak
4. Waste Disposal		
4.1 Conversion Waste	4.1D.1	Safety monitor failure
4.2 Waste-Water Treatment	4.2D.1	Uncontrolled reaction

TABLE B.1-2. SPECIFIC ACCIDENTS LIST (Continued)

UNIT OPERATIONS	ACCIDENTS/INCIDENTS	
4.3 Incineration	4.3C.1	High Incinerator Temperature
	4.3D.1	High Incinerator Pressure
4.4 Calcium Fluoride Disposal		
G. General	GD.1	Interlock bypass switch disables a second interlock
	GD.2	Elevated stack discharge
	GD.3	Fire in controlled area
	GD.4	Valving error causes overheated ("deadheaded") pump
	GD.5	Airborne activity release
	GD.6	Power failure

Key to accident numbering:

- The first set of characters refers to the unit operation. For example, in 2.3C.1, the 2.3 refers to the pellet sintering operation. Alternatively, the letter "G" refers to several operations, but none in particular.
- Next, the letter refers to the hazard as listed in Table A.2. In 2.3C.1, the letter "C" refers to Fire. As can be seen at the top of Table A.2, the letter "D" refers to a nonspecific list of hazards.
- The .1 is only a number in a sequence.

APPENDIX B.2 UF_6 DRY CONVERSION HAZOP

In this example, the HAZOP Method is used to model the hazards in a UF_6 Dry Conversion Process. The process is depicted in Figures B.2-1 and B.2-1. In the process, UF_6 gas is converted to a dry powder. The UF_6 gas arrives in large steel cylinders which are loaded into horizontal vaporizer chest, heated by circulating hot water sprays. The vaporized UF6 and superheated steam are then introduces to a slab shaped disentrainment chamber at the feed end of a conversion kiln. Here they undergo dry hydrolysis to form UO_2F_2 powder and HF gas. The powder falls to the chamber bottom and is continuously removed to the discharge end of the kiln. H_2 gas and superheated steam are fed to the kiln discharge end to strip the fluoride and reduce the powder to UO2. H_2, HF, N_2, and steam are continuously removed from the kiln through process filters. Product powder is continuously removed into a UO_2 check-hopper, which is nitrogen purged.

The first step in the HAZOP process is to apply guide words to process parameters, as illustrated below for "Flow".

Process Section: Nitrogen gas line at vaporizer chest

Design Intention: Pressure testing pigtail

Guide Word: No Process Parameter: Flow

Deviation: No flow

Consequences:	1) Ineffective purging of UF_6 line pigtail
Causes:	1) Low pressure
	2) Valve fails closed
Safeguards:	1) Multiple pressure indicators
	2) Administrative controls

The steps are then repeated for additional parameters and guide words, and the results tabulated in the HAZOP study tables, as follow.

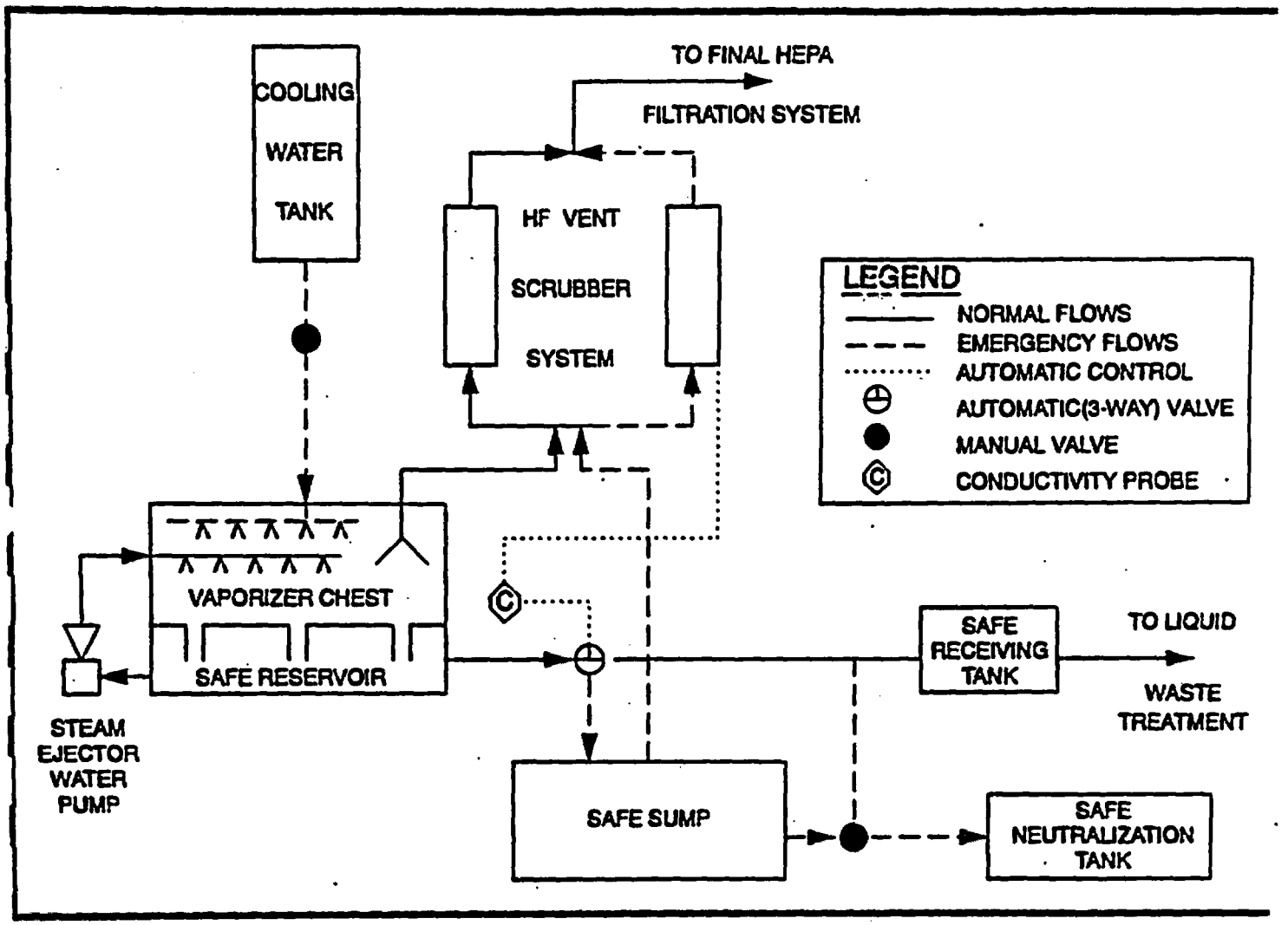


Figure B.2-1
UF_6 Dry Conversion Process

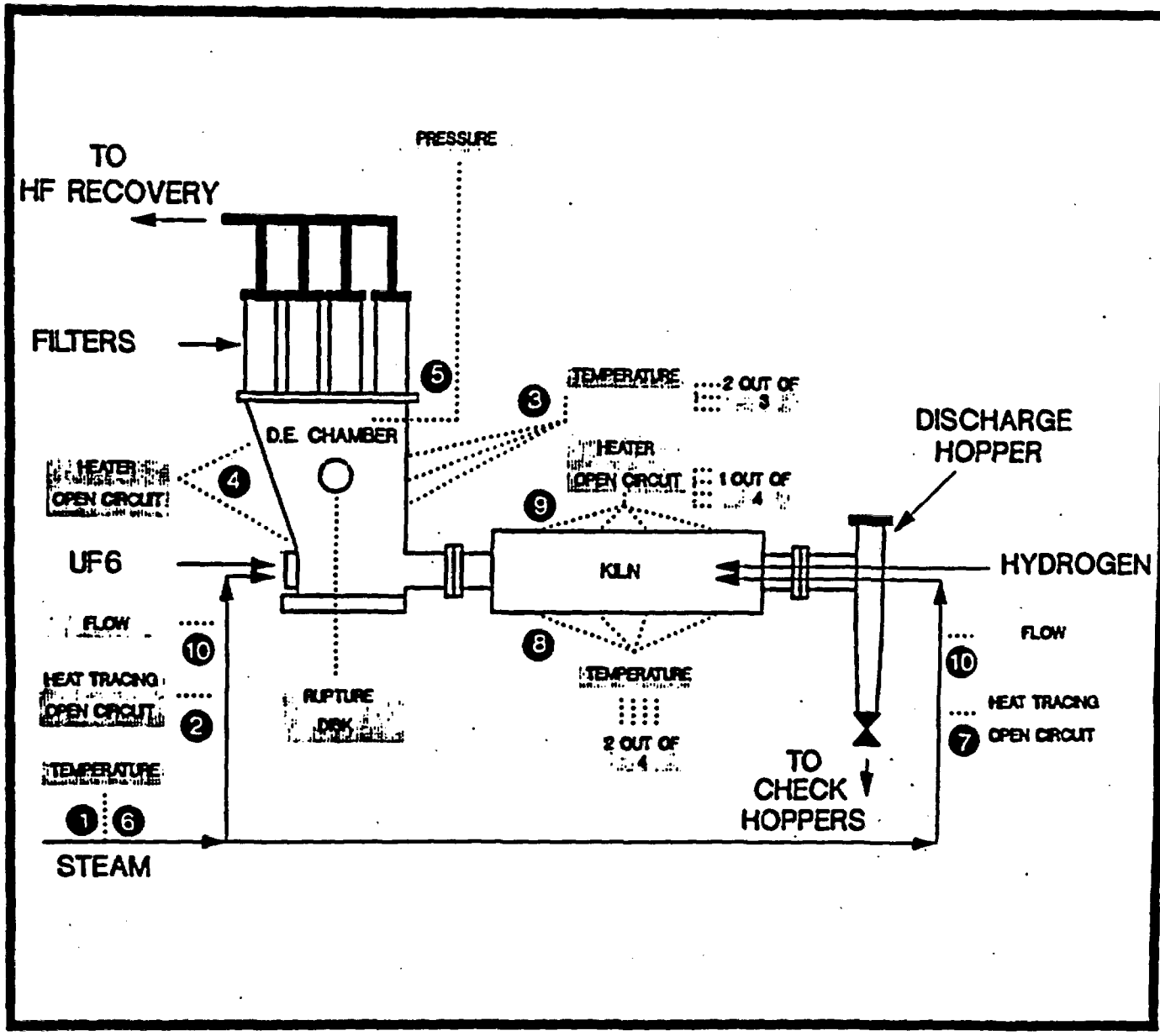


Figure B.2-2
UF_6 Dry Conversion Process

APPENDIX B.2

HAZOP TABLE

FOR

UF_6 DRY CONVERSION

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		1.0 LINE - 120-PSIG NITROGEN GAS (FOR TESTING PIGTAIL CONNECTIONS)					
1.1	High flow	High pressure (Item 1.7)	.	Potential to overwhelm the scrubber, resulting in a potential UO2F2 release in the Bay Area	.....	Pressure regulator Pressure relief valve Multiple pressure indications	
1.2	Low/no flow	Low pressure (Item 1.8) Valve failure (closed)	. .	Potential license violation - ineffective purging of the UF6 line pigtail	.....	Multiple pressure indications Administrative procedures and controls specify to leak check pigtail prior to use Provisions to leak check UF6 cylinder-to-conversion system connections	
1.3	Reverse flow			NCI - No credible cause	.....	Check valve Multiple valves normally closed when nitrogen purge is not in use Flex hose disconnected when nitrogen purge is not in use Operator training	
1.4	Misdirected flow			NCI	.....		
1.5	High temperature			NCI	.....		
1.6	Low temperature			NCI	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				1.0 LINE - 120-PSIG NITROGEN GAS (FOR TESTING PIGTAIL CONNECTIONS) (continued)			
1.7	High pressure	Tank farm nitrogen pressure excursion and nitrogen pressure regulator failure	.	High flow (item 1.1)	.....	Pressure regulator Pressure relief valve Multiple pressure indications	
1.8	Low pressure	Loss of pressure in the nitrogen system Manual valve closed Nitrogen pressure regulator failure (closed)	. . .	Low/no flow (item 1.2)	.....	Multiple pressure indications Operator training	
1.9	High concentration of contaminants			NCI - No credible cause	.....		
1.10	Loss of containment			NCI - Release of nitrogen to the atmosphere NCI - Loss of production	....		
				2.0 LINE - 120-PSIG PLANT STEAM TO VAPORIZER			
2.1	High flow	Steam flow control valve failure (open)	.	High temperature in the vaporizer steam chest (item 5.3)	.....	Vaporizer condensate drain Passive overflow line	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		2.0 LINE - 120-PSIG PLANT STEAM TO VAPORIZER (continued)					
2.2	Low/no flow	Steam flow control valve failure (closed)	.	Low temperature in the vaporizer steam chest (Item 5.4)	.....		
		Manual valve closed	.	Loss of production	.....		
		Low pressure (Item 2.8)	.				
		Plug in line (debris, corrosion)	.				
		Failure of plant steam supply system (boilers, etc.)	.				
2.3	Reverse flow			NCI	.....		
2.4	Misdirected flow			NCI	.....		
2.5	Exposure to high steam temperature	Operator error - no PPE used when working with pigtail steam tracing or hot steam lines	4	Potential for personnel burn injury	3	Line insulation Operator training Heat resistant PPE (gloves, etc.)	
2.6	Low temperature	Loss of steam tracing to the pigtail in the vaporizer	.	NCI - Pigtail plugging, resulting in a loss of production	.....		
		Failure of plant steam supply system (boilers, etc.)	.				
2.7	High pressure	High pressure in the plant steam supply system	1	Potential loss of containment if the pressure exceeds the pressure rating of the line (Item 2.10)	4		
				High pressure in the vaporizer steam chest (Item 5.5)	2		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				2.0 LINE - 120-PSIG PLANT STEAM TO VAPORIZER (continued)			
2.8	Low pressure	Loss of plant steam supply system	.	Low/no flow (Item 2.2)	.....		
2.9	High concentration of contaminants	Contaminated steam supply system	.	HCl - Potential for line plugging or accelerated corrosion	.....	PUT team responsible for plant utilities maintenance	
		Line corrosion	.			Corrosion suppression chemicals added to steam supply	
2.10	Loss of containment	High pressure if the pressure exceeds the pressure rating for the line (Item 2.7)	1	Potential for personnel burn injury	3	Bumper cage around piping	
		Corrosion	1			Periodic visual inspection for leaks performed by operators	
		External impact	2			PUT team responsible for plant utilities maintenance	
		Valve or gasket failure	1			Corrosion suppression chemicals added to steam supply	
		Improper maintenance	1				
		3.0 LINE - 20-PSIG NITROGEN PURGE GAS LINES (UF6 LINE, VALVE HOT BOXES & FILTER BLOWBACK					
3.1	High flow	Valve failure (open)	.	High pressure in the UF6 gas line to the kiln (via valve) (Item 7.7)	.....	Flow orifice in the nitrogen purge to the UF6 line	
		Pressure regulator failure at the pressure reducing station (open)	.	High pressure in the valve hot boxes	.....	Flow indication in the UF6 line	
		High pressure (Item 3.8)	.			High flow alarm in the UF6 line	
						Flow indication at the purge panel	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBD	Safeguards	Actions
		3.0 LINE - 20-PSIG NITROGEN PURGE GAS LINES (UF6 LINE, VALVE HOT BOXES & FILTER BLOWBACK (continued)					
3.2	Low/no flow	Manual valve closed (improper set-up)	2	Loss of production from loss of nitrogen purge	2	Flow indication in the UF6 line	
		Valve failure closed (e.g., UF6 line nitrogen purge	1	Potential for license violation, criticality and safety concerns if nitrogen purge is not available when needed	3	Low flow alarm in the UF6 line Multiple pressure indications Flow indication at the purge panel	
		Line plugging	2				
		Low pressure (Item 3.9)	1				
		Pressure regulator failure (closed)	1				
3.3	Reverse flow	Loss of pressure in the nitrogen system and high pressure in the UF6 supply lines	.	Potential for contamination of the nitrogen system with UF6	.....	Multiple check valves Multiple pressure indications	
3.4	Reverse flow through the 610L valves	Loss of pressure in the nitrogen system with the purge line valves open	.	Potential for contamination of the nitrogen system with UF6	.....	Multiple check valves	
3.5	Misdirected flow (having purge when not needed)			NCI	.....		
3.6	High temperature			NCI	.....		
3.7	Low temperature	Loss of nitrogen line heat tracing	2	NCI - loss of production due to UF6 line plug from cold purge	1	Heat tracing indication and alarm	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETISD	Safeguards	Actions
		3.0 LINE - 20-PSIG NITROGEN PURGE GAS LINES (UF6 LINE, VALVE HOT BOXES & FILTER BLOWBACK (continued)					
3.8	High pressure	Pressure regulator failure (open)	.	High flow (Item 3.1)	.....	Pressure relief valve Pressure regulator Multiple pressure indications	
3.9	Low pressure	Failure of the nitrogen supply system	.	Low/no flow (Item 3.2)	.....	Multiple pressure indications	
3.10	High concentration of contaminants	Loss of nitrogen pressure during D.E. Chamber filter blowback Loss of nitrogen pressure during UF6 line purge	.	Contamination of the nitrogen system with UF6 or kiln off-gases	.....	Multiple check valves TDC pressure indication and low pressure alarm for nitrogen purge	
3.11	Loss of containment			NCI - Loss of production	.....		
		4.0 LINE - EMERGENCY COOLING WATER					
4.1	High flow	Control valve failure (open)	.	High level in the vaporizer steam chest (Item 5.1)	.....	Flow indication (local flow meter) Manual isolation valve remains closed when system not in use	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				4.0 LINE - EMERGENCY COOLING WATER (continued)			
4.2	Low/no flow	Low level in the emergency cooling head tank (item 4.6)	1	Potential license violation - Cooling water not available for emergency cooling when needed	3	Flow indication (local flow meter)	
		Line plugging	1			System for cooling UF6 cylinder	
		Control valve failure (closed)	1	High temperature in the vaporizer steam chest (item 5.3)	2		
		Manual valve closed	1				
		Loss of containment (item 4.12)	1	High pressure in the UF6 cylinder in the VAPORIZER STEAM CHEST (item 5.7)	2		
4.3	Reverse flow			NCI	.....		
4.4	Misdirected flow to the wrong vaporizer	Operator error - valve misalignment	.	Potential criticality concern - failure to cool down correct cylinder	.....	Operator training	
4.5	High level in the emergency cooling head tank	Failure of the high level probe interlock to stop filling cooling water tank	.	NCI - Spill of water through the overflow line into the West trench	.....		
4.6	Low level in the emergency cooling head tank	Failure of the level probe (false high reading)	.	Low/no flow (item 4.2)	.....	Low level alarm	
		Operator error - control valve on the refill water line switched to off mode	.	Potential license violation - Cooling water not available for emergency cooling when needed	.....	System for cooling UF6 cylinder	
4.7	High temperature			NCI	.....		
4.8	Low temperature			NCI	.....		
4.9	High pressure			NCI	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				4.0 LINE - EMERGENCY COOLING WATER (continued)			
4.10	Low pressure			NCI	.....		
4.11	High concentration of rust	Corrosion in water lines and city water supply	.	High concentration of rust and debris in the vaporizer steam chest (Item 5.9)	.....		
4.12	Loss of containment	Corrosion	.	Low/no flow (Item 4.2)	.....	Periodic visual inspection by operators	
		External impact	.				
		Valve or gasket failure	.				
		Improper maintenance	.				
				5.0 VESSEL - VAPORIZER STEAM CHEST			
5.1	High level	Level probe failure	1	Potential criticality concern - Loss of barrier	3	Vaporizer gravity drain	
		Normal condensate drain overwhelmed or plugged and passive overflow line plugged	2	Potential safety concern - Cylinder floating, breaking pigtail	3	Passive overflow line with strainer to prevent line plugging	
		High flow in the emergency cooling water line (Item 4.1)	1			Preventive maintenance on vaporizer	
						Administrative control to check for debris (foreign material) following maintenance and prior to each cylinder installation	
						* (Note: During the HCSE, it was determined that this interlock cannot be regarded as a criticality safety significant interlock for slab thickness.)	
						Operability test of level float at each cylinder installation	
						High level alarm	

(continued)

Item Number	Deviation	Causes	f c	Consequences	FXETIBO	Safeguards	Actions
				5.0 VESSEL - VAPORIZER STEAM CHEST (continued)			
5.7	High pressure in the UF6 cylinder	Low/no flow in the EMERGENCY COOLING WATER (Item 4.2)	.	Potential criticality concern (UO2F2-H2O in the vaporizer) - Damage pigtail and release UF6 to the vaporizer and the atmosphere	.....	High pressure indication and alarm in UF6 gas line to the kiln	
		Heat overfilled cylinder from Oak Ridge	.			Administrative controls to verify net weight of cylinder is less than maximum safe fill limits prior to use	
				High flow in the UF6 gas line to the kiln (Item 7.1)	.....		
5.8	Low pressure in the UF6 cylinder	Empty UF6 cylinder	.	Potential criticality concern - Backflow of moderator into UF6 cylinder (Item 7.3)	.....		
				Low pressure in the UF6 gas line to the kiln (Item 7.8)	.....		
5.9	High concentration of dirt, dust, rust, and debris	High concentration of rust in the emergency cooling water (Item 4.11)	.	HCl - Conductivity false alarm	.....	Conductivity monitor	
				Potential for plugging drain lines	.....	Administrative control to check for debris (foreign material) following maintenance and prior to each cylinder installation	
		Accumulation of dirt, dust, and debris during maintenance	.				
5.10	High concentration of UF6	UF6 cylinder leak or rupture	.	Potential release or personnel exposure to UF6 and/or HF acid	.....	Ventilation scrubber to remove potential UF6 or HF releases and prevent release to the atmosphere	
		Reverse flow in the vaporizer steam chest vent line to S-675 AEB (Item 6.3)	.	Potential criticality concern	.....		
		Low temperature in the vaporizer steam chest, valve hot box, vaporizer safe sump and check hopper vents to S-675 and S-665 AEB (Item 6.6)	.			Detect breach of UF6 containment in vaporizer Conductivity monitor	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		5.0 VESSEL - VAPORIZER STEAM CHEST (continued)					
5.2	Low level			NCI	.....		
5.3	High temperature	High flow in the 120-psig plant steam to vaporizer (raw steam) (Item 2.1)	.	Potential loss of containment if the temperature exceeds the temperature rating of the cylinder vessel (Item 5.11)	.....	High temperature alarm Temperature indication	
		Low/no flow in the emergency cooling water line when needed (Item 4.2)	.				
5.4	Low temperature	Low/no flow in the 120-psig plant steam line to the vaporizer (Item 2.2)	.	Potential loss of production - Form solid UF6 plug in the pigtail; also unable to maintain the cylinder pressure	.....	Temperature indication	
5.5	High pressure in the vaporizer steam chest	Valve in vent line closed	.	Release of steam with the potential for injury to personnel (e.g., burn hazard)	.....	Conservation vent valve on vaporizer vent line (relieves at 7 inches WC pressure)	
		High pressure in the steam supply (Item 2.7)	.	Potential leak (Item 5.11)	.....		
		Low/no flow in the vaporizer steam chest vent line to ! Item 6.2)	.	Potential rupture (Item 5.12)	.....		
5.6	Low pressure in the vaporizer steam chest	Rapid cooling of the steam chest or steam condensation	.	Potential process upset	.....	Conservation vent valve on vaporizer vent line (draws air in at 1 inch WC vacuum)	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBD	Safeguards	Actions
		5.0 VESSEL - VAPORIZER STEAM CHEST (continued)					
5.11	Leak of UF6 cylinder in vaporizer steam chest	High temperature (Item 5.3)	.	Potential criticality concern	.....	Administrative controls for checking for leaks	
		Faulty connections on the cylinder valve	.	Potential release or personnel exposure to UF6 and/or HF acid	.....	Startup checklist	
		High pressure (Item 5.5)	.				
		Cylinder valve leaking	.				
		Corrosion	.				
		External impact	.			Conductivity monitor	
		Valve or gasket failure	.			Ventilation scrubber to remove potential UF6 or HF releases and prevent release to the atmosphere	
		Improper maintenance	.				
5.12	Rupture of UF6 cylinder in vaporizer steam chest	Faulty conections on the cylinder	.	Potential criticality concern	.....	Cylinder recertification every 5 years	
		Cylinder valve leaking	.	Potential release or personnel exposure to UF6 or HF acid	.....		
		Crane failure	.				
		Pigtail failure	.			Ventilation scrubber to remove potential UF6 or HF releases and prevent release to the atmosphere	
		Cylinder failure	.				
		High pressure (Item 5.5)	.				
		Corrosion	.				
		External impact	.			Administrative controls to verify net weight of cylinder is less than maximum safe fill limits prior to use	

(continued)

Item Number	Deviation	Causes	F C	Consequences	EXTERO	Safeguards	Actions
6.0	LINE - VAPORIZER STEAM CHEST, VALVE HOT BOX AND CHECK HOPPER VENTS						
6.1	High flow	Failure of process vent scrubber (pull too much vacuum)	.	Low pressure (Item 6.8)	.....	Scrubber controls and instrumentation	
6.2	Low/no flow	Valve failure (closed)	.	High pressure in the VAPORIZER STEAM CHEST (Item 5.5)	.....	Procedural control to verify vent line and vaporizer "E" valve operations	
		Failure of vaporizer steam chest vent valve (closed)	.	High pressure (no ventilation) in valve hotboxes	.....		
		Too many open maintenance pick ups	.	High pressure in the UO2 CHECK HOPPER, (Item 13.5)	.....		
				Potential to overwhelm from open maintenance pick ups (scrubber actually goes positive)	.....		
6.3	Reverse flow	Water vapor in vent offgasses condenses in contaminated vent line and then condensed liquid drains back into vaporizer steam chest or UO2 check hopper	.	High concentration of UF6 in the VAPORIZER STEAM CHEST (Item 5.10)	.....		
				High concentration of moisture in the UO2 CHECK HOPPER	.....		
		Failure of process vent scrubber fan	.			Conductivity meter in vaporizer steam chest	
						Dew point analyzer in UO2 check hopper	
						Check hopper powder sampled for moisture content	
6.4	Misdirected flow			HCl	.....		
6.5	High temperature			HCl	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		6.0 LINE - VAPORIZER STEAM CHEST, VALVE HOT BOX AND CHECK HOPPER VENTS					
6.6	Low temperature	Low ambient temperature	.	High concentration of UF6 in the VAPORIZER STEAM CHEST (Item 5.10)	.....		
		Water vapor in vent offgasses condenses in contaminated vent line and then condensed liquid drains back into vaporizer steam chest or UO2 check hopper	.	High concentration of moisture in the UO2 CHECK HOPPER	.....		
6.7	High pressure			NCI - Loss of ventilation	.....	Conservation vent valve set at 7 inches WC pressure in vaporizer steam chest vent line	
6.8	Low pressure	High flow (Item 6.1)	.	NCI - Pull too much vacuum	.....	Conservation vent valve set at 1 inch WC vacuum in vaporizer steam chest vent line	
6.9	High concentration of contaminants			NCI	.....		
6.10	Loss of containment			NCI - Loss of ventilation	.....		
		7.0 LINE - UF6 GAS FROM VAPORIZER THROUGH VALVE HOT BOX TO KILN					
7.1	High flow	Flow control valve failure (open)	.	High temperature in the DE chamber (Item 10.3)	.....	Flow indication	
		High pressure in the UF6 cylinder (Item 5.7)	.	Potential for unreacted UF6 in the kiln off-gas line (Item 14.9)	.....	High flow alarm	
		Excessive nitrogen purge flow	.	High pressure in the DE CHAMBER (Item 10.5)	.....	Flow orifice that helps prevent high flow	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		7.0 LINE - UF6 GAS FROM VAPORIZER THROUGH VALVE HOT BOX TO KILN (continued)					
7.2	Low/no flow	Closed manual valve	.	MCI - Loss of production	.....	Flow indication	
		Flow control valve failure (closed)	.			Low flow alarm	
						Line heat tracing	
		Low temperature causing UF6 to solidify and plug line (Item 7.6)	.				
		Low pressure (Item 7.8)	.				
		High concentration of scale plugging the line (Item 7.9)	.				
7.3	Reverse flow	Low pressure in the UF6 cylinder (Item 5.8)	.	Criticality concern - Backflow of moderator into UF6 cylinder	.....		
7.4	Misdirected flow to the wrong kiln			MCI	.....		
7.5	High temperature	Failure of heat tracing (runaway temperature)	1	Potential loss of containment if the temperature is high enough to melt teflon gaskets (Item 7.10)	3	Multiple temperature indications	
				High pressure (Item 7.7)	2		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		7.0 LINE - UF6 GAS FROM VAPORIZER THROUGH VALVE HOT BOX TO KILN (continued)					
7.6	Low temperature	Failure of heat tracing (no temperature)	1	UF6 line pluggage, causing low/no flow (item 7.2)	2	Low temperature alarms Multiple temperature indications	
				Potential for UF6 contamination during maintenance	3	Line heat tracing	
				Potential license violation - Failure to detect loss of heat tracing during operation	3	Line insulation	
7.7	High pressure	High flow in the 20-PSIG NITROGEN PURGE GAS LINES (UF6 LINE, VALVE HOT BOXES & FILTER BLOWBACK (item 3.1)	.	Potential loss of containment if pressure is high enough to excede pressure rating of line or instrumentation (item 7.10)	.....	Multiple pressure indications	
		High temperature (item 7.5)	.				
		Undesirable reaction of UF6 with contaminants introduced into line	.				
7.8	Low pressure	Low pressure in the UF6 cylinder (item 5.8)	.	Low/no flow (item 7.2)	.....		
						Multiple pressure indications	
						Low pressure alarm	
7.9	High concentration of scale	UF6 coating the line and forming scale	.	Flow transmitter or flow control valve plugging, causing low/no flow (item 7.2)	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		7.0 LINE - UF6 GAS FROM VAPORIZER THROUGH VALVE MOT BOX TO KILN (continued)					
7.10	Leak	High temperature if the temperature is high enough to melt teflon gasket (Item 7.5)	1	Small release of UF6 - Airborn contamination 3		QC testing of jet to verify integrity	
		Valve or gasket failure	4			Containment area at the kiln	
		External impact	3			Containment area in the bay	
		Pigtail failure	1			Leak check of the UF6 line as required by maintenance	
		Cylinder rotating in vaporizer steam chest, causing the pigtail to rupture	1			Operator surveillance during production	
		Instrumentation failure	4			Emergency shutdown procedures	
		Jet failure at the kiln (installation, misalignment or thumper rate too high)	4			Remote cylinder valve shut-off	
		Corrosion	1				
		Improper maintenance	4				
		High pressure (Item 7.7)	1				

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBD	Safeguards	Actions
		7.0 LINE - UF6 GAS FROM VAPORIZER THROUGH VALVE MOT BOX TO KILN (continued)					
7.11	Rupture	Valve or gasket failure	2	Uncontrolable release of UF6, resulting in NRC notification and potential production shutdown for investigation	4	Operator surveillance during production	
		Crane failure	2			QC testing of jet to verify integrity	
		External impact	2	Potential for personnel injury	3	Containment area at the kiln	
		Pigtail failure	1			Containment area in the bay	
		Cylinder rotating in steam chest, causing the pigtail to rupture	1			Leak check of the UF6 line as required by maintenance	
		Instrumentation failure	2			Emergency shutdown procedures	
		Jet failure at the kiln (installation, misalignment or thumper rate too high)	3			Remote cylinder valve shut-off	
		Corrosion	1				
		Improper maintenance	1				
		Pressure generated from heating solid UF6 plug in line and expansion to gaseous state	1				

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETISO	Safeguards	Actions
		8.0 LINE_X - 9-PSIG SUPERHEATED STEAM FOR D.E. CHAMBER AND KILN BARREL					
8.1	High flow to the jet	Flow control valve failure (open)	.	Product quality concern	.....	Flow indication	
				High pressure in the DE chamber (Item 10.5)	.....	High flow alarm	
8.2	Low/no flow to the jet	Closed manual valve	.	Potential for contamination of process vent scrubber system (S-655) with UF6 if no steam for reaction	.....	Flow indication	
		Steam trap failure	.			Low flow alarm	
		Low pressure (Item 8.11)	.	Potential license violation	.....		
		Flow control valve failure (closed)	.				
		Three way valve (6103) failure - misdirect steam to calibration condenser	.				
		Misdirected flow of steam from the jet to the UF6 line (Item 8.6)	.				
8.3	High flow to the discharge of the kiln	Flow control valve failure	.	High pressure in the KILN BARREL (Item 11.5)	.....	Flow indication	
				Potential product quality concern	.....	High flow alarm	
8.4	Low/no flow to the discharge of the kiln	Low pressure (Item 8.11)	.	Potential license violation	.....	Flow indication	
		Closed manual valve	.			Low flow alarm	
		Steam trap failure	.				
		Misdirected flow from the steam at the discharge of the kiln to the check hopper (Item 8.7)	.				

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		8.0 LINE_X - 9-PSIG SUPERHEATED STEAM FOR D.E. CHAMBER AND KILN BARREL (continued)					
8.5	Reverse flow			NCI - No credible cause	.....		
8.6	Misdirected flow of steam from the jet to the UF6 line	Loss of flow (lower pressure) in the UF6 line than in the DE chamber	.	Low/no flow to the jet - plugging at the jet due to moisture reacting with UF6 gas (Item 8.2)	.....		
8.7	Misdirected flow from the steam at the discharge of the kiln to the check hopper	Loss of check hopper nitrogen purge	.	Loss of barrier - Steam flowing into check hopper	.....		
		Low pressure (lower than in the discharge hopper and kiln) in the UO2 check hopper (Item 13.6)	.	High concentration of moisture in the check hopper UO2 powder	.....		
				Low/no flow to the discharge of the kiln (Item 8.4)	.....		
8.8	High temperature			NCI	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBD	Safeguards	Actions
		8.0 LINE_X - 9-PSIG SUPERHEATED STEAM FOR D.E. CHAMBER AND KILN BARREL (continued)					
8.9	Low temperature	Steam superheater failure Heat tracing failure (no temperature)	. .	Potential criticality concern - Steam condensing in the DE chamber or kiln barrel	.....	Temperature indication Low temperature alarm Overtemp interlock on the steam superheater Line heat tracing Line insulation	
8.10	High pressure	Pressure regulator failure (open)	2	High pressure in the DE chamber (Item 10.5) High pressure in the kiln barrel (Item 11.5)	.....2 2	Relief valve Redundant pressure regulators Pressure indication High pressure alarm	
8.11	Low pressure	Pressure regulator failure (closed) Valve failure (closed)	. .	Low/no flow to the jet (Item 8.2) Low/no flow to the discharge of the kiln (Item 8.4)	....	Redundant pressure regulators Pressure indication Low pressure alarm	
8.12	High concentration of contaminants			MCI - Potential for powder quality concerns if steam supply is contaminated	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBD	Safeguards	Actions
		8.0 LINE_X - 9-PSIG SUPERHEATED STEAM FOR D.E. CHAMBER AND KILN BARREL (continued)					
8.13	Loss of containment	Corrosion External impact Valve or gasket failure Improper maintenance	. . . .	Release of steam with the potential for injury to personnel (i.e., burn hazard)	.....	Periodic visual inspection by operators	
		9.0 LINE - 3.5-PSIG HYDROGEN GAS TO KILN					
9.1	High flow	Pressure regulator failure (open) Tank farm process upset	. .	MCI - Excess hydrogen in kiln off-gases	.....	Flow indication High flow alarm Emergency hydrogen cut-off switch Flow control valve	
9.2	Low/no flow	Manual valve closed Hydrogen flow control valve failure (closed) High level in the kiln discharge hopper, blocking the flow of hydrogen (Item 12.1) Orifice pluggage	2 1 1 1	MCI - Loss of production and powder quality concerns Potential criticality concern - No N2 or N2 flow through line during production could result in a process upset (pressure imbalance) in the discharge hopper, allowing steam to flow to the check hopper (Item 9.8)	.....2 3	Flow indication Low flow alarm Emergency hydrogen cut-off switch Automatic nitrogen purge when hydrogen flow is stopped Flow control valve	
9.3	Reverse flow	Loss of pressure in the nitrogen purge line with the purge line valves open	.	Potential to contaminate the nitrogen purge line with kiln atmosphere	.....	Manual check to verify nitrogen purge is flowing	

(continued)

Item Number	Deviation	Causes	f c	Consequences	FXETIBO	Safeguards	Actions
		9.0 LINE - 3.5-PSIG HYDROGEN GAS TO KILN (continued)					
9.4	Misdirected flow to the process vent scrubber	Operator error - valve misalignment	•	Potential for an explosive mixture (hydrogen and air) forming at the scrubber	.....	Process interlock that helps to prevent the valve to the scrubber from opening unintentionally	
		Valve failure (open)	•				
9.5	High temperature			HCl	.....		
9.6	Low temperature			HCl	.....		
9.7	High pressure	Pressure regulator failure (open)	•	High pressure in the kiln barrel (Item 11.5)	.....	High pressure alarm Pressure indication Redundant pressure regulators Flow orifice	
9.8	Low pressure	Tank farm upset (loss of hydrogen supply)	•	Potential criticality concern	.....	Pressure indication Low pressure alarm Redundant pressure regulators	
		Pressure regulator failure (closed)	•				
		Valve failure (closed)	•				
		Low/no flow (Item 9.2)	•				
9.9	High concentration of air	Leak into the hydrogen line around valves or flanges during low pressure	•	Potential for an explosive mixture (hydrogen and air) forming	.....	Vendor Air Products QA/QC program Periodic line inspections	
		Contamination from vendor	•				

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				9.0 LINE - 3.5-PSIG HYDROGEN GAS TO KILN (continued)			
9.10	Loss of containment	Corrosion	1	Release of hydrogen with the potential for an explosion	5	Hydrogen analyzer on kiln barrel seals	
		External impact	1			Portable hydrogen analyzer used to periodically check for leaks	
		Valve or gasket failure	1				
		Improper maintenance	1				
						Bumper guard on hydrogen line and mercoid-type shut-off sensors	
				10.0 VESSEL - DE CHAMBER			
10.1	High level	Scroll failure	.	Potential criticality concern - High moisture content in the UO2F2	.....	Operator surveillance of kiln bearings	
		Low temperature - causing excessive steam condensation (Item 10.4)	.	High level in the kiln barrel (Item 11.1)	.....	Scroll design	
		Bearing failure	.				
		Pressure greater than 50-psig, causing steam condensation (Item 10.5)	.				
10.2	Low level			HCl - Loss of production	.....		
10.3	High temperature	High flow in the UF6 gas line to the kiln, increasing exothermic reaction rate (Item 7.1)	.	HCl - Product quality concern	.....	Multiple temperature indications	
						Multiple high temperature alarms	

(continued)

Item Number	Deviation	Causes	FC	Consequences	FXETIBO	Safeguards	Actions
			10.0	VESSEL - DE CHAMBER (continued)			
10.4	Low temperature	Failure of heat tracing	2	High level (Item 10.1)	3	Multiple heat tracing circuits	
		Thermocouple failure	2	High concentration of unreacted UF6 in the kiln off-gas line (Item 14.9)	3	Multiple temperature indications and alarms	
		Cold carbon filters (loss of filter heat tracing)	3			Kiln insulation	
		Loss of electric power	3			Backup power system	
		Low pressure (Item 10.6)	2				
10.5	High pressure	High flow in the 9-psig superheated steam line to the jet at the D.E. chamber (Item 8.1)	1	High level (Item 10.1)	3	Pressure indication (PI 610N) and high pressure alarm	
				Potential airborn release of UF6, UO2F2, HF or H2	3	Operator training	
		Operator error - valve misalignment	2	High pressure in the KILN BARREL (Item 11.5)	3		
		Low/no flow in the kiln off-gas line (Item 14.2)	2	Potential criticality concern (pressure exceeds 50 psig) - Water vapor condensing, resulting in a high concentration of moisture (Item 10.7)	3		
		High pressure in the 9-psig superheated steam line (Item 8.10)	2				
		Plugged carbon filters	2				
		High flow in the UF6 gas from vaporizer through valve hot box to kiln (Item 7.1)	1				

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
			10.0	VESSEL - DE CHAMBER (continued)			
10.6	Low pressure	Pulling too much vacuum from the blower Seal failure	.	Ingress of air, potentially resulting in an explosive mixture forming (hydrogen and air)	.....	Pressure indication and low pressure alarm Low pressure alarm on the kiln seals	
				Potential criticality concern - pulling kiln atmosphere through PT , resulting in a high concentration of moisture in the check hopper	.....	Pressure indication on the kiln seals Scrubber controls and instrumentation	
				Ingress of water vapor from the air, resulting in high concentration of water (item 10.7)	.....		
				Low temperature (item 10.4)	.....		
				Low pressure in the KILN BARREL (item 11.6)	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				10.0 VESSEL - DE CHAMBER (continued)			
10.7	High concentration of water/HF	Water/HF vapor condensing due to low temperature (Item 10.4)	.	Potential criticality concern	.....	Prevent moderator condensation in DE Chamber	
				Accelerated corrosion	.....		
		Water vapor being drawn in from the air due to low pressure (Item 10.6)	.			Pressure indication and low pressure alarm on DE Chamber seals	
		Improper maintenance (e.g., nuts and bolts not tightened properly)	.			Controls to prevent low temperature and high pressure	
		Failure of DE Chamber heater or heat tracing	.				
		Reverse flow in the KILN OFF-GAS THROUGH CARBON AND BACKUP FILTERS TO HF CONDENSER (Item 14.3)	.				
		High pressure (Item 10.5)	.				
10.8	Loss of containment	External impact	3	Potential release of UF6, UO2F2, HF or N2	3	Kiln is leak checked following maintenance	
		Improper maintenance	2			Pressure indications	
		Seal failure	3			Operator surveillance of purge panel (checked twice per shift)	
		Barrel cracking	2			Operator surveillance of kiln during operation	
		Corrosion	2			Pressure indication and low pressure alarm on the kiln seals	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBD	Safeguards	Actions
				11.0 VESSEL - KILN BARREL			
11.1	High level	High level in the DE CHAMBER (Item 10.1) High level in the kiln discharge hopper (discharge hopper pluggage) (Item 12.1) Pressure greater than 50-psig, causing moisture condensation (Item 11.5) Slow/no rotation (low angular velocity) (Item 11.8) Low temperature - causing excessive steam condensation (Item 11.4) Bearing failure	. . . . . .	Potential criticality concern - High moisture content in the UO2F2	.....	Operator surveillance of check hopper weight for powder flowing to the check hopper Operator has the capability to calculate differential pressure between kiln and check hopper Operator surveillance of kiln bearings	
11.2	Low level			NCI - Loss of production	.....		
11.3	High temperature			NCI - Product quality concern	.....	Multiple temperature indications Multiple high temperature alarms	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
			11.0	VESSEL - KILN BARREL (continued)			
11.4	Low temperature	Failure of heaters Thermocouple failure Loss of electric power Failure of heat tracing Low pressure (Item 11.6)	. . . . .	High level (Item 11.1) Potential criticality concern - water vapor condensing, resulting in a high concentration of water (Item 11.9)	....	Multiple temperature indications and low temperature alarms Backup power system Prevent moderator condensation Insulation Heat tracing	
11.5	High pressure	High pressure in the 9-psig superheated steam line to the D.E. chamber and the kiln (Item 8.10) Operator error - valve misalignment High pressure in the 22-psig hydrogen gas line to the kiln (Item 9.7) High pressure in the DE CHAMBER (Item 10.5) High flow to the discharge of the kiln in the 9-psig superheated steam for D.E. chamber and kiln barrel (Item 8.3)	. . . . .	Potential airborn release of UF6, UO2F2, HF or H2 High level (Item 11.1) Higher pressure in the KILN DISCHARGE HOPPER, than in the check hopper (Item 12.5)	....	Pressure indication in the DE chamber Operator training Prevent moderator condensation in the kiln	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				11.0 VESSEL - KILN BARREL (continued)			
11.6	Low pressure	Pulling too much vacuum from the blower	.	Ingress of air, potentially resulting in an explosive mixture forming (hydrogen and air)	.....	Pressure indication in the DE chamber	
		Seal failure	.			Low pressure alarm on the kiln seals	
		Low pressure in the DE CHAMBER (Item 10.6)	.	Ingress of water vapor from the air, resulting in a high concentration of water (Item 11.9)	.....	Pressure indication on the kiln seals	
				Low temperature (Item 11.4)	.....		
11.7	Fast rotation (high angular velocity)			HCl - Product quality concern	.....		
11.8	Slow/no rotation	Driver failure	.	High level (Item 11.1)	.....	Operator surveillance of drive during production	
		Bearing failure	.			Operators periodically grease bearings	
11.9	High concentration of water/HF	Operator error - valve misalignment	.	Potential criticality concern	.....	Valve lockout procedure	
				Accelerated corrosion	.....	Prevent moderator condensation in kiln	
		Improper maintenance (e.g., nuts and bolts not tightened properly)	.	High concentration of contaminants in the KILN DISCHARGE HOPPER, (Item 12.7)	.....	Pressure indication and low pressure alarm on kiln seals	
		Water vapor being drawn in from the air due to low pressure (Item 11.6)	.			Controls to prevent low temperature and high pressure	
		Low temperature (Item 11.4)	.				

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				11.0 VESSEL - KILN BARREL (continued)			
11.10	Loss of containment	Corrosion	2	Potential release of UF6, UO2F2, HF or H2	3	Kiln barrel is leak checked following maintenance	
		External impact	3			Operator surveillance of purge panel (checked twice per shift)	
		Improper maintenance	2			Operator surveillance of kiln during operation (form CF101-003)	
		Seal failure	3			Periodic UT testing of kiln barrel	
		Barrel cracking	2			Pressure indication and low pressure alarm on kiln seals	
				12.0 VESSEL - KILN DISCHARGE HOPPER			
12.1	High level	Plug in the line from the discharge hopper to the check hopper	.	High level in the kiln barrel (item 11.1)	.....	Operator has the capability to calculate differential pressure between the DE Chamber and the check hopper	
		. valve failure (closed)	.	Previous license violation	.....		
		High level in the UO2 check hopper (item 13.1)	.	Potential criticality concern due to cooling effect of powder	.....	Nitrogen blowback to clear plugs as needed	
				Low/no flow in the 3.5-psig hydrogen gas line to the kiln (item 9.2)	.....	Operator surveillance of sampling by the auto sampler during operation	
				Loss of product (UO2) flow to the auto sampler	.....		
12.2	Low level			NCI	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
				12.0 VESSEL - KILN DISCHARGE HOPPER			
12.3	High temperature			HCl - Product quality concern	.....		
12.4	Low temperature	Failure of heat tracing	.	Potential criticality concern - Condensation of water vapor	.....	Temperature indication and TDC alarm Spare set of heat tracing	
12.5	Higher pressure in the discharge hopper (kiln) than in the check hopper	High pressure in the KILN BARREL (Item 11.5)	4	Potential criticality concern - Contamination of the check hopper with kiln atmosphere, including moisture	3	Operator has the capability to calculate differential pressure between the DE Chamber and the check hopper	
		Spike in the hydrogen pressure	2				
		High sampler purge	2				
		Loss of check hopper nitrogen purge	1				
12.6	Lower pressure in discharge hopper than in the kiln	Leak at the sample cup	.	Potential criticality concern - Contamination of the discharge hopper with kiln atmosphere, including moisture	.....	Heat tracing of the discharge hopper will help prevent condensation Indication that sample cup is properly mated to system	
		Loss of nitrogen purge at the check hopper	.				
				Potential for hydrogen or steam (moisture) accumulation in the discharge hopper or the check hopper	.....		
12.7	High concentration of contaminants	High concentration of contaminants in the KILN BARREL (Item 11.9)	.	Potential criticality concern	.....	Process controls of kiln	
				Accelerated corrosion	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		12.0 VESSEL - KILN DISCHARGE HOPPER (continued)					
12.8	Loss of containment	Corrosion	1	Release of UO2 and hydrogen with the potential for personnel exposure and explosion	3	Leak testing following maintenance	
		External impact	2			Periodic visual inspection by operators	
		Valve or gasket failure (gasket or nye)	2				
		Improper maintenance (e.g., improper weld)	1				
		Leaks around powder sampling system	2				
		13.0 VESSEL - UO2 CHECK HOPPER					
13.1	High level	Check hopper outlet valve failure (closed)	.	High level in the kiln discharge hopper (item 12.1)	.....	Weight indication and high weight alarm	
		Plugging in the check hopper outlet line	.			Interlock to prevent valves from opening at the same time	
		Check hopper inlet valve failure (opens to a full check hopper)	.				
13.2	Low level			NCI	.....		
13.3	High temperature	Loss of nitrogen purge	.	Potential for powder burnback if an oxygen atmosphere (air) exists	.....		
13.4	Low temperature			NCI	.....		

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		14.0 LINE - KILN OFF-GAS THROUGH CARBON AND BACKUP FILTERS TO HF CONDENSER					
14.1	High flow	Excessive nitrogen purge	.	Potential for contaminating the scrubber sump tanks with HF acid	.....	Procedure specify startup sequence	
		Operator error during startup allowing excessive steam flow	.				
		Blower overspeeding	.	Potential to overload the condenser and/or scrubber	.....		
14.2	Low/no flow	Scrubber failure	.	High pressure in the DE chamber (Item 10.5)	.....	Differential pressure indication across the backup filters	
		Carbon filter plugging (e.g., failure of nitrgen blowback, loss of air to solenoid)	.			High differential pressure alarm across the backup filters	
		Venturi plugging	.			Differential pressure indication across the carbon filters	
		Backup filter plugging	.			High differential pressure alarm across the carbon filters	
		Condenser (chiller) failure	.			Automatic filter blowback sequence	
		Manual valve closed	.			Automatic nitrogen purge for kiln feed streams via nitrogen purge panel	
						Filter heat tracing	
						Multiple carbon filters	
						Pressure indication and high pressure alarm in the DE Chamber	
						Water purge to prevent venturi plugging at the scrubber	

(continued)

Item Number	Deviation	Causes	F C	Consequences	FXETIBO	Safeguards	Actions
		14.0 LINE - KILN OFF-GAS THROUGH CARBON AND BACKUP FILTERS TO MF CONDENSER (continued)					
14.3	Reverse flow	Improper maintenance causing backflow of city water, condenser solution, and/or scrubber solution through the vent line to the DE Chamber	.	Potential criticality concern - High concentration of water in the DE CHAMBER (item 10.7)	.....	Maintenance lockout procedure specifies to isolate condenser	
14.4	Misdirected flow through the bypass line to the backup filter at the other kiln	Operator error - valve misalignment	.	RCI - Potential for overloading the backup filter at the other kiln	.....	Operator training	
		Valve seat leakage	.				
14.5	High temperature	Condenser (chiller) failure (i.e., loss of condensing)	.	High pressure (item 14.7)	.....	Multiple temperature indications	
		Failure of heat tracing in the filters (runaway temperature)	.			Condenser can handle failure of heat tracing in the filters	
		High glycol temperature in the chiller	.			Periodic maintenance/service of chiller by outside vendor, McQuay	
						Periodic monitoring of chiller temperature by operators	
14.6	Low temperature	Failure of heat tracing on the filters (no temperature)	2	Potential for MF acid and steam condensation in the vent line	3	Multiple low temperature alarms	
						Multiple temperature indications	
14.7	High pressure	High temperature (item 14.5)	.	No additional safety concerns noted. See high pressure in the kiln and DE chamber	.....		
14.8	Low pressure			No additional safety concerns noted. See low pressure in the kiln and DE chamber	.....		

(continued)

Item Number	Deviation	Causes	f c	Consequences	FXETIBO	Safeguards	Actions
14.0 LINE - KILN OFF-GAS THROUGH CARBON AND BACKUP FILTERS TO HF CONDENSER (continued)							
14.9	High concentration of unreacted UF6	High flow in the UF6 gas line to the kiln (item 7.1)	.	Contamination of the scrubber or condenser system with UF6	.....	Interlock to prevent UF6 flow if feed steam is not on	
		Low temperature in the DE chamber (no steam for UF6 reaction) (item 10.4)	.				
14.10	High concentration of UO2F2	Breakthrough of the carbon filters	.	Contamination of the scrubber or condenser system with UO2F2	.....	Backup filters	
				High uranium level in the Q tanks	.....		
14.11	Loss of containment	Corrosion	.	Airborn release of UF6, HF and hydrogen gas with the potential for personnel exposure and an explosion	.....	Teflon coating inside vent line	
		External impact	.			Periodic visual inspection of line by operators	
		Valve or gasket failure	.				
		Improper maintenance	.	Loss of ventilation of the kiln	.....	Heat tracing of filters kept in operation continuously to help prevent thermal cycling	
		Thermal cycling - causing loose fittings for leaks	.				

APPENDIX B.3 UNH BULK STORAGE HAZOP

In this example, the HAZOP Method is used to model the hazards in a UNH storage area, shown in Figure B.3-1. Uranyl Nitrate solution is stored in bulk before processing in ADU conversion operations. The vessels are large capacity cylindrical stainless steel tanks in a 2 by 3 array outside the process building. The tanks are supplied with multiple safety features such as on-line analysis units with readouts and alarms, continuous recirculating system, electrical heat tracing, and temperature indicators. Tank design includes a cone shaped bottom for solids collection.

The first step in the HAZOP process is to apply guide words to process parameters, as illustrated below for "Level".

Process Section: UNH Storage Tank

Design Intention: Safely store bulk UNH solution

Guide Word: Low Process Parameter: Level

Deviation: Low level in tank

Consequences:
1) Pump explosion

Causes:
1) Operator error, pump runs after tank emptied
2) Operator error, no indication from receivers that flow has stopped

Safeguards:
1) Low level interlock
2) Pressure indicator in recirculation line
3) Low flow alarm
4) Administrative control to check pressure in recirculating line

The steps are then repeated for additional parameters and guide words, and the results tabulated in the HAZOP study tables, as follow.

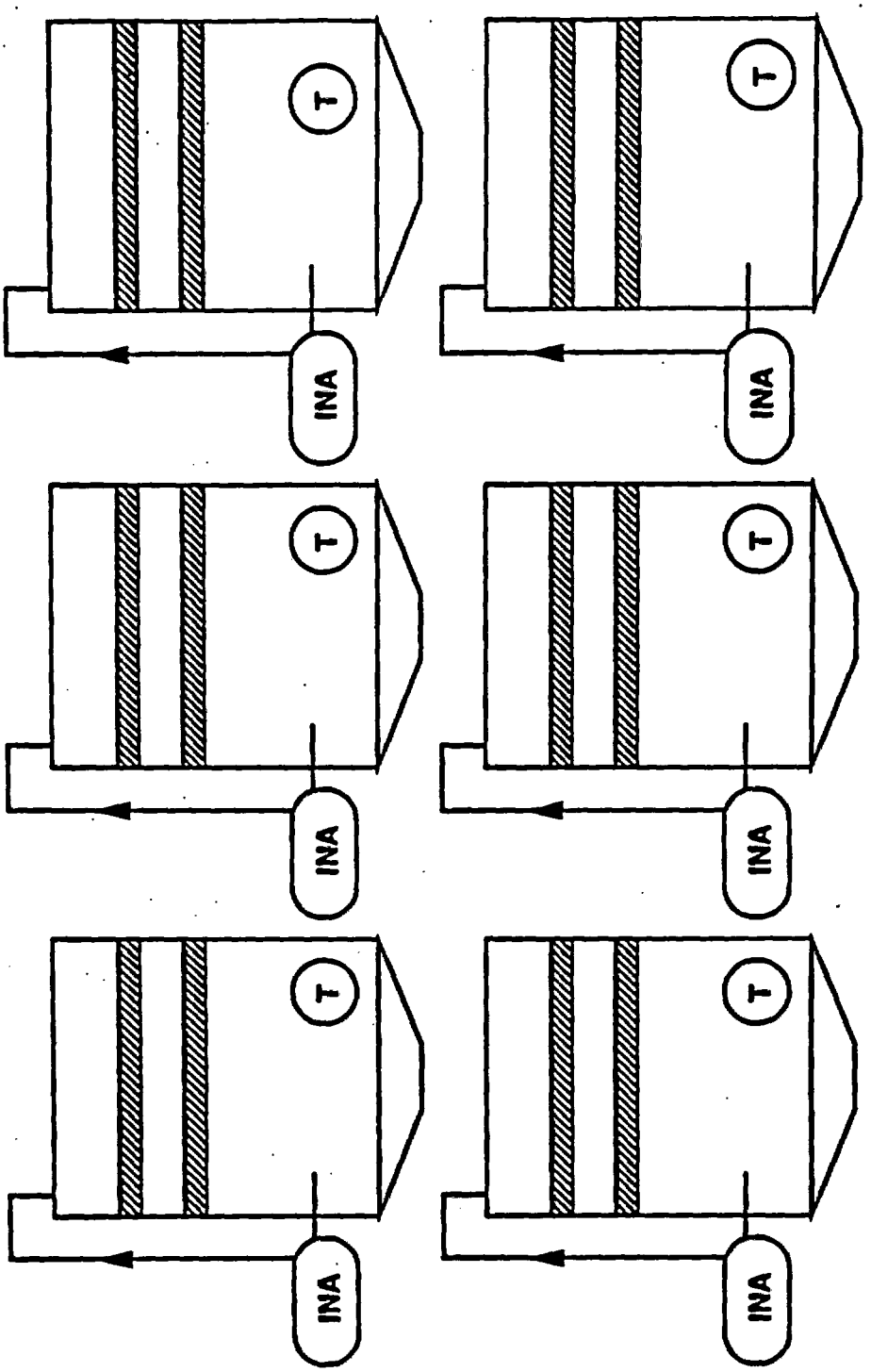


Figure B.3-1
UNH Storage Area

APPENDIX B.3

HAZOP TABLE

FOR

URANYL NITRATE BULK STORAGE

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
		1.0 VESSEL - TANK TRUCK			
1.1	High level	Supplier overfilled tank truck	High pressure (Item 1.5)	Supplier requirements and operating criteria	
1.2	Low level		No Consequence of Interest (NCI)-flag something is wrong with delivery shipment	Invoice check	
1.3	High temperature	Vehicle accident (wreck)	High pressure (Item 1.5)	Traffic control requirements	
		External fire	Criticality concern-concentrate UO2	Trucks are escorted by security or operations	
				On-site Emergency Brigade	
				Diked truck unloading area	
				Insulated tank truck	
1.4	Low temperature	Cold winter/small volume of UO2 in tank truck	NCI-unlikely to freeze truck contents and concentrate solution	Insulated tank truck	
				Tank truck fill requirements: external temperature must be greater than freezing point of solution	
1.5	High pressure	High level (Item 1.1)	Loss of containment-leak or rupture of tank truck (Item 1.8)		
		High temperature (Item 1.3)			
		Inadvertent pressurization of tank truck using 90 psi plant air when filling storage tank			
1.6	Low pressure	Unwanted pump-out of empty tank truck	Loss of containment-collapse tank (Item 1.8)		
1.7	High concentration of contaminants	Operator error-confuse UO2 and HF storage tanks when filling	Contamination and corrosion of supplier truck	Operator present during truck-to-tank transfer	
1.8	Loss of containment	High pressure (Item 1.5)	Criticality concern-fissile material into an unfavorable geometry container	On-site Emergency Brigade	
		Low pressure (Item 1.6)	Contamination of ground, equipment, etc.	Spill control procedures	
		Vehicle accident (wreck)			
		Forklift accident			
		Corrosion of supplier truck			

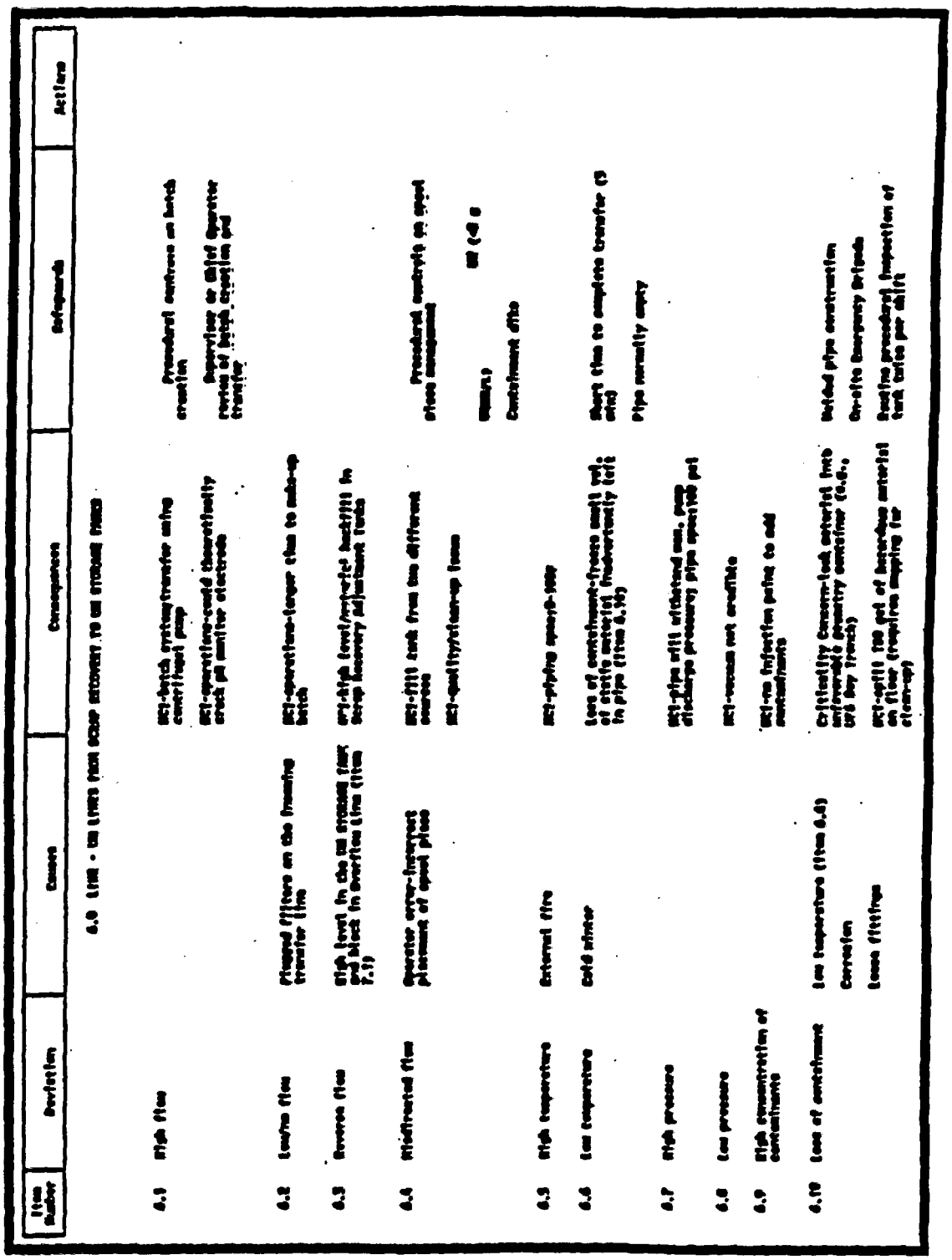
Item Number	Deviation	Causes	Consequences	Safeguards	Actions
			1.0 VESSEL - TANK TRUCK (continued)		
1.9	Emptying	Operator error-non representative sample of tank truck contents	Transfer off-spec HH	Vendor sample results	
			2.0 LINE - TANK TRUCK UNLOADING LINE TO HH TANKS		
2.1	High flow		HCl		
2.2	Low/no flow		HCl		
2.3	Reverse flow		HCl		
2.4	Misdirected flow	Operator error-supervisor wrong valve(s)	High level in the HH STORAGE TANK-plumbing aligns for diversion to any tank and could fill wrong tank (Item 7.1) HCl-potential spill of HH in tank containment pad	Containment dike	
2.5	High temperature	External fire	HCl-piping spec'd-1000		
2.6	Low temperature	Cold winter	Loss of containment-freeze small vol. of static material inadvertently left in pipe (Item 2.10)	Pipe normally empty	
2.7	High pressure		HCl-cannot generate pressures exceeding pipe spec 100 psi		
2.8	Low pressure		HCl-vacuum not credible.		
2.9	High concentration of contaminants		HCl-no injection point to add contaminants		
2.10	Loss of containment	Truck driver driving off while still attached Low temperature (Item 2.6)	Criticality concern-leak material into an unfavorable geometry container (storm drain) Contamination of ground, equipment, etc.	Spill control procedures Wheel chocks Sign in front of truck Place caution tape around truck	

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
		2.0 LINE - TANK TRUCK UNLOADING LINE TO 8D TANKS (continued)			
				On-site Emergency Brigade Operator present during truck-to-tank transfer Containment dike	
		3.0 LINE - TANK TRUCK UNLOADING LINE TO 8D TANKS			
3.1	High flow		HCl		
3.2	Low/no flow		HCl		
3.3	Reverse flow		HCl		
3.4	Misdirected flow	Operator error-open/close wrong valve(s)	High level in the 8D STORAGE TANK-plumbing allows for diversion to any tank and could fill wrong tank (item 7.1) HCl-potential spill of 8D in tank containment pad	Containment dike	
3.5	High temperature	External fire	HCl-piping above 0-300F		
3.6	Low temperature	Cold winter	Loss of containment-freeze small vol. of static material inadvertently left in pipe (item 3.10)	Pipe normally empty	
3.7	High pressure		HCl-cannot generate pressures exceeding pipe spec 100 psi		
3.8	Low pressure		HCl-[illegible] not credible		
3.9	High concentration of contaminants		HCl-no injection point to add contaminants		
3.10	Loss of containment	Truck driver driving off while still attached	Criticality concern-leak material into an unfavorable geometry container (storm drain)	Spill control procedures Weld checks	

Item Number	Deviation	Cause	Consequence	Safeguards	Actions
		3.0 LINE - TANK TRUCK UNLOADING LINE TO HW TANKS			
		Low temperature (Item 3.6)	Contamination of ground, equipment, etc.	Sign in front of truck Place caution tape around truck Operator present during truck-to-tank transfer On-site Emergency Brigade Containment dike	
		4.0 LINE P - HW TRANSFER LINE THROUGH PUMP TO THE HP UPTAKE STATION			
4.1	High flow		HCl		
4.2	Low/no flow		HCl		
4.3	Reverse flow		HCl		
4.4	Misdirected flow	Operator error-Instail wrong spool piece	HCl-potential spill of HW in tank containment pad	Procedural controls on spool piece management Containment dike	
4.5	High temperature	External fire	HCl-piping spec'd-1000°		
4.6	Low temperature	Cold winter	Loss of containment-freeze small vol. of static material inadvertently left in pipe (Item 4.10)	Pipe normally empty	
4.7	High pressure		HCl-normal generate pressures exceeding pipe spec: 100 psi		
4.8	Low pressure		HCl-vacuum not credible		
4.9	High concentration of contaminants		HCl-no injection point to add contaminants		
4.10	Loss of containment	Low temperature (Item 4.6)	Criticality concern-fish material into an unfavorable geometry container (steam drain)	Spill control procedures Visual checks	

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
			4.0 LINE_P - UR TRANSFER LINE FROM PUMP TO THE UF SPIKING STATION (continued)		
		Truck driver driving off site still attached	Criticality concern-pump located in unfavorable geometry catch basin Contamination of ground, equipment, etc.	Sign in front of truck Place caution tape around truck On-site Emergency Brigade Operator present during truck-to-tank transfer Containment dike	
			5.0 LINE - UR TRANSFER LINE TO UF SPIKING		
5.1	High flow		UCI		
5.2	Low/no flow		UCI		
5.3	Reverse flow		UCI		
5.4	Misdirected flow		UCI-only one direction flow is possible		
5.5	High temperature	External fire	UCI-piping spec=0-300F		
5.6	Low temperature	Cold winter	Loss of containment-freeze could rupture pipe spec 100 psi	Pipe normally empty	
5.7	High pressure		UCI-cannot generate pressures exceeding pipe spec 100 psi		
5.8	Low pressure		UCI-vacuum not credible		
5.9	High concentration of contaminants		UCI-no injection point to add contaminants		
5.10	Loss of containment	Low temperature (Item 5.6)	Criticality concern-leak material into an unfavorable geometry container Contamination of ground, equipment, etc.	Spill control procedures On-site Emergency Brigade Containment dike	

HAZOP TABLE (CONTINUED)



Item Number	Deviation	Causes	Consequences	Safeguards	Actions
6.0 LINE - ON LINES FROM SCRAP RECOVERY TO 6H STORAGE TANKS					
6.1	High flow		HCl-batch contamination due to premature transfer	Procedural controls on batch transfer	
			HCl-operations-could theoretically crack pH monitor electrode	Supervisor or shift operator review of batch operation and transfer	
6.2	Reverse flow	Flapped flippers on the incoming transfer line	HCl-operations-longer than to make-up batch		
6.3	Reverse flow	High level in the 6H storage tank and block in overflow line (Item 2.1)	HCl-high level/overfill backfills in scrap recovery pit/effluent tanks		
6.4	Misdirected flow	Operator error-incorrect placement of spool pieces	HCl-fills tank from the different sources	Procedural controls on spool piece management	
			HCl-contamination from [illegible]	[illegible]	
				Containment dike	
6.5	High temperature	External fire	HCl-piping upset-leak		
6.6	Low temperature	Cold winter	Loss of containment-freeze until rpt; of entire material inadvertently left in pipe (Item 6.10)	Short time to complete transfer (3 min)	
				Pipe normally empty	
6.7	High pressure		HCl-pipe refill unrestricted max. pump discharge pressure; pipe rupture pit		
6.8	Low pressure		HCl-vacuum not credible		
6.9	High concentration of constituents		HCl-no injection point to add constituents		
6.10	Loss of containment	Low temperature (Item 6.6)	Criticality Concern-leak material into unfavorable geometry container (e.g., 6H day tranks)	Bolted pipe construction	
		Corrosion		On-site Emergency Brigade	
		Loose fittings	HCl-refill the pit of hazardous material on floor (requires mopping for cleanup)	Routine procedural inspection of tank farm per shift	

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
		6.0 LINE - HB LINES FROM SCRAP RECOVERY TO HB STORAGE TANKS (continued)			
			Contamination of ground, equipment, etc.	Containment dike Batch process	
		7.0 VESSEL - HB STORAGE TANK			
7.1	High level	Misdirected flow in the TANK TRUCK UNLOADING LINE TO HB TANKS (Item 2.4)	Reverse flow in the HB LINES FROM SCRAP RECOVERY TO HB STORAGE TANKS (Item 6.3)	Low concentration of HB (<5 g HB3F/L)	
		Misdirected flow in the TANK TRUCK UNLOADING LINE TO HB TANKS (Item 3.4)	Contamination of ground-tank HB3F potentially could spill into the valve station, outside of main containment dike	Procedural controls specifying authorized transfers to and from HB tanks Level indicator	
		Low/no flow in the OVERFLOW LINE FROM HB TANKS TO OVERFLOW TANK (Item 10.2)	High level in the OVERFLOW TANK (Item 11.1)	High level alarm	
		Level indication failure	HCl-potential spill of HB in tank containment pad	Independent high high level alarm Containment dike	
		Operator error-transfer material into full tank			
7.2	Low level	Operator error-leave pump on while tank is empty	Pump explosion (if run pump dry for extended period of time)	Procedure-check pressure in recirc line when start pump	
		Poor communications-no phone call from area receiving HB to inform of no flow		Local pressure indicators in recirc line Remote low flow alarm in ASU control room	
				Remote on/off indicator for recirc pump in ASU control room	
				Low level interlock to shut off pump in automatic mode	
				Phone communications between SRTC and ASU	
7.3	High agitation	Instill wrong speed agitator motor	HCl-splashing/turbulence effects may interfere with level indication	Timed, low rpm agitator motor	
			HCl-equipment damage to agitatory no risk to integrity of tank		
7.4	Low agitation	Loss of power	Criticality concern-settling of precipitated U in tank		

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
			7.0 VESSEL - HLW STORAGE TANK (continued)		
		Equipment damage to agitator			
				"LC" Two operating pumps monitors per tank on recirc line	
				"LS" Deinventation of tank contents	
				Weekly sampling of tank contents-viscosity impact clarity of sample	
				Routine procedural inspection of tank twice per shift	
				"LC" Emergency power for key components	
7.6	High temperature	Vehicle accident-spill flammable material near trunk unloading facility	Criticality concern-concentrate HLW solution	On-site emergency brigade	
			High pressure (Item 7.7)	Slow evaporation rate of HLW	
		External fire		"LC" Procedure-check HLW temperature twice per shift	
				Containment dike	
7.8	Low temperature	Cold climate	Criticality concern-concentrate HLW solution	"LS" Heat tracing on recirc line	
			Loss of containment-freeze tank contents-concentrate HLW solution (Item 7.10)	"LC" Two operating pumps monitors per tank on recirc line	
				"LS" Deinventation of tank contents	
				Steam lance to heat outside unit of tank	
				Procedure-turn on heat at specified temperature	
				"LS" Capability to dump tank	
				"LC" Procedure-check HLW temperature twice per shift	
				Containment dike	
7.9	High pressure	High temperature (Item 7.5)	Act-loss of containment-potential spill of HLW to tank containment pad (Item 7.10)	2 tank vent line	

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
		7.8 VESSEL - UO2 STORAGE TANK (continued)			
				Unsealed entrances into tank around instrumentation (agitator, level transducer)	
				Containment dike	
7.8	Low pressure	Unwanted pump out of tank contents	HCl-vacuum not credible	2 inch vent line	
				Unsealed entrances into tank around instrumentation (agitator, level transducer)	
				Containment dike	
7.9	High concentration of contaminants	Operator error-add caustic DI water (water wash)	Criticality concern-precipitation of U under caustic conditions	"LC" Supervisor verification to ensure proper tank wash	
		Operator error-inadvertent addition of caustic to tank	Corrosion from NF	"LC" Supervisor verification of drummed material transfers ...	
		High fluoride concentration in feed material	Criticality concern-concentrate UO2	"LC" Procedural controls to not add DI water directly to UO2 tanks for dilution	
		High solvent concentration from SOLEX	Gamma alarms activated; solution dumped to pad at 10 g U235/L	"LC" Top operating gamma chalters per tank on recirc line	
		Drummed material added to adjustment tanks		Gamma and pH monitors on Scrap Recovery Adjustment tanks	
		Tank truck supplier delivers UO2 > 5 g U235/L		"LC" Procedural controls authorizing transfers to and from the UO2 tanks	
				Routine procedural inspection of tank tanks per shift	
				All additions to UO2 tanks are covered by PIP	
				Containment dike	
7.10	Loss of containment	Low temperature (Item 7.6)	High level in the SUMP (Item 12.1)	Routine procedural inspection of tank twice per shift	
		High pressure (Item 7.7)	HCl-potential spill of UO2 in tank containment pad	Material of construction-SS	
		Corrosion		On-site Emergency Brigade	
		Spill control procedures		Containment dike	

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
8.0 LINE_P - RECIRCULATION LINE FOR UH STORAGE TANKS					
8.1	High flow		HC1-no effect on gamma monitors; increases tank mixing		
8.2	Low/no flow	Pump failure	Criticality concern-loss safeguards/gamma monitor and tank recirculation	Alarm-no flow	
		Operator error-incorrectly throttles manual valve		On-line spare pump	
		Loss of electric power	Criticality concern-increased potential for U precipitation	"LC" Emergency power for key components	
		Debris-plug line or pump	Pump explosion	"LC" Heat tracing on recirc line	
		Loss of containment-major leak in recirc line (item 8.10)		Procedure-check pressure in recirc line when start pump	
		Low temperature-freeze line (item 8.6)		Local pressure indicators in recirc line	
		Deadhead pump		Remote low flow alarm in ADU control room	
				Remote on/off indicator for recirc pump in ADU control room	
				Low level interlock to shut off pump in automatic mode	
				Flame arrestor/valve between UH18 and ADU	
				Spare parts-two extra pumps	
				Routine procedural inspection of tank twice per shift	
8.3	Reverse flow		HC1-spin impeller off pump;operator would know immediately		
8.4	Misdirected flow	Operator error	HC1-inadvertent transfer of UH in line up to blind flange	"LC" Procedural controls on spool piece management	
				Normally closed valves	
8.5	High temperature	Deadhead pump	Loss of containment-pump explosion (item 8.10)	Procedure-check temperature sensing strips on pumps	
		External fire	HC1-piping upset-ADU	Routine procedural inspection of tank twice per shift	

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
		8.0 LINE_P - RECIRCULATION LINE FOR 8H STORAGE TANKS (continued)			
				Phone communications between 8H09 and AB9	
				Spare parts-two extra pumps	
				Routine procedural inspection of tank twice per shift	
		9.0 LINE - DISCHARGE LINE FROM CIRCULATION PUMPS TO THE VALVE STATION			
9.1	High flow	Operator error-violate administrative controls	Potential (confined spill of 8H at valve station, if not expecting transfer	Batch process	
				Controlled, diked & ventilated areas	
				Operator present at fill area	
				Spill control material	
				"IC" Procedural controls on asset piping arrangement	
				Multiple isolation valves	
9.2	Low/no flow		NCI-operations standpoint		
9.3	Reverse flow		NCI-not physically possible to overcome line pressure		
9.4	Misdirected flow	Operator error-install wrong spool piece	NCI-operations/quality control issue	"IC" Procedural controls on spool piece arrangement	
			Contamination of ground, equipment, etc.		
9.5	High temperature	External fire	NCI-piping specs-1900F		
9.6	Low temperature	Cold winter	Loss of containment-freeze small vol. of static material inadvertently left in pipe (item 9.10)	Pipe normally empty	
9.7	High pressure		NCI-cannot generate pressures exceeding pipe spec 150 psi		
9.8	Low pressure		NCI-vacuum not credible		

Item Number	Deviation	Causes	Consequences	Safeguards	Actions
		9.0 LINE - DISCHARGE LINE FROM CIRCULATION PUMPS TO THE VALVE STATION (continued)			
9.9	High concentration of contaminants		HCl-no injection point to add contaminants		
9.10	Loss of containment	Low temperature-freeze line (item 9.6)	Criticality concern-tank material into an unfavorable geometry container	Routine procedural inspection of tank twice per shift	
		Valve failure	Contamination of ground, equipment, etc.	On-site Emergency Brigade	
		Corrosion		Operator present during tank-to-tank transfer	
				Spill control procedures	
				Containment dike	
		10.0 LINE - OVERFLOW LINE FROM HX TANKS TO OVERFLOW TANK			
10.1	High flow		HCl		
10.2	Low/no flow	Check valve failure	High level in the HX STORAGE TANK (item 7.1)	Level indication in Overflow and HX tanks	
		Debris-plug in line		High level alarms in Overflow and HX tanks	
				Independent High High level alarm in HX tanks	
				Containment pad	
10.3	Reverse flow		HCl		
10.4	Misdirected flow		HCl		
10.5	High temperature	External fire	HCl-piping spec#9-1000		
10.6	Low temperature		HCl-no liquid accumulation in gravity fed line		
10.7	High pressure		HCl-cannot generate pressures exceeding pipe spec 100 psi		
10.8	Low pressure		HCl-vacuum not credible		

Item Number	Deviation	Cause	Consequences	Safeguards	Actions
			10.0 LINE - OVERFLOW LINE FROM [illegible] TANKS TO OVERFLOW TANK (continued)		
10.9	High concentration of contaminants		HCl-no injection point to add contaminants		
10.10	Loss of containment	Valve failure Corrosion	HCl-potential spill of [illegible] in tank containment pad	Routine procedural inspection of tank twice per shift Containment dike	
			11.0 VESSEL - OVERFLOW TANK		
11.1	High level	High level in the [illegible] STORAGE TANK (Item 7.1) Level indication failure	High level in the SUMP (Item 12.1) HCl-potential spill of [illegible] in tank containment pad	Low concentration of [illegible] (<3 g NH3/l) Level indicator High level alarm Containment dike	
11.2	Low level		HCl-normal operations		
11.3	High temperature	External fire	HCl-criticality concern-concentrate [illegible] solution	On-site Emergency Brigade Slow evaporation rate of [illegible] Low concentration of [illegible] (<3 g NH3/l) Level indicator High level alarm Tank normally empty Containment dike	
11.4	Low temperature	Cold winter	HCl-tank normally empty		
11.5	High pressure	Plugged vent line Check valve failure	HCl-potential tank damage, if pressurization more credible	Atmospheric tank 0.3 inch vent line	
11.6	Low pressure		HCl-vacuum not credible		

INSTRUMENT AIR SYSTEM						
Item No.	Header Number	Description	Failure Mode On Loss of Air	Effect	Safety Response	Actions
1	IA-12	Level Readouts Cold Feed Prep.		Loss of tank level instrument readout.	None	
2	IA-12	Eductor Nitric Acid Supply Valves 30PV, 31PV, & 32PV	Fail closed	Shut down process because of loss of transfer.	None	
3	IA-13	Room Exhaust Control Dampers Isolation Valve #1 Isolation Valve #2	Fail open Fails open Fails closed	Exhaust System will function in spite of loss of Instrument Air.	None	
4	IA-13	High Volume Air Monitoring System Isolation Valves 1509 & 1510	Fail closed	Loss of automatic air monitoring	"Low flow" alarm indicates to HP that the monitors are not functional. LCO 3.2.6 in the OSR requires that personnel in monitored areas that are not wearing respiratory protection exit. Personnel can return wearing respiratory protection as determined by HP or if compensatory air monitoring is established	
5	IA-13	Vent Condenser System Freon Control Valves	Fail closed	Loss of cooling	High vent temperature switch will automatically shut down the process.	
6	IA-10	Phase I Glovebox Exhaust Control Dampers Normal Exhaust Header Isolation Maintenance Exhaust Header Isolation	Fail open Fails open Fails closed	No effect if the system is in the normal mode. Automatically switch to Normal Exhaust if system is in the maintenance mode. Potential air imbalance between rooms resulting in flow reversal.	None	Recommend that an air balance analysis be performed for the exhaust system functioning in the normal exhaust mode with a maintenance panel removed.
7	IA-9	Independent Cooling Water Supply Control Valve 5040PV	Fails open	None	None	

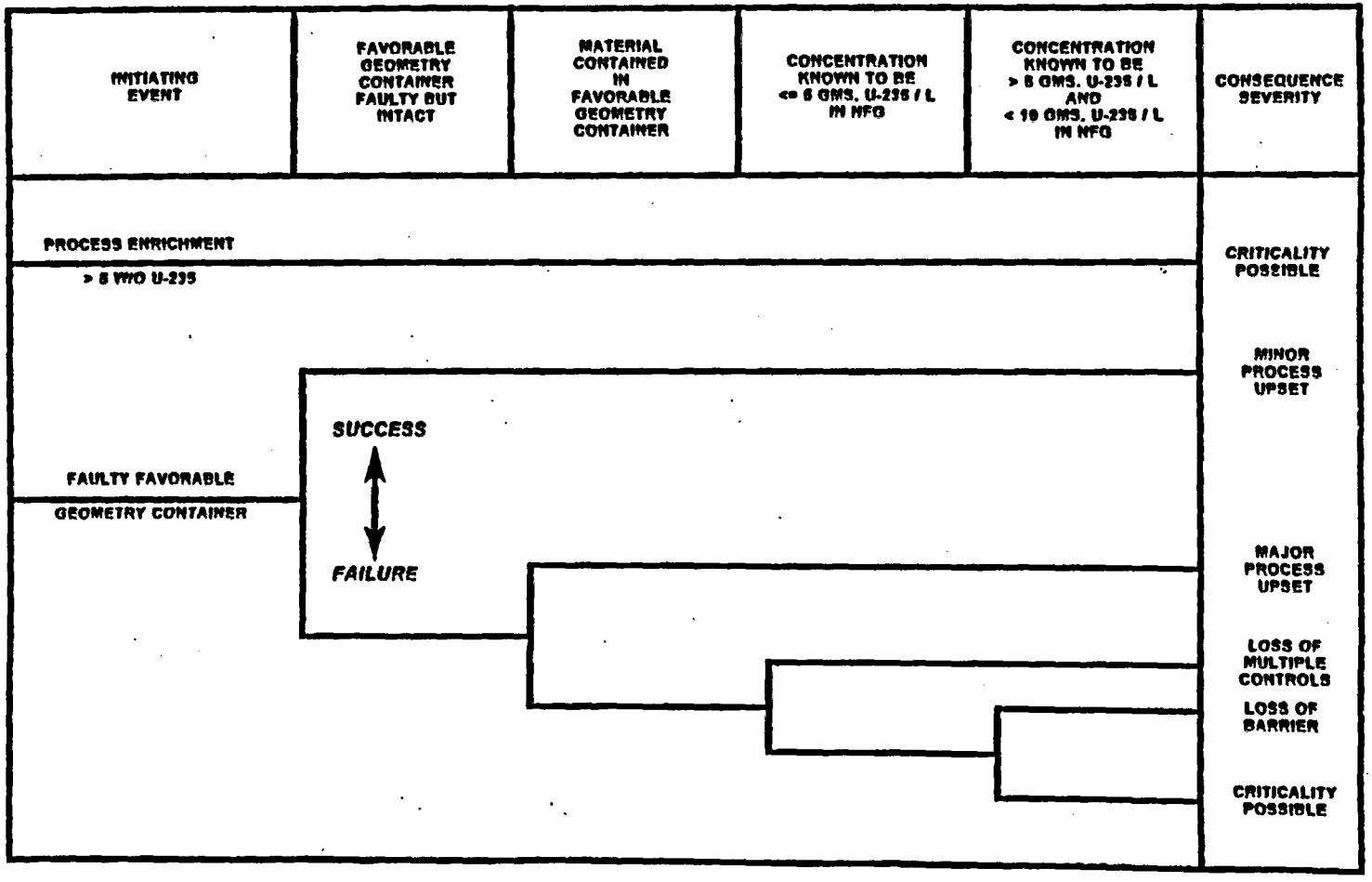
Example Failure Modes and Effects Analysis for Instrument Air
APPENDIX B.4

Item No.	Header Number	Description	Failure Mode On Loss of Air	Effect	Safety Response	Actions
8	IA-9	Soft Structure Air Handling Unit Controls		Loss of climate control in soft structure.	None	
9	IA-9	Fire Dampers 223HV & 461HV	Fail closed with mechanical stop. Set for minimum 10% flow	Reduced air flow in building.	None. Preferred state in case fire suppression equipment is needed.	
10	IA-9	Temperature Control Valves for Breathing Air Compressor Cooling Water	Fail closed	Cooling water continues to flow through temperature control valve bypass.	None	
11	IA-9	Cooling Water Control Valves To Air Supply System Chillers ICWS 305TV & ICWS 316TV	Fail open	Loss of humidity control in Supply Air. Could result in false activation of NIMs and ionizing fire detectors.	Automatic activation of the Fire Suppression Equipment is manually bypassed and a fire watch is set to activate fire suppression, if required. Fire detection equipment and automatic fire alarms remain active.	
12	IA-9	Air Supply Controls-Phases I, II, & III		Loss of Air Supply System	None	
13	IA-23	Glovebox Exhaust Control Dampers Normal Exhaust Header Isolation Maintenance Exhaust Header Isolation	Fail open Fails open Fails closed	No effect if the system is in the normal mode. Automatically switch to Normal Exhaust if system is in the maintenance mode. Potential air imbalance between rooms resulting in flow reversal.	None	Recommend that an air balance analysis be performed for the exhaust system functioning in the normal exhaust mode with a maintenance panel removed.
14	IA-20	B-Line Cooling Water Make-up Valve 5027LV	Fails closed	Make-up water valve will be inoperable.	None. Operational concern rather than safety concern.	
15	IA-20	B-Line Cooling Water Make-up Tank Level Indicator	Low level indication	Shuts off BCW pumps and cooling water is lost to the storage vault, vessel vent heat exchanger, and various process coolers.	Operator can manually bypass the low level interlock and restart the pumps.	Recommend that a step be added to the BCW operating procedure to manually bypass the low level interlock upon loss of Instrument Air.

Example Failure Modes and Effects Analysis for Instrument Air

Item No.	Header Number	Description	Failure Mode On Loss of Air	Effect	Safety Response	Actions
16	IA-20	B-Line Cooling Water Pressure Control Valve 5042PV	Fails open	Reduced BCW pressure in the heat exchanger.	None. Failure mode continues to maintain BCW pressure less than ICW, preventing contamination of ICW.	
17	IA-20	Vessel Vent Scrubber Temperature Control Valve 81TV	Fails open	Increased flow of BCW to the heat exchanger.	None	
18	IA-12	Level Readouts Cold Feed Prep.		Loss of tank level instrument readout.	None	
19	IA-729	High Volume Air Monitor Exhauster Bypass Control Valve 425PV	Fails closed	Loss of monitoring capability.	None	
20	IA-729	High Volume Air Monitor Exhauster Control Valves 430HV, 431HV	Fail closed	Loss of automatic air monitoring	"Low flow" alarm indicates to HP that the monitors are not functional. LCO 3.2.6 in the OSR requires that personnel in monitored areas that are not wearing respiratory protection exit. Personnel can return wearing respiratory protection as determined by HP or if compensatory air monitoring is established.	
21		Temperature Control Valves, Product Storage Vault Bath Cooling Coils	Fail open	Maximum cooling water flow.	None	

Example Failure Modes and Effects Analysis for Instrument Air



Event Tree for Scrap Recovery
Solvent Extraction Favorable Geometry Vessels
APPENDIX B.5

APPENDIX B.6 Qualitative Fault Tree Example for Release of Uf_6 During Vaporization

In this example, Fault Tree Analysis is used to model the scenarios leaking to a UF_6 release during vaporization.

Figure B.6-1 shows an example system for vaporization of UF_6. The system consists of a vaporizer chest with steam supply, emergency cooling water, receiving tank, safe sump and reservoir and scrubber system. This fault tree, labeled "Example Tree for Release of UF_6 During Vaporization", is a qualitative model of the vaporizer chest only. The UF_6 is transported in large steel cylinders. The vaporizer chest is designed to enclose this cylinder and all its connections, and the steam condensate line is supplied with a conductivity cell (with alarm, automatic steam shutoff, and isolation capability) for the detection of leaks.

Analysis

The first step in the analysis is to define the problem by documenting the Top Event, Existing Conditions, and Physical Boundaries. The vaporization process is studied and a logic diagram is constructed that documents all the various mechanisms that can lead to a release of UF_6, which is the Top Event for this tree. The logic uses AND gates to represent events that must exist simultaneously to result in the Top Event. For example, under Gate 2 in the tree, for a liquid release to the building to occur, there must be two events; a release within the chest, and a failure to detect and stop it in time (Gates 6 AND 8). The logic uses OR gates for events where any singe one can result in the Top Event. For example, under Gate 8 in the tree, there are three separate ways (failures for the steam condensate to carry UF_6 out; instrument fails to detect, fails to shutoff, or fails to alarm and operator does not catch this failure. Tree development uses this logic to analyze until all events go to basic event, or the system boundary is reached. Mitigation of such a release, to prevent its release to the environment, is a system boundary, and could be analyzed separately in an event tree.

Evaluation

The next step in the analysis is to determine the minimal cutsets, shown in the table labeled as such. Since no values were assigned to this example, the program (CAFTA), assigned a probability of 1 to all basic events. Qualitatively, it can be seen that a release of UF_6 to the buildings can occur as a result of a single event, such as an impact to the piping or valve. Quantification of this top event would require failure rates, human error probabilities and historical operating data. Quantification may demonstrate that some events described in this tree are in actuality a combination of events that would require further restudy (i.e., cylinder rupture is a result of an overweight cylinder and failure to check weight upon arrival).

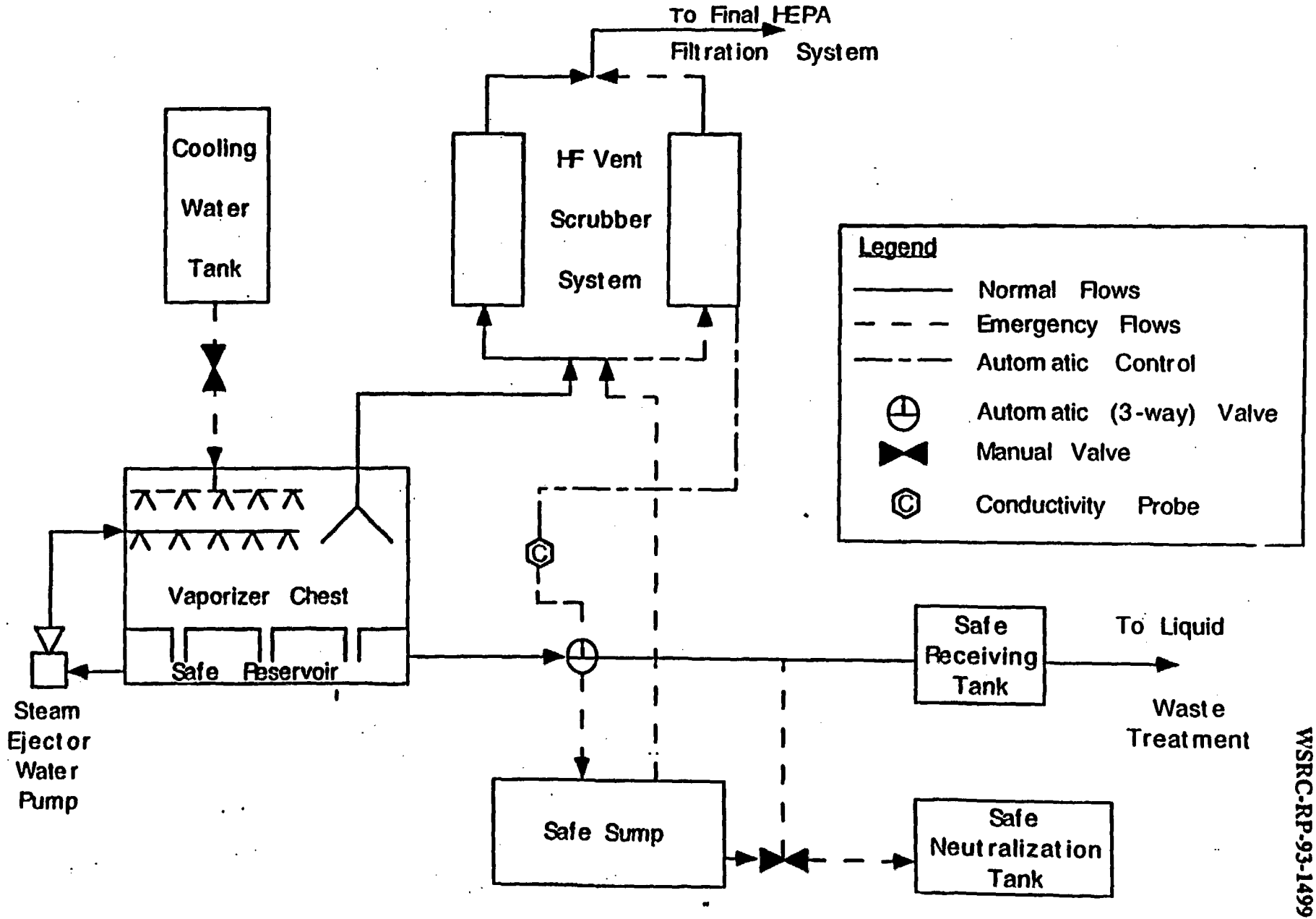
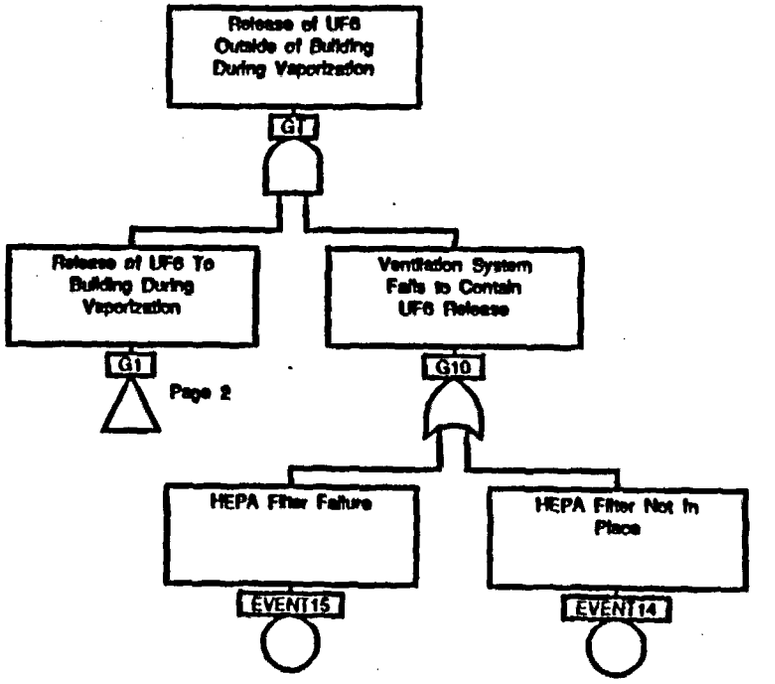
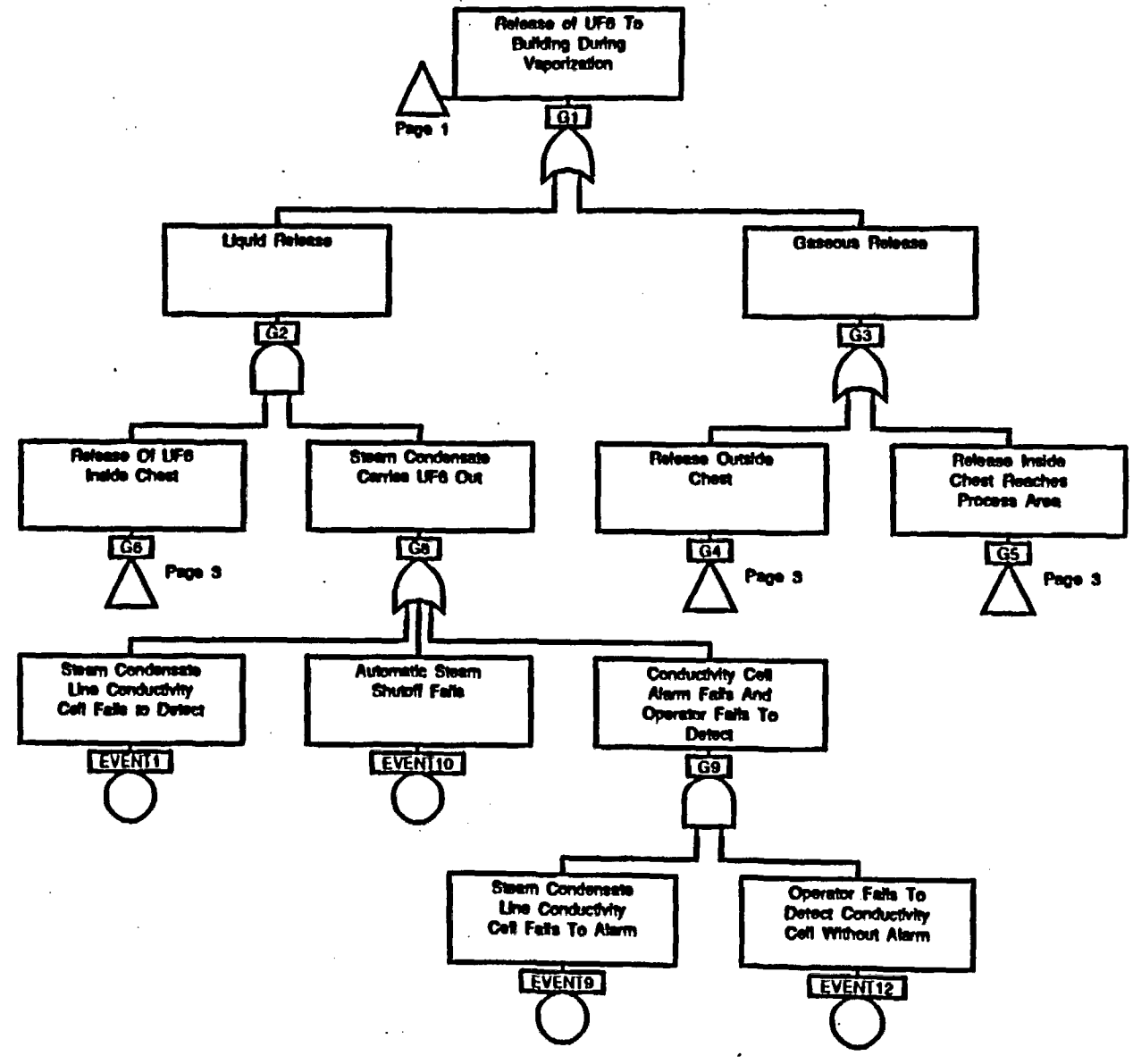

To Final HEPA
Filtration System
Cooling
Water
Tank
HF Vent
Scrubber
System
Legend
Normal Flows
Emergency Flows
Automatic Control
Automatic (3-way) Valve
Manual Valve
Conductivity Probe
Vaporizer Chest
Safe Reservoir
Steam
Ejector
Water
Pump
Safe
Receiving
Tank
To Liquid
Waste
Treatment
Safe Sump
Safe
Neutralization
Tank

FIGURE B.6-1

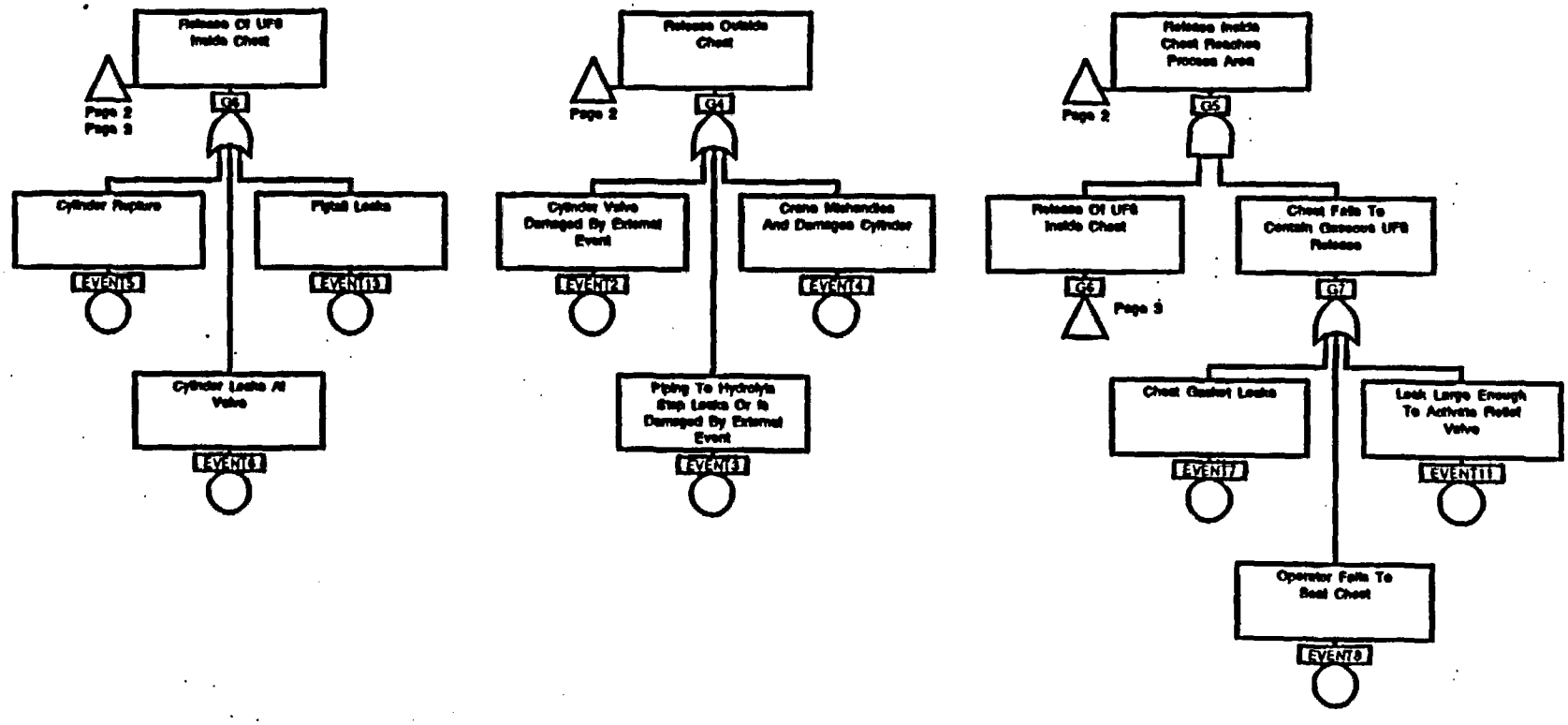


Release of UF6 During Vaporization | .\RAY.CAF | 6-14-94 | Page 1



1 2 3 4

Release of UF6 During Vaporization | .\RAY.CAF | 6-14-94 | Page 2



Release of UF6 During Vaporization	.\RAY.CAF	6-14-94	Page 3

Gate/Event Name	Page	Zone	Gate/Event Name	Page	Zone	Gate/Event Name	Page	Zone	Gate/Event Name	Page	Zone
EVENT1	2	1									
EVENT10	2	2									
EVENT11	3	7									
EVENT12	2	3									
EVENT13	3	2									
EVENT14	1	3									
EVENT15	1	2									
EVENT2	3	3									
EVENT3	3	4									
EVENT4	3	4									
EVENT5	3	1									
EVENT6	3	2									
EVENT7	3	6									
EVENT8	3	6									
EVENT9	2	2									
G1	1	1									
G1	2	2									
G10	1	2									
G2	2	2									
G3	2	4									
G4	2	3									
G4	3	4									
G5	2	4									
G5	3	6									
G6	2	1									
G6	3	2									
G6	3	5									
G7	3	6									
G8	2	2									
G9	2	3									
GT	1	2									

Cutsets for Example UF6 Release Fault Tree

Set No.	Event Name	Description	C	B.E. Prob	Calc. Result	Cutset Prob
	GT					0.00E+00
1.	EVENT11	Leak Large Enough To Activate Relief Valve				1.00E+00
	EVENT13	Pigtail Leaks				
	EVENT15	HEPA Filter Failure				
2.	EVENT11	Leak Large Enough To Activate Relief Valve				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT6	Cylinder Leaks At Valve				
3.	EVENT15	HEPA Filter Failure				1.00E+00
	EVENT2	Cylinder Valve Damaged By External Event				
4.	EVENT15	HEPA Filter Failure				1.00E+00
	EVENT4	Crane Mishandles And Damages Cylinder				
5.	EVENT15	HEPA Filter Failure				1.00E+00
	EVENT3	Piping To Hydrolyis Step Leaks Or Is Damaged By External Event				
6.	EVENT11	Leak Large Enough To Activate Relief Valve				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT5	Cylinder Rupture				
7.	EVENT13	Pigtail Leaks				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT7	Chest Gasket Leaks				
8.	EVENT15	HEPA Filter Failure				1.00E+00

Cutsets for Example UF6 Release Fault Tree (CONT.)

Set No.	Event Name	Description	C	B.E. Prob	Calc. Result	Cutset Prob
	EVENT6	Cylinder Leaks At Valve				
	EVENT7	Chest Gasket Leaks				
9.	EVENT15	HEPA Filter Failure				1.00E+00
	EVENT5	Cylinder Rupture				
	EVENT8	Operator Fails To Seal Chest				
10.	EVENT13	Pigtail Leaks				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT8	Operator Fails To Seal Chest				
11.	EVENT15	HEPA Filter Failure				1.00E+00
	EVENT6	Cylinder Leaks At Valve				
	EVENT8	Operator Fails To Seal Chest				
12.	EVENT12	Operator Fails To Detect Conductivity Cell Without Alarm				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT6	Cylinder Leaks At Valve				
	EVENT9	Steam Condensate Line Conductivity Cell Fails To Alarm				
13.	EVENT12	Operator Fails To Detect Conductivity Cell Without Alarm				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT5	Cylinder Rupture				
	EVENT9	Steam Condensate Line Conductivity Cell Fails To Alarm				
14.	EVENT12	Operator Fails To Detect Conductivity Cell Without Alarm				1.00E+00
	EVENT13	Pigtail Leaks				

Cutsets for Example UF6 Release Fault Tree (CONT.)

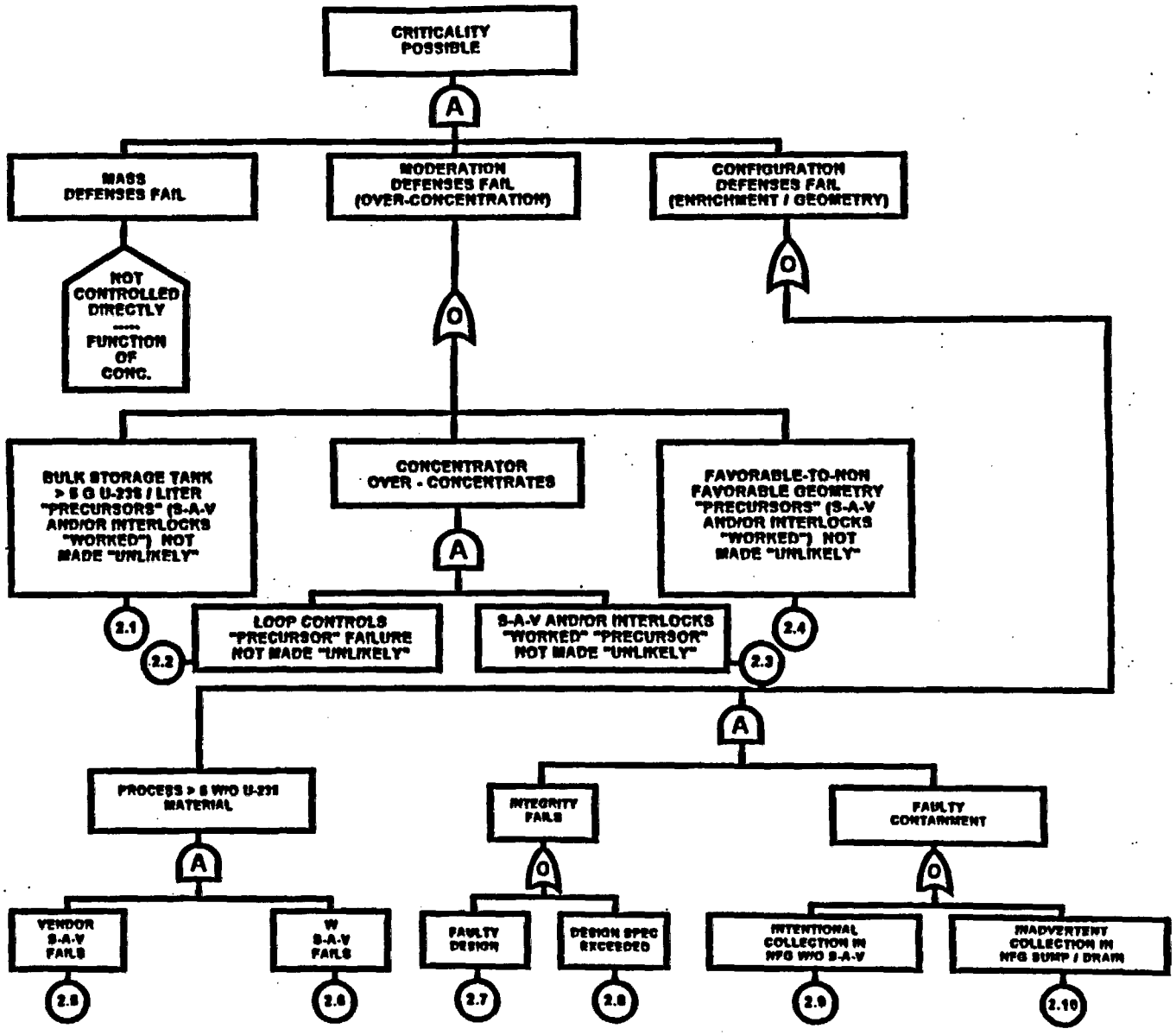
Set No.	Event Name	Description	C	B.E. Prob	Calc. Result	Cutset Prob
	EVENT15	HEPA Filter Failure				
	EVENT9	Steam Condensate Line Conductivity Cell Fails To Alarm				
15.	EVENT14	HEPA Filter Not In Place				1.00E+00
	EVENT6	Cylinder Leaks At Valve				
	EVENT7	Chest Gasket Leaks				
16.	EVENT15	HEPA Filter Failure				1.00E+00
	EVENT5	Cylinder Rupture				
	EVENT7	Chest Gasket Leaks				
17.	EVENT10	Automatic Steam Shutoff Fails				1.00E+00
	EVENT13	Pigtail Leaks				
	EVENT15	HEPA Filter Failure				
18.	EVENT1	Steam Condensate Line Conductivity Cell Fails to Detect				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT6	Cylinder Leaks At Valve				
19.	EVENT1	Steam Condensate Line Conductivity Cell Fails to Detect				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT5	Cylinder Rupture				
20.	EVENT1	Steam Condensate Line Conductivity Cell Fails to Detect				1.00E+00
	EVENT13	Pigtail Leaks				
	EVENT15	HEPA Filter Failure				

Cutsets for Example UF6 Release Fault Tree (CONT.)

Set No.	Event Name	Description	C	B.E. Prob	Calc. Result	Cutset Prob
21.	EVENT10	Automatic Steam Shutoff Fails				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT6	Cylinder Leaks At Valve				
22.	EVENT10	Automatic Steam Shutoff Fails				1.00E+00
	EVENT15	HEPA Filter Failure				
	EVENT5	Cylinder Rupture				
23.	EVENT11	Leak Large Enough To Activate Relief Valve				1.00E+00
	EVENT13	Pigtail Leaks				
	EVENT14	HEPA Filter Not In Place				
24.	EVENT11	Leak Large Enough To Activate Relief Valve				1.00E+00
	EVENT14	HEPA Filter Not In Place				
	EVENT6	Cylinder Leaks At Valve				
25.	EVENT14	HEPA Filter Not In Place				1.00E+00
	EVENT2	Cylinder Valve Damaged By External Event				
26.	EVENT14	HEPA Filter Not In Place				1.00E+00
	EVENT4	Crane Mishandles And Damages Cylinder				
27.	EVENT14	HEPA Filter Not In Place				1.00E+00
	EVENT3	Piping To Hydrolyis Step Leaks Or Is Damaged By External Event				
28.	EVENT14	HEPA Filter Not In Place				1.00E+00
	EVENT5	Cylinder Rupture				

Cutsets for Example UF6 Release Fault Tree (CONT.)

Set No.	Event Name	Description	C	B.E. Prob	Calc. Result	Cutset Prob
	EVENT8	Operator Fails To Seal Chest				
29.	EVENT13	Pigtail Leaks				1.00E+00
	EVENT14	HEPA Filter Not In Place				
	EVENT7	Chest Gasket Leaks				
30.	EVENT14	HEPA Filter Not In Place				1.00E+00
	EVENT6	Cylinder Leaks At Valve				
	EVENT8	Operator Fails To Seal Chest				



Fault Tree for Scrap Recovery
Solvent Extraction Favorable Geometry Vessels
APPENDIX B.7

APPENDIX C.1 Quantitative Event Tree Example for Airborne Activity Release

In this example, Event Tree Analysis is used to evaluate the important accident sequences that link ventilation failures to releases of airborne radioactive material from process equipment.

Introduction

The event tree is a logic method for identifying the various possible outcomes of a given initiating event. The number of possible final outcomes depends upon various options that are applicable following the initiating event. In this analysis, the initiating event for each tree was chosen based on its energetics (i.e., medium). Events subsequent to the initiating event are analyzed by system characteristics, and the sequence from the intiating event to final outcome is diagrammed on the event tree.

Release sequences are naturally based on the physical confinement equipment (sometimes referred to as confinement barriers). When dealing with airborne materials, the ventilation equipment became the significant confinement barriers for releases. Event trees provided combined accident sequences from the intiating event to the release of activity at the points of interest. The points of interest are releases to the rooms and cabinets, which may ultimately reach the outside and become a source of an airborne release from the stack.

Analysis

The event tree for this study is shown in Figure C.1-1. In the preparation of an event tree, the first step is to determine which systems affect the subsequent course of events. Given an initiating event (release to the room), the system which affects the subsequent course of events is the ventilation exhaust system and the sand (or HEPA) filter. Each of these barriers are ordered in their sequence across the top of the figure. The upper branch of the tree represents failure of the system to fulfill its confinement function. There are known relationships (constraints) between system functions. For example, if the room exhaust system fails, then no release to the stack will occur because the activity cannot be transported to the stack for release. Once these relationships are determined, some of the chains can be eliminated because they represent illogical or inconsequential sequences. These reduced event trees are used in the analysis.

Evaluation

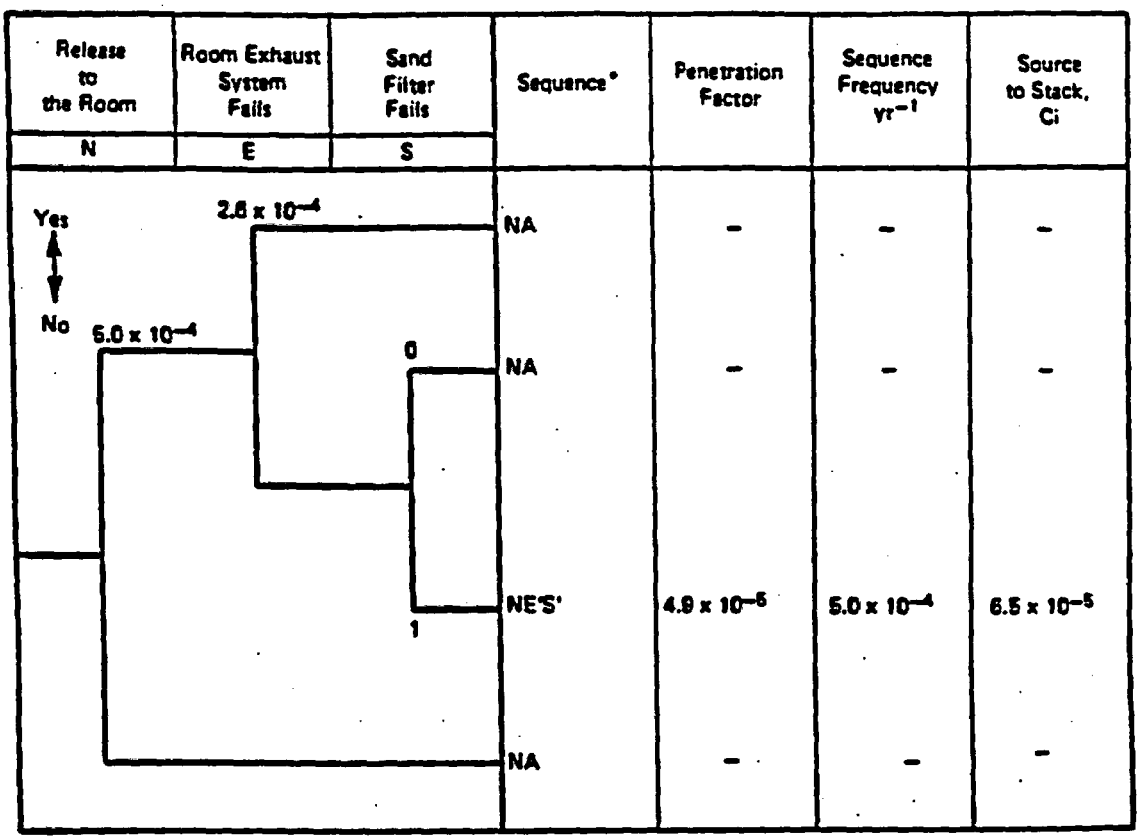
If the event sequences are independent, then the expected frequency of occurrence of a given sequence is the product of the initiating event frequency and the individual demand probabilities of the individual systems in that sequence. Since the failure demand probabilities are almost always 0.1 or less, it is common practice to approximate success (1-p) as 1. It should be noted that as indicated in Figure C.1-1, the event tree at each branch point provides only two options, system failure or success. No consideration is given to the fact that partial system success may occur within an accident sequence. Thus, an accident sequence is conservatively assumed to lead to the total consequence. The effects of partial system failure are not treated, but are accounted for by adjusting the consequence (in curies) to compensate for partial failure.

Input data for the sequence analysis include:

1. the frequency of releases to the room (5.0E-04/yr),
2. the probability of concurrent room exhaust failure (2.6E-04), and
3. the probability of concurrent filter failure (conservatively assigned a value of 1).

The first two values come from other sources (e.g., fault tree analyses). The third value is a conservative assumption (p=1) that the filter will fail concurrently with the release to the room

and with the exhaust fan failure. Consequence assessment determines the source term (6.5E-05 Ci), the release from the stack, by combining the release to the room (1.3 Ci) with the filter penetration factor (4.9E-09). These values were determined separately.



*Sequences in the Yes Direction Carry the System Letter. Sequences in the No Direction are Denoted with a Prime Notation.
NA—Not Applicable

FIGURE C.1-1. Event Tree

APPENDIX C.2

QUANTITATIVE FAULT TREE EXAMPLE FOR NUCLEAR CRITICALITY

In this example, Fault Tree Analysis is used to assess nuclear safety in an enriched uranium (EU) storage vault.

Introduction

To identify the major causes of a criticality event, Figure C.2-1, a Nuclear Criticality Fault Tree was drawn. Computer codes are available to evaluate this fault tree. All of the factors shown on the fault tree were considered while the facility was being designed. These factors include the density of the fissionable isotopes, geometry, reflection, and moderation. Safety features are included in the design, and with the exception of geometry, they cannot be exceeded easily even by human error. It is possible to exceed the safety factors designed into the facility for geometry, and the most likely cause is human error. The next section discusses how these geometric considerations could be exceeded.

Description

Since EU in the vault area is only handled or stored in DOT-approved shipping containers and since the number of these packages (shipping containers) calculated to be subcritical is greater than the capacity of the vault area, a nuclear criticality accident is deemed incredible.

However, the possibility exists for the storage of EU in the vault outside of a shipping container. This would violate the normal storage procedure, and would offer some criticality risk. Feed material which has not been placed into the processing stream by the end of the shift must be returned to a vault for storage purposes. This material is presently being stored in vaults with no shipping container. Other EU material is also stored in these vaults with only product cans for containment. Since this is a normally accepted method of storage, it is possible, given the need to store the materials (i.e., end of shift or the possibility of exceeding operating limits if material is not moved), that material would be stored in the vault outside of a shipping container. This would require basically two steps, a decision to store the material in this fashion in the vault and the establishment of a criticality array.

Analysis

Violation of the geometric considerations would require a violation of the normal storage procedure for this material. Failure to properly store a single can of material in the vault would not result in a critical array. Upon the storage of the second container of material, the operator is faced with a storage decision similar to that encountered for the first container (i.e., what geometry should be used in storing these "odd" containers) and therefore the portability of failure should be the same. The situation for the third and succeeding cans is not identical. By placement of the first two cans, the operator has established a storage "plan" with which he is comfortable and he will most likely continue this established pattern until corrected.

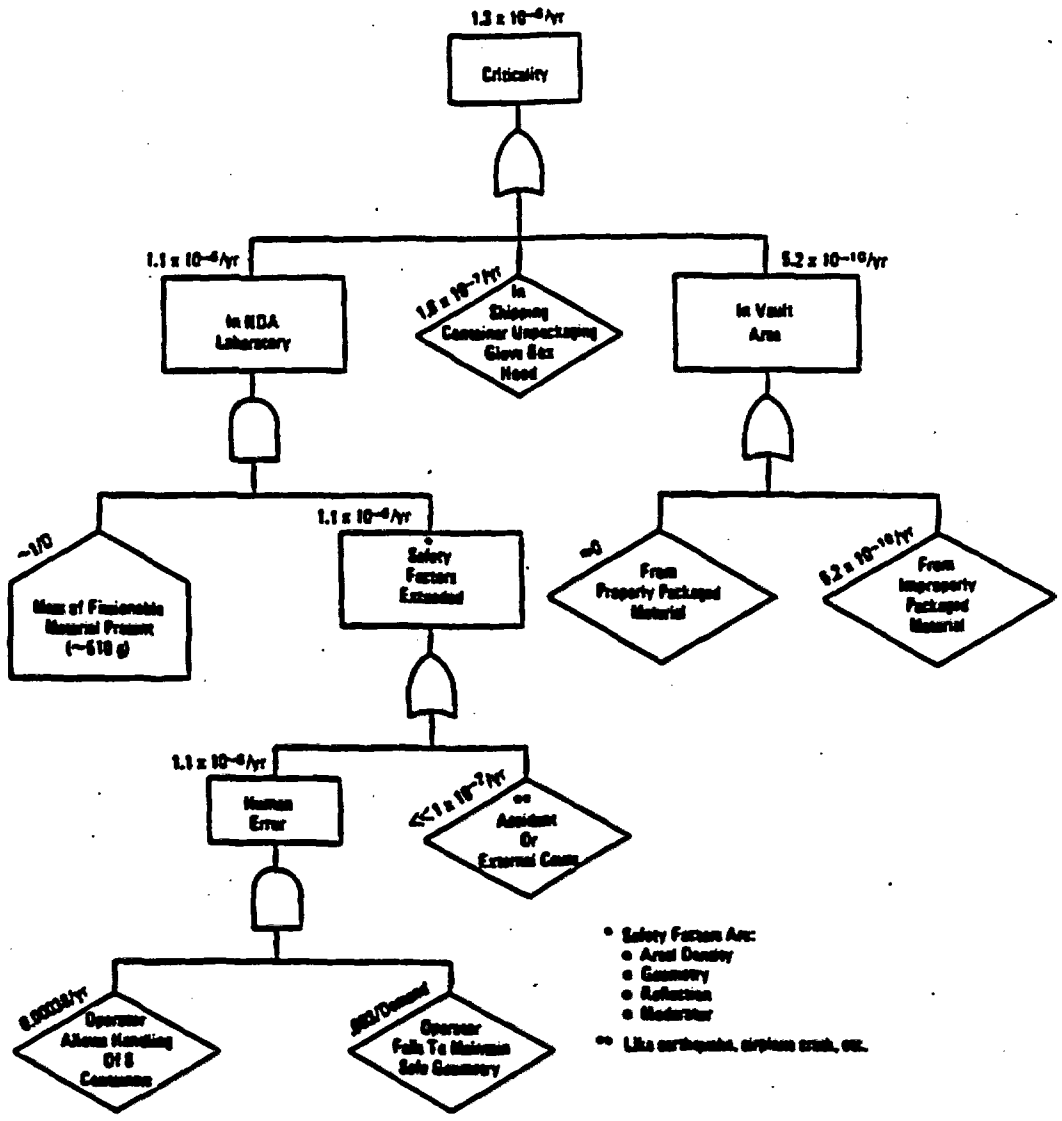


FIGURE C.2-1. A Nuclear Criticality Fault Tree

APPENDIX D.1

EXAMPLE OPERATIONAL SAFETY REQUIREMENTS (OSRs)

The following tables illustrate the LCOs and the Surveillance Requirements that could result from an ISA. Each of these applies to a ventilation system in a nuclear materials processing facility. Other OSRs would be prepared for each of the other unit operations in the facility.

Table 3.5.1 Confinement Ventilation System (Nuclear Materials Plant)
Table 3.6.1 Stack Exhaust System (Nuclear Materials Plant)
Table 3.6.2 Dissolver Offgas System (Fuel Reprocessing Plant)
Table 3.6.3 Dissolver Offgas System - Decladding Operation (Fuel Reprocessing Plant)
Table 3.6.4 Dissolver Offgas System - Fuel Dissolution Operation (Fuel Reprocessing Plant)
Table 3.6.5 Ammonia Offgas System (Fuel Reprocessing Plant)
Table 3.6.6 Glovebox Offgas System (Nuclear Materials Plant)

Each OSR contains three parts: a set of LCOs, required actions (when the system fails), and surveillance requirements.

The LCOs consist of a list of equipment, instruments, and systems that are assumed as part of the safety analysis and that validate the analysis. Should any of these items not be available, the safety analysis may be invalidated or inapplicable.

Required actions define the conditions (failures) for which action must be taken to correct the deficiency. The required action(s) and response times are specified.

Surveillance requirements specify what must be inspected, for what ,and at what intervals. Failure to comply with these requirements may be interpreted as failure to ensure that the facility is maintaining safety-related equipment in the conditions assumed in the safety analysis.

3/4.5 CONFINEMENT SYSTEM

3:5.1 CONFINEMENT VENTILATION SYSTEM

LCO:

A. For (primary/secondary) confinement, two Confinement Ventilation Systems shall be OPERABLE with each system having the following components:

- One supply fan
- One exhaust fan
- One in-line charcoal filter
- One in-line HEPA filter
- Instrumentation:
  - One exhaust flow indicator, with alarm
  - One beta-gamma radiation monitor, with alarm
  - One gas temperature sensor downstream of the filter

B. For (primary/secondary) confinement, one Confinement Ventilation System shall be in operation.

MODE APPLICABILITY: OPERATION, STANDBY, and PARTIAL SHUTDOWN

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. One (Primary/Secondary) Confinement Ventilation System train is inoperable.	A.1 Restore Confinement Ventilation System train to OPERABLE status.	72 Hours
B. The ACTION and associated Completion Time of Condition A are not met.	B.1 Place the [ ] in FULL SHUTDOWN.	6 Hours
C. Both (Primary/Secondary) Confinement Ventilation System trains are inoperable.	C.1 Place the [ ] in PARTIAL SHUTDOWN. **AND** C.2 Restore one system to OPERABLE status.	1 Hour 2 Hours

3/4.5 CONFINEMENT SYSTEM

3.5.1 CONFINEMENT VENTILATION SYSTEM (continued)

SURVEILLANCE REQUIREMENTS

	SURVEILLANCE REQUIREMENT	FREQUENCY
SR 4.5.1.1	Verify that the (Primary/Secondary) Confinement Ventilation System train in operation is taking suction on the (Primary/Secondary) confinement zone at a rate of [ ] scfm or more.	8 Hours
SR 4.5.1.2	Verify that the (Primary/Secondary) Confinement Ventilation System train in standby is aligned to take suction on the (Primary/Secondary) confinement zone and that the fan control is in "AUTO" position.	8 Hours
SR 4.5.1.3	Operate each (Primary/Secondary) Confinement Ventilation System train for [≥ 10 hours continuous with the heaters operating or (for systems without heaters) ≥ 15 minutes].	Monthly
SR 4.5.1.4	Perform the following on each (Primary/Secondary) confinement exhaust flow indicator and alarm:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL TEST	Quarterly
	• CHANNEL CALIBRATION	Annually
SR 4.5.1.5	Perform the following on each (Primary/Secondary) beta-gamma radiation monitor and alarm:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL TEST	Quarterly
	• CHANNEL CALIBRATION	Annually

3/4.5 CONFINEMENT SYSTEM

3.5.1 CONFINEMENT VENTILATION SYSTEM (continued)

SURVEILLANCE REQUIREMENTS (continued)

	SURVEILLANCE REQUIREMENT	FREQUENCY
SR 4.5.1.6	Perform the following on each (Primary/Secondary) gas temperature sensor:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL TEST	Quarterly
	• CHANNEL CALIBRATION	Annually
SR 4.5.1.7	For each (Primary/Secondary) Confinement Ventilation System train, verify that the filter cleanup system satisfies the in-place penetration and bypass leakage testing acceptance criteria of < [*]% and uses the test procedure guidance in Regulatory Positions C.5.a, C.5.c, and C.5.d of Regulatory Guide 1.52, Revision 2, March 1978, and verify that the system flow rate is [ ] cfm ±10%.	18 Months OR After any structural maintenance on the HEPA filter or charcoal absorber housings OR Following painting, fire, or chemical release in any ventilation zone communicating with the system

3/4.5 CONFINEMENT SYSTEM

3.5.1 CONFINEMENT VENTILATION SYSTEM (continued)

SURVEILLANCE REQUIREMENTS (continued)

	SURVEILLANCE REQUIREMENT	FREQUENCY
SR 4.5.1.8	For each (Primary/Secondary) Confinement Ventilation System train, verify, within 31 Days after removal, that a laboratory analysis of a representative carbon sample obtained in accordance with Regulatory Position C.6.b of Regulatory Guide 1.52, Revision 2, March 1978, meets the laboratory testing criteria of Regulatory Position C.6.a of Regulatory Guide 1.52, Revision 2, March 1978, for a methyl iodide penetration of <[**]%.	18 Months OR After any structural maintenance on the HEPA filter or charcoal absorber housings OR Following painting, fire, or chemical release in any ventilation zone communicating with the system
SR 4.5.1.9	For each (Primary/Secondary) Confinement Ventilation System train, verify a system flow rate of [ ] cfm ±10% during system operation when tested in accordance with ANSI N510-1975.	18 Months OR After any structural maintenance on the HEPA filter or charcoal absorber housings. OR Following painting, fire, or chemical release in any ventilation zone communicating with the system

3/4.5 CONFINEMENT SYSTEM

3.5.1 CONFINEMENT VENTILATION SYSTEM (continued)

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.5.1.10	For each (Primary/Secondary) Confinement Ventilation System train, verify, within 31 Days after removal, that a laboratory analysis of a representative carbon sample obtained in accordance with Regulatory Position C.6.b of Regulatory Guide 1.52, Revision 2, March 1978, meets the laboratory testing criteria of Regulatory Position C.6.a of Regulatory Guide 1.52, Revision 2, March 1978, for a methyl iodide penetration of <[**]%.	After every 720 Hours of charcoal absorber operation
SR 4.5.1.11	For each (Primary/Secondary) Confinement Ventilation System train, verify that the pressure drop across the combined HEPA filters and charcoal absorber banks is <[6] inches WG while operating the system at a flow rate of [ ] cfm ±10%.	18 Months
SR 4.5.1.12	For each (Primary/Secondary) Confinement Ventilation System train, verify that the filter cooling bypass valves can be manually opened.	18 Months
SR 4.5.1.13	For each (Primary/Secondary) Confinement Ventilation System train, verify that each system produces a negative pressure of ≥ [ ] inches WG in the zone within [ ] minutes after a start signal.	18 Months
SR 4.5.1.14	For each (Primary/Secondary) Confinement Ventilation System train, verify that the heaters dissipate [ ] ± [ ] kW when tested in accordance with ANSI N510-1975.	18 Months
SR 4.5.1.15	For each (Primary/Secondary) Confinement Ventilation System train, verify that the cleanup system satisfies the in-place penetration and bypass leakage testing acceptance criteria of < [*]% in accordance with ANSI N510-1975 for a DOP test aerosol while operating the system at a flow rate of [ ] cfm ±10%.	After each complete or partial replacement of a HEPA filter bank

3/4.5 CONFINEMENT SYSTEM

3.5.1 CONFINEMENT VENTILATION SYSTEM (continued)

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.5.1.16	For each (Primary/Secondary) Confinement Ventilation System train, verify that the cleanup system satisfies the in-place penetration and bypass leakage testing acceptance criteria of < [*]% in accordance with ANSI-1975 for a halogenated hydrocarbon refrigerant-test gas while operating the system at a flow rate of [ ] cfm ±10%.	After each complete or partial replacement of a charcoal absorber bank

* A value of 0.5% is applicable when a HEPA filter or charcoal absorber efficiency of 99% is assumed, or 1% when a HEPA filter or charcoal absorber efficiency of 95% or less is assumed in the ID staff's safety evaluation. (Use the value assumed for the charcoal absorber efficiency if the value for the HEPA filter is different from the charcoal absorber efficiency in the DOE ID staff's safety evaluation).

** The applicable value shall be determined by when P equals the value to be used in the test requirement (%), E is efficiency assumed in the Safety Evaluation Report (SER) for methyl iodide removal (%), and Safety Factor (SF) is the safety factor to account for charcoal degradation between tests (5 for systems with heaters and 7 for systems without heaters).

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.1 STACK EXHAUST SYSTEM (FUEL REPROCESSING PLANT)

LCO: The Stack Exhaust System shall be OPERABLE with:

- Two exhaust fans operating
- Two HEPA filter banks on line
- Two exhaust air activity monitors operating

MODE APPLICABILITY: Whenever any of the offgas subsystems (dissolver, ammonia scrubber, or gloveboxes) are in OPERATION, STANDBY, or PARTIAL SHUTDOWN

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. One exhaust fan is inoperable or not operating.	A.1 Terminate operations in the dissolver, scrubber, or gloveboxes.	30 Minutes
	AND	
	A.2 Verify isolation damper closure.	30 Minutes
	AND	
	A.3 Place the [ ] in FULL SHUTDOWN.	72 Hours
B. One filter bank is inoperable or not in service.	B.1 Terminate operations in the dissolver, scrubber, and gloveboxes.	30 Minutes
	AND	
	B.2 Place the [ ] in FULL SHUTDOWN.	72 Hours

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.1 STACK EXHAUST SYSTEM (FUEL REPROCESSING PLANT) (continued)

ACTIONS

CONDITION	ACTION	COMPLETION TIME
C. One exhaust air activity monitor is inoperable.	C.1 Conduct manual exhaust air activity sampling.	8 Hours
	AND	
	C.2 Place the [ ] in FULL SHUTDOWN.	72 Hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.6.1.1	Verify that the exhaust fan flow alarms are OPERABLE.	Monthly
SR 4.6.1.2	Verify that the HEPA filters are OPERABLE as specified in SRs 4.5.1.7, 4.5.1.9, and 4.5.1.11.	Frequency as stated in SRs 4.5.1.7, 4.5.1.9, and 4.5.1.11
SR 4.6.1.3	Perform the following on the beta-gamma activity monitoring system:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL CHECK	Quarterly
	• CHANNEL CALIBRATION	Annually
SR 4.6.1.4	Verify that the exhaust paths are open by ensuring that dampers are in the correct positions during OPERATION.	Semiannually
SR 4.6.1.5	Verify that the isolation dampers are OPERABLE.	Semiannually

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.2 DISSOLVER OFFGAS SYSTEM (FUEL REPROCESSING PLANT)

LCO: The Dissolver Offgas System shall be OPERABLE with:

- Offgas H_2 concentration $\leq$ 3%
- Offgas NH_3 concentration $\leq$ 14%
- Offgas I-129 and I-131 activity $\leq$ [ ] μCi/mL
- Temperature of the inlet gas to the silver reactor $\geq$ 196°C
- Temperature of the silver reactor $\geq$ 196°C
- On-line particulate filters upstream of the Dissolver Offgas System or Stack Exhaust System interface

MODE APPLICABILITY: OPERATION, STANDBY, and PARTIAL SHUTDOWN

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. H_2 concentration is > 3%. OR NH_3 concentration is > 14%.	A.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND A.2 Enter LCO 3.0.3.	15 Minutes 1 Hour
B. Iodine activity is > [ ] μCi/mL.	B.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND B.2 Enter LCO 3.0.3. AND B.3 Perform an engineering evaluation.	15 Minutes 1 Hour 48 Hours

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.2 DISSOLVER OFFGAS SYSTEM (FUEL REPROCESSING PLANT) (continued)

ACTIONS (continued)

CONDITION	ACTION	COMPLETION TIME
C. Silver reactor temperature or gas temperature is < 196°C.	C.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND C.2 Enter LCO 3.0.3.	2 Hours 3 Hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.6.2.1	Perform the following for the hydrogen concentration, ammonia concentration, and iodine activity indicators and alarms:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL CHECK	Quarterly
	• CHANNEL CALIBRATION	Annually
SR 4.6.2.2	Verify that silver reactor and inlet gas temperatures are within limits.	Before placing the [ ] in STANDBY AND every 8 Hours thereafter
SR 4.6.2.3	Verify that the HEPA filters are OPERABLE as specified in SRs 4.5.1.7, 4.5.1.9, and 4.5.1.11.	Frequency as stated in SRs 4.5.1.7, 4.5.1.9, and 4.5.1.11
SR 4.6.2.4	Verify that the exhaust path is open by ensuring that dampers are in the correct positions.	Semiannually
SR 4.6.2.5	Verify that the isolation dampers are OPERABLE.	Semiannually

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.3 DISSOLVER OFFGAS SYSTEM—DECLADDING OPERATION (FUEL REPROCESSING PLANT)

LCO: The H_2 suppression and ammonia scrubbers (of the Dissolver Offgas System) shall be OPERABLE and operating with:

- H_2 suppression
- Ammonia scrubbers OPERABLE with a water flow rate $\geq$ [ ] gpm

MODE APPLICABILITY: OPERATION, STANDBY, and PARTIAL SHUTDOWN during Decladding Operations

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. Water flow rate to ammonia scrubbers is < [ ] gpm.	A.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY.	2 Hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE REQUIREMENTS		FREQUENCY
SR 4.6.3.1	Verify that the H_2 suppressant chemical, NH_4F-NH_4NO_3, has been charged to the dissolver with concentration $\geq$ [ ] g/L.	Before placing the [ ] in STANDBY during startup
SR 4.6.3.2	Verify that the water flow rate in the ammonia scrubbers is within limits.	Before placing the [ ] in STANDBY during startup AND every 8 Hours thereafter

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.4 DISSOLVER OFFGAS SYSTEM—FUEL DISSOLUTION OPERATION (FUEL REPROCESSING PLANT)

LCO: The acid absorption units (of the Dissolver Offgas System) shall be OPERABLE and operating with one OPERABLE acid absorption unit on line.

MODE APPLICABILITY: OPERATION, STANDBY, and PARTIAL SHUTDOWN during Fuel Dissolution Operations

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. An acid absorption unit is inoperable.	A.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY.	30 Minutes
	AND	
	A.2 Enter LCO 3.0.3.	3 Hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.6.4.1	Verify that at least one acid absorption unit is OPERABLE.	Before initiating fuel dissolution in OPERATION

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.5 AMMONIA OFFGAS SYSTEM (FUEL REPROCESSING PLANT)

LCO: The Ammonia Offgas System (AOS) shall be OPERABLE with:

- One AOS exhaust fan operating
- One prefilter/primary HEPA filter bank in service
- One secondary HEPA filter bank in service
- Primary and secondary HEPA filter differential pressure alarm/shutdown interlocks OPERABLE with:
  - Alarms at 3.0 inches WG
  - Automatic air bleed bypass at 4.0 inches WG
  - Automatic fan shutdown at 5.0 inches WG
- Exhaust air from the AOS containing ammonia concentration ≤ [ ] ppm and radioactivity ≤ [ ] μCi/mL

MODE APPLICABILITY: OPERATION, STANDBY, and PARTIAL SHUTDOWN

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. One AOS exhaust fan is inoperable or not operating.	A.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY.	30 Minutes
	AND	
	A.2 Verify isolation damper closure.	30 Minutes
	AND	
	A.3 Place the [ ] in FULL SHUTDOWN.	24 Hours

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.5 AMMONIA OFFGAS SYSTEM (FUEL REPROCESSING PLANT) (continued)

ACTIONS (continued)

CONDITION	ACTION	COMPLETION TIME
B. One prefilter/primary HEPA filter bank is inoperable or not in service.	B.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND B.2 Place the [ ] in FULL SHUTDOWN.	30 Minutes 24 Hours
C. One secondary HEPA filter bank is inoperable or not in service.	C.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND C.2 Place the [ ] in FULL SHUTDOWN.	30 Minutes 24 Hours
D. An AOS exhaust air activity monitor is inoperable.	D.1 Conduct manual AOS air activity sampling. AND D.2 Place the [ ] in FULL SHUTDOWN.	Hourly 24 Hours
E. An AOS ammonia concentration air monitor is inoperable.	E.1 Conduct manual AOS air ammonia concentration sampling. AND E.2 Place the [ ] in FULL SHUTDOWN.	Hourly 24 Hours

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.5 AMMONIA OFFGAS SYSTEM (FUEL REPROCESSING PLANT) (continued)

ACTIONS (continued)

CONDITION	ACTION	COMPLETION TIME
F. The ammonia concentration in exhaust air is > [ ] ppm.	F.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND	30 Minutes
	F.2 Place the [ ] in FULL SHUTDOWN.	24 Hours
G. The radioactivity in exhaust air is > [ ] µCi/mL.	G.1 Initiate cooling of the dissolver, and place the [ ] in STANDBY. AND	30 Minutes
	G.2 Place the [ ] in FULL SHUTDOWN.	24 Hours

SURVEILLANCE REQUIREMENTS

	SURVEILLANCE REQUIREMENT	FREQUENCY
SR 4.6.5.1	Verify that the AOS fan flow alarms are OPERABLE.	Monthly
SR 4.6.5.2	Verify that the HEPA filters are OPERABLE as specified in SRs 4.5.1.7, 4.5.1.9, and 4.5.1.11.	Frequency as stated in SRs 4.5.1.7, 4.5.1.9, and 4.5.1.11
SR 4.6.5.3	Perform the following on the filter differential pressure alarm/shutdown interlocks:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL CHECK	Quarterly
	• CHANNEL CALIBRATION	Annually

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.5 AMMONIA OFFGAS SYSTEM (FUEL REPROCESSING PLANT) (continued)

SURVEILLANCE REQUIREMENTS (continued)

	SURVEILLANCE REQUIREMENT	FREQUENCY
SR 4.6.5.4	Perform the following on the beta-gamma activity monitoring system:	
	• CHANNEL CHECK	Daily
	• CHANNEL FUNCTIONAL CHECK	Quarterly
	• CHANNEL CALIBRATION	Annually
SR 4.6.5.5	Perform the following on the ammonia concentration monitoring system:	
	• CHANNEL CHECK	8 Hours
	• CHANNEL FUNCTIONAL CHECK	Monthly
	• CHANNEL CALIBRATION	Semiannually
SR 4.6.5.6	Verify that the AOS path is open by ensuring that the dampers are in the correct positions.	Semiannually
SR 4.6.5.7	Verify that the isolation dampers upstream of the AOS and Exhaust Stack System interface are OPERABLE.	Semiannually

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.6 GLOVEBOX OFFGAS SYSTEM

LCO: The Glovebox Offgas System (GBOS) shall be OPERABLE with:

- Two GBOS fans OPERABLE and one GBOS fan operating
- Header vacuum relief valves set at $\leq$ 4.0 inches WG
- Glovebox inlet and outlet filters OPERABLE with differential pressures $\leq$ 1.0 inches WG
- GBOS primary and secondary HEPA filters OPERABLE with differential pressures $\leq$ 2.0 inches WG
- GBOS HEPA filter preheaters OPERABLE with air exit temperature $\geq$ 80°C

MODE APPLICABILITY: OPERATION, STANDBY, and PARTIAL SHUTDOWN

PROCESS AREA APPLICABILITY: [ ]

ACTIONS

CONDITION	ACTION	COMPLETION TIME
A. Two fans are inoperable.	A.1 Terminate all glovebox operations.	24 Hours
B. One fan is inoperable.	B.1 Terminate all glovebox operations.	48 Hours
C No fans are operating.	C.1 Terminate all glovebox operations.	IMMEDIATELY
D. Header vacuum relief valves are inoperable.	D.1 Terminate affected glovebox operations.	2 Hours
E. Individual glovebox inlet or outlet filters are inoperable.	E.1 Terminate affected glovebox operations.	2 Hours

3/4.6 FACILITY VENTILATION/CONFINEMENT

3.6.6 GLOVEBOX OFFGAS SYSTEM (continued)

ACTIONS (continued)

CONDITION	ACTION	COMPLETION TIME
F. Primary or secondary HEPA filters are inoperable.	F.1 Terminate all glovebox operations.	48 Hours
G. HEPA filter preheater is inoperable.	G.1 Terminate affected glovebox operations.	48 Hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE REQUIREMENT		FREQUENCY
SR 4.6.6.1	Perform a functional test of each GBOS fan.	Monthly
SR 4.6.6.2	Verify that vacuum relief valves are set within limits.	Annually
SR 4.6.6.3	Verify that the filter differential pressures are within limits.	Daily
SR 4.6.6.4	Verify that the temperature of the air exiting the preheaters is $\geq 80^{\circ}C$.	4 Hours

APPENDIX E.1

Management Oversight and Risk Tree

Introduction

Frequently, management allocates resources to correct hazards without first obtaining sufficient information to determine whether more hazardous conditions are being neglected, or whether the corrective costs are justified by the benefit or the reduction in risk. In addition, management frequently has little or no information of how risk compares to the actual value of a given program, and thus must make decisions regarding safety without adequate background.

The Management Oversight and Risk Tree (MORT) methodology provides a system for identifying management oversights and specific risks. Once risks have been identified, it is then management's responsibility to provide required resources to reduce or eliminate specific risks and to assume the residual risks. This example describes a few simple techniques which can be used to quantify risks. It also presents a format for presenting risk information to management. Dollar values can be assigned to indirect tangible and intangible costs, including the loss of life. This enables one to present risks in terms of dollar resources which may then be compared to dollar resources allocated to risk reduction.

This in not to imply that human life is of limited value or that it is simple to place a dollar value on intangible effects. Nevertheless, placing a dollar value or some other quantitative scale is necessary in order to approach risk management or to make decisions with logic and good judgment. Dollar value are the simplest means of comparison to maximize benefits derived from risk control expenditure. If analysis indicates that the cost of reducing a hazard is not justified, it does not mean that the hazard should be ignored. Rather, it indicates that management must consider items that fall below established criteria in their decision making.

Risk Identification and Ranking

A systematic search for all risks greatly reduces the number if hazards which will be neglected because of management oversight. Based on the premise that all accident result from unplanned and unwanted transfers of energy, the Risk Identification Tree was developed at EG&G Idaho, and is presented in the following example.

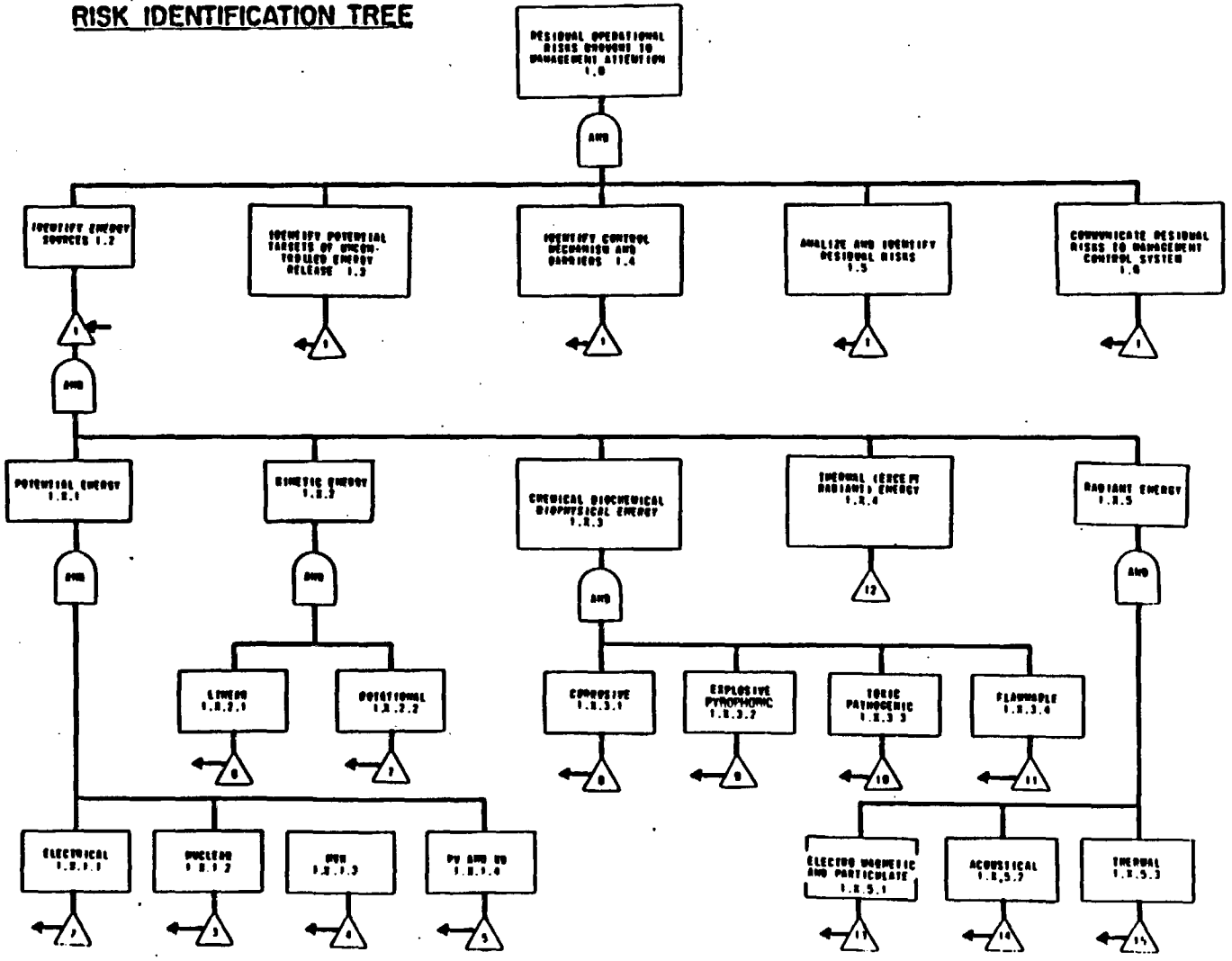
Block 1.0 defines the objective of brining to management attention "Residual Operational Risks" that remain after a risk analysis has been completed, and corrective action has been taken to eliminate and control major risks. Subordinate blocks 1.0 through 5.0 define the necessary and sufficient conditions to achieve fulfillment of the objective stated in Block 1.0. These conditions are:

- All energy sources must be identified
- All potential targets of uncontrolled energy release must be identified for each energy source
- All control mechanisms and barriers to energy release must be identified for each energy source
- An analysis must be performed in each case to determine failure modes and effects, in order to identify the residual risks

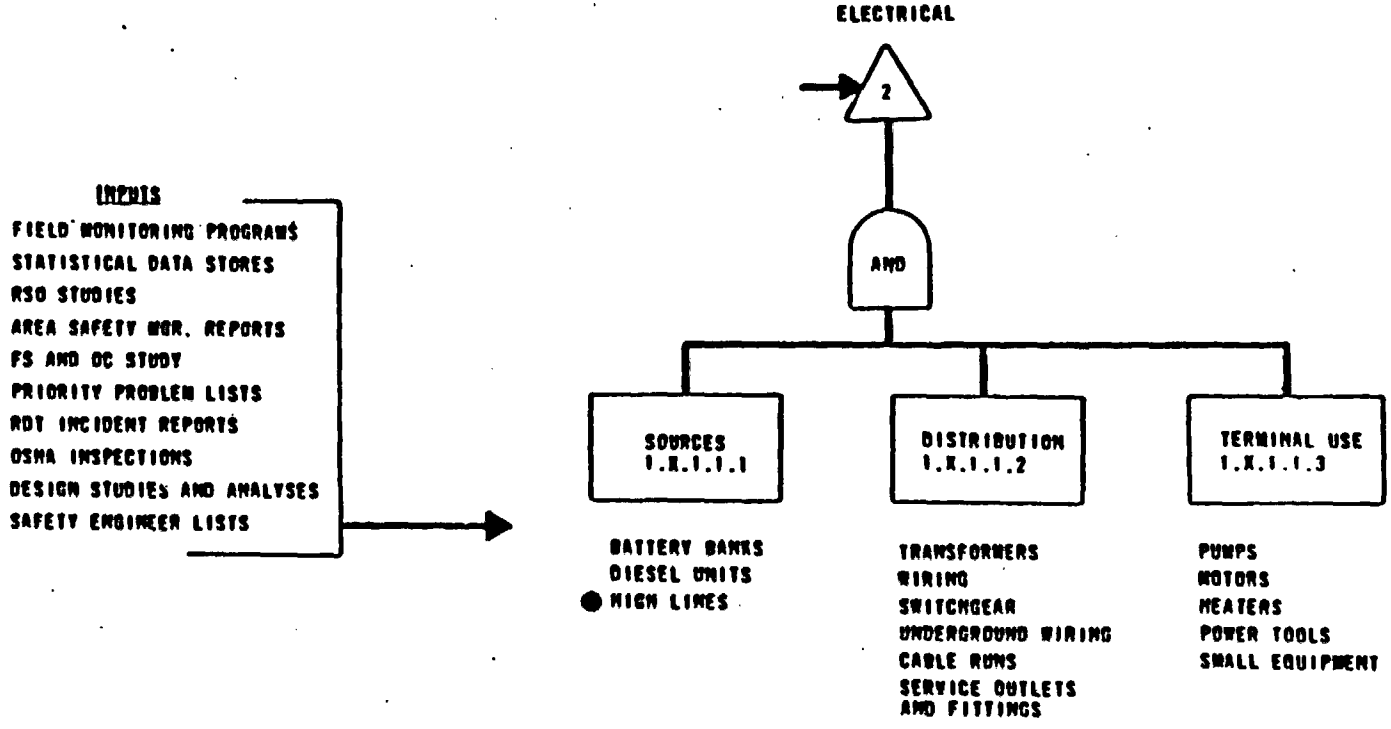
The balance of the tree provides a guide for identifying all energy sources. The two lower tiers on the first page of the example identify the various forms of energy. The transfers relate to tabulations of the specific risk situations that follow. The tabulations are general in nature, but are traceable to specific hardware, locations, and organizational units.

The identifying of all energy sources and the tracing to specific hardware has the primary benefit of preventing oversight of specific hazards. The safety analysis steps required would be time-consuming, therefore the high risk energy sources should be consider first and the use of analytical effort scaled to the degree of risk. The selection and scaling should be made by safety specialists. Although the selection of high risk hazards does not quantify the risk, it will help to prevent oversight of the high risk areas.

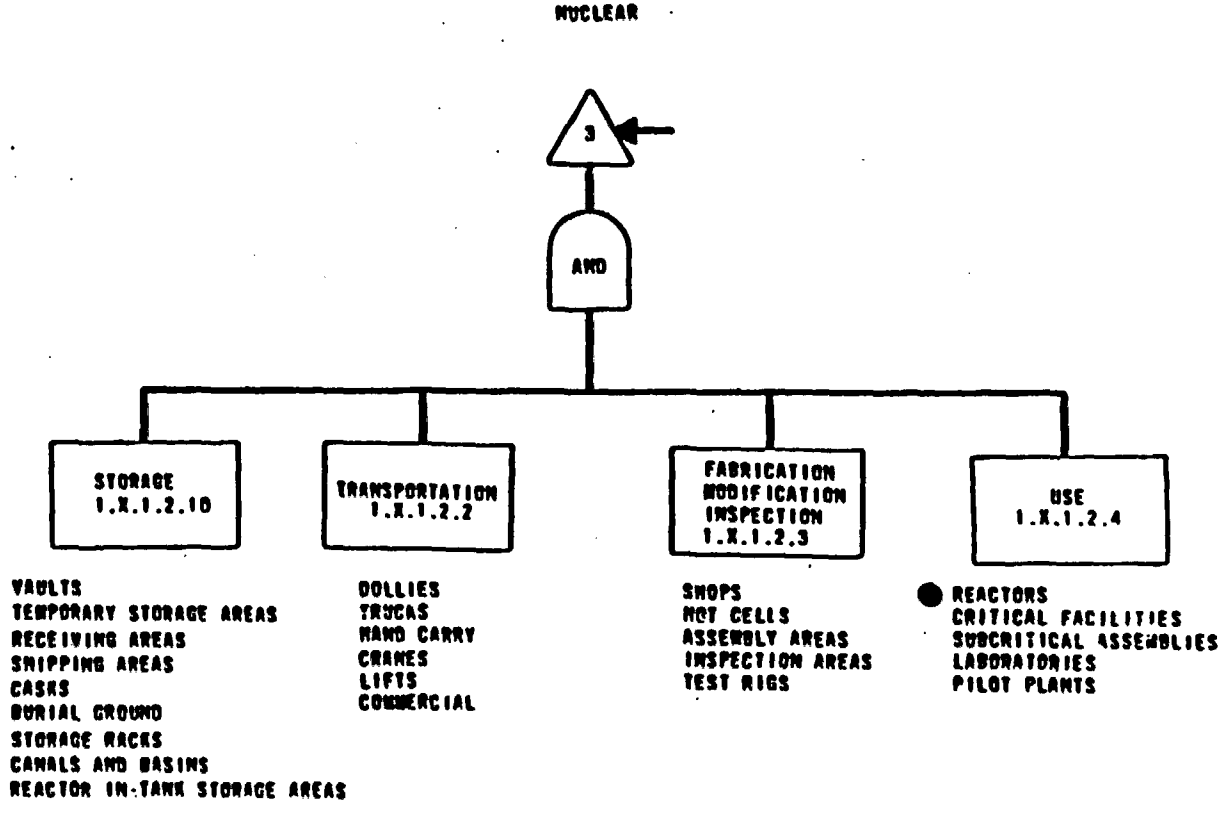
RISK IDENTIFICATION TREE

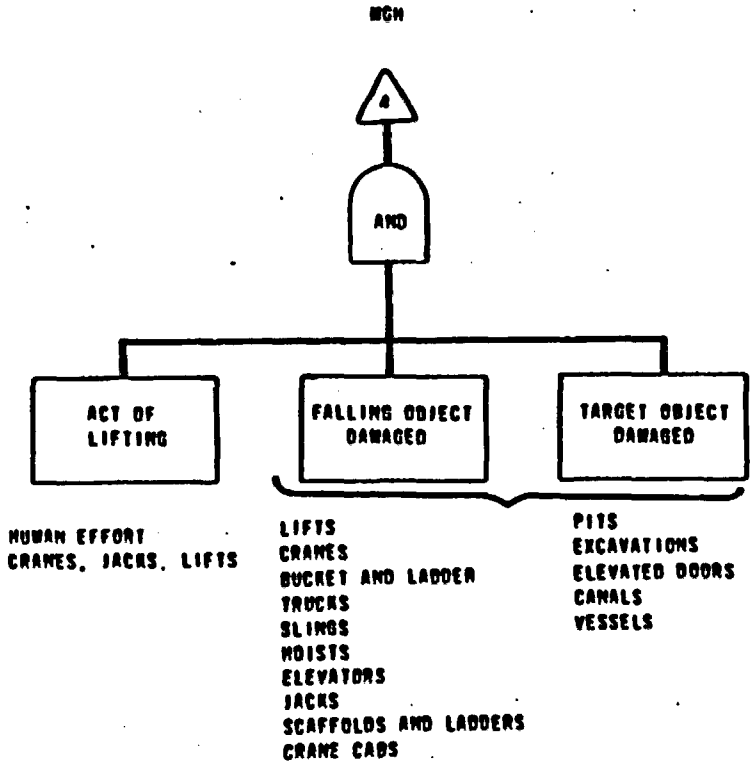


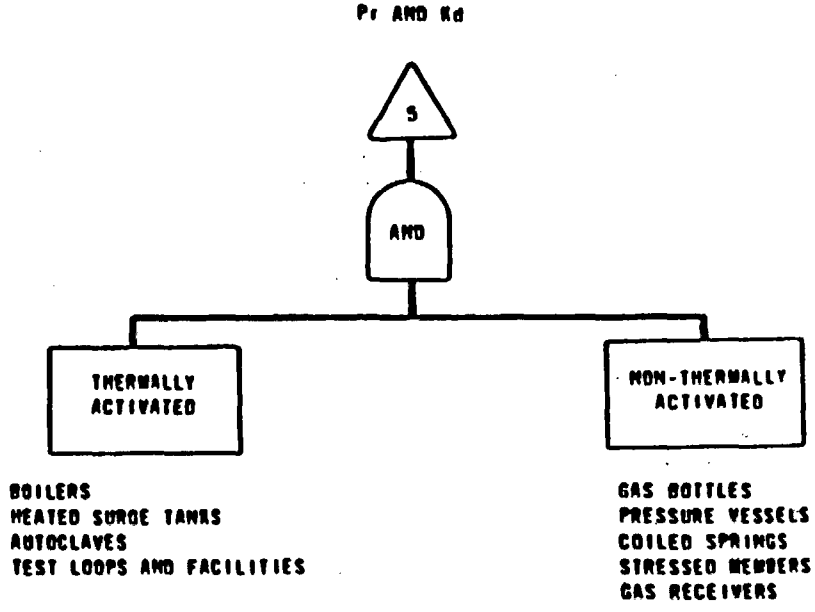
TYPICAL LOWER TIER STRUCTURE
(ENERGY SOURCES GEOGRAPHICALLY FIXED)

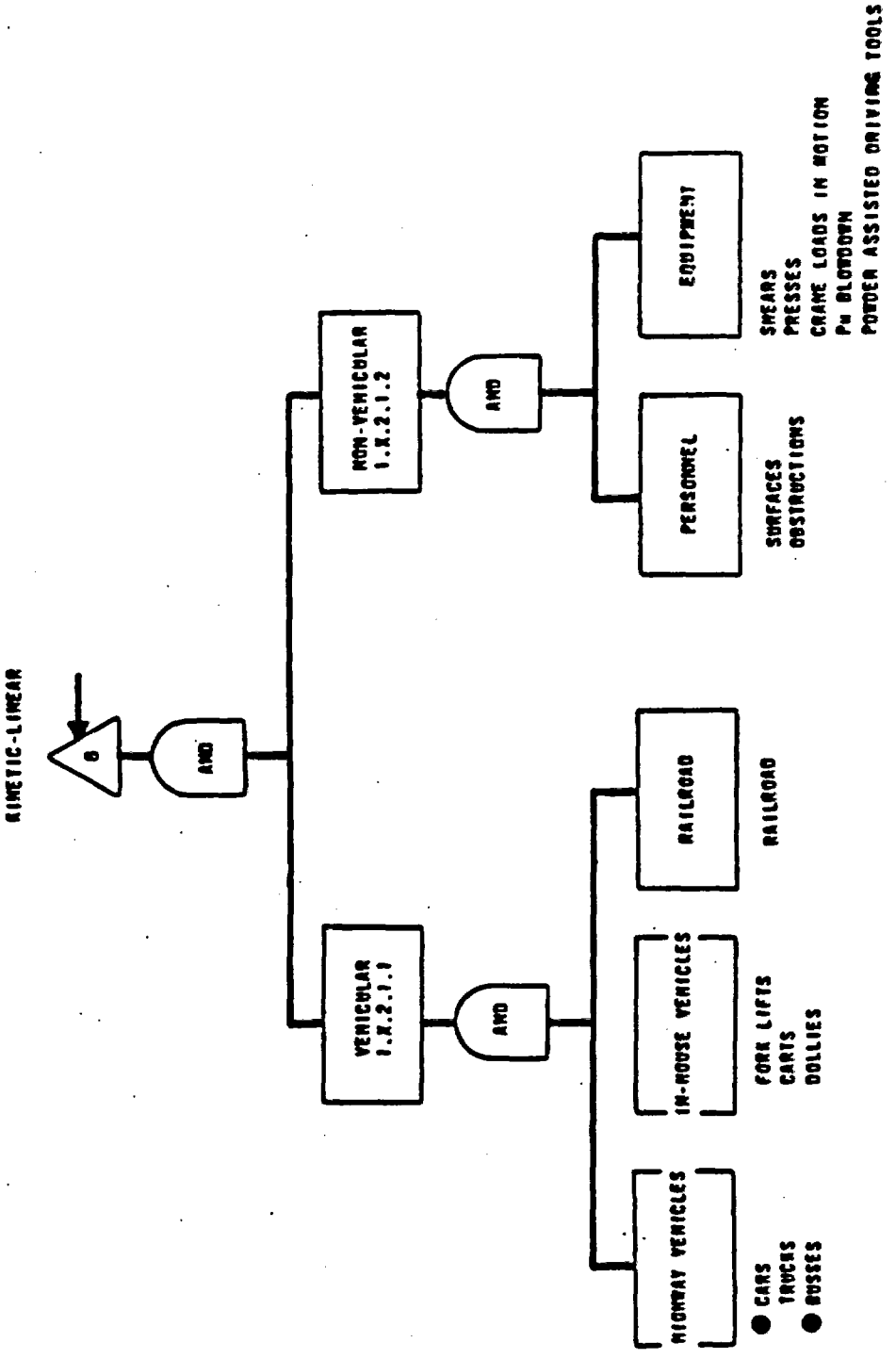


TYPICAL LOWER TIER STRUCTURE
(ENERGY SOURCES GEOGRAPHICALLY MOBILE)




MCH
4
AND
ACT OF LIFTING
FALLING OBJECT DAMAGED
TARGET OBJECT DAMAGED
HUMAN EFFORT
CRANES, JACKS, LIFTS
LIFTS
CRANES
BUCKET AND LADDER
TRUCKS
SLINGS
HOISTS
ELEVATORS
JACKS
SCAFFOLDS AND LADDERS
CRANE CABS
PITS
EXCAVATIONS
ELEVATED DOORS
CANALS
VESSELS


Pr AND Rd
5
AND
THERMALLY ACTIVATED
NON-THERMALLY ACTIVATED
BOILERS
HEATED SURGE TANKS
AUTOCLAVES
TEST LOOPS AND FACILITIES
GAS BOTTLES
PRESSURE VESSELS
COILED SPRINGS
STRESSED MEMBERS
GAS RECEIVERS


KINETIC-LINEAR
G
AND
VEHICULAR
1.X.2.1.1
AND
RAILROAD
RAILROAD
IN-HOUSE VEHICLES
FORK LIFTS
CARTS
DOLLIES
HIGHWAY VEHICLES
CARS
TRUCKS
BUSSES
NON-VEHICULAR
1.X.2.1.2
AND
EQUIPMENT
SHEARS
PRESSES
CRANE LOADS IN MOTION
Pu BLOWDOWN
POWDER ASSISTED DRIVING TOOLS
PERSONNEL
SURFACES
OBSTRUCTIONS

KINETIC-ROTATIONAL

CENTRIFUGES
MOTORS
PUMPS
COOLING TOWER FANS
CAFETERIA EQUIPMENT
LAUNDRY EQUIPMENT
GEARS
SHOP EQUIPMENT (GRINDERS, SAWS, BRUSHES, ETC.)
FLOOR POLISHERS

CORROSIVE

ACIDS
CAUSTICS
"NATURAL" CHEMICALS (SOIL, AIR, WATER)
DECON SOLUTIONS

EXPLOSIVE PYROPHORIC

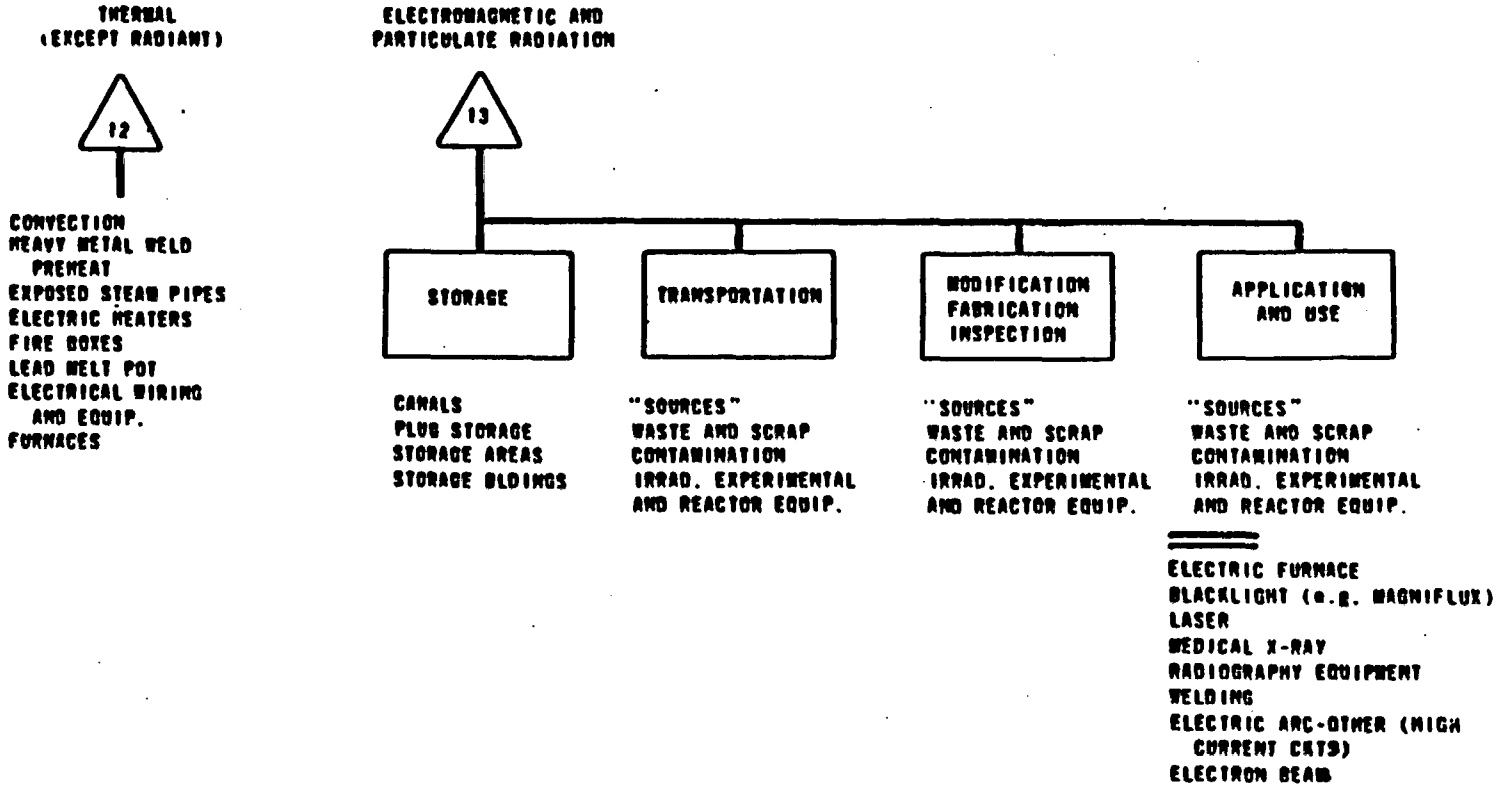
CAPS
PRIMER CORD
DYNAMITE
POWDER METALLURGY
DUSTS
HYDROGEN (INCL. BATTERY BANKS AND WATER DECOMP.)
GASES-OTHER
Gd NITRATE
ELECTRIC SQUIBBS
PEROXIDES-SUPEROXIDES

TOXIC PATHOGENIC

ACETONE
FLOURIDES
Co
LEAD
AMMONIA
ASBESTOS
TRICHLORETHYLENE
DUSTS AND PARTICULATES
PESTICIDES-HERBICIDES-INSECTICIDES
BACTERIA
Be
CHLORINE
DECON SOLUTIONS
SANDBLAST
METAL PLATING
ASPHYXIATION-DROWNING

FLAMMABLE MATERIALS

PACKING MATERIAL
RAGS
GASOLINE (STORAGE AND IN VEHICLES)
LUBE OIL
COOLANT OIL
PAINT SOLVENT
DIESEL FUEL
BUILDINGS AND CONTENTS
TRAILERS AND CONTENTS
GREASE
HYDROGEN-(INCL. BATTERY BANKS)
GASES - OTHER
SPRAY PAINT
SOLVENT VATS


THERMAL
(EXCEPT RADIANT)
12
CONVECTION
HEAVY METAL WELD PREHEAT
EXPOSED STEAM PIPES
ELECTRIC HEATERS
FIRE BOXES
LEAD MELT POT
ELECTRICAL WIRING AND EQUIP.
FURNACES
ELECTROMAGNETIC AND PARTICULATE RADIATION
13
STORAGE
TRANSPORTATION
MODIFICATION FABRICATION INSPECTION
APPLICATION AND USE
CANALS
PLUG STORAGE
STORAGE AREAS
STORAGE BLDINGS
"SOURCES"
WASTE AND SCRAP
CONTAMINATION
IRRAD. EXPERIMENTAL AND REACTOR EQUIP.
"SOURCES"
WASTE AND SCRAP
CONTAMINATION
IRRAD. EXPERIMENTAL AND REACTOR EQUIP.
"SOURCES"
WASTE AND SCRAP
CONTAMINATION
IRRAD. EXPERIMENTAL AND REACTOR EQUIP.
ELECTRIC FURNACE
BLACKLIGHT (e.g. MAGNIFLUX)
LASER
MEDICAL X-RAY
RADIOGRAPHY EQUIPMENT
WELDING
ELECTRIC ARC-OTHER (HIGH CURRENT CKTS)
ELECTRON BEAM


ACOUSTICAL
RADIATION
14
EQUIPMENT NOISE
ULTRASONIC CLEANERS
THERMAL
RADIATION
15
FURNACES
BOILERS
STEAM LINES
LAB AND PILOT
PLANT EQUIP.

APPENDIX E.2_

EXAMPLE OF ROOT-CAUSE ANALYSIS IN INCIDENT INVESTIGATION

INCIDENT: Accidental Halon Discharge in a Process Cabinet

DESCRIPTION OF THE OCCURRENCE:

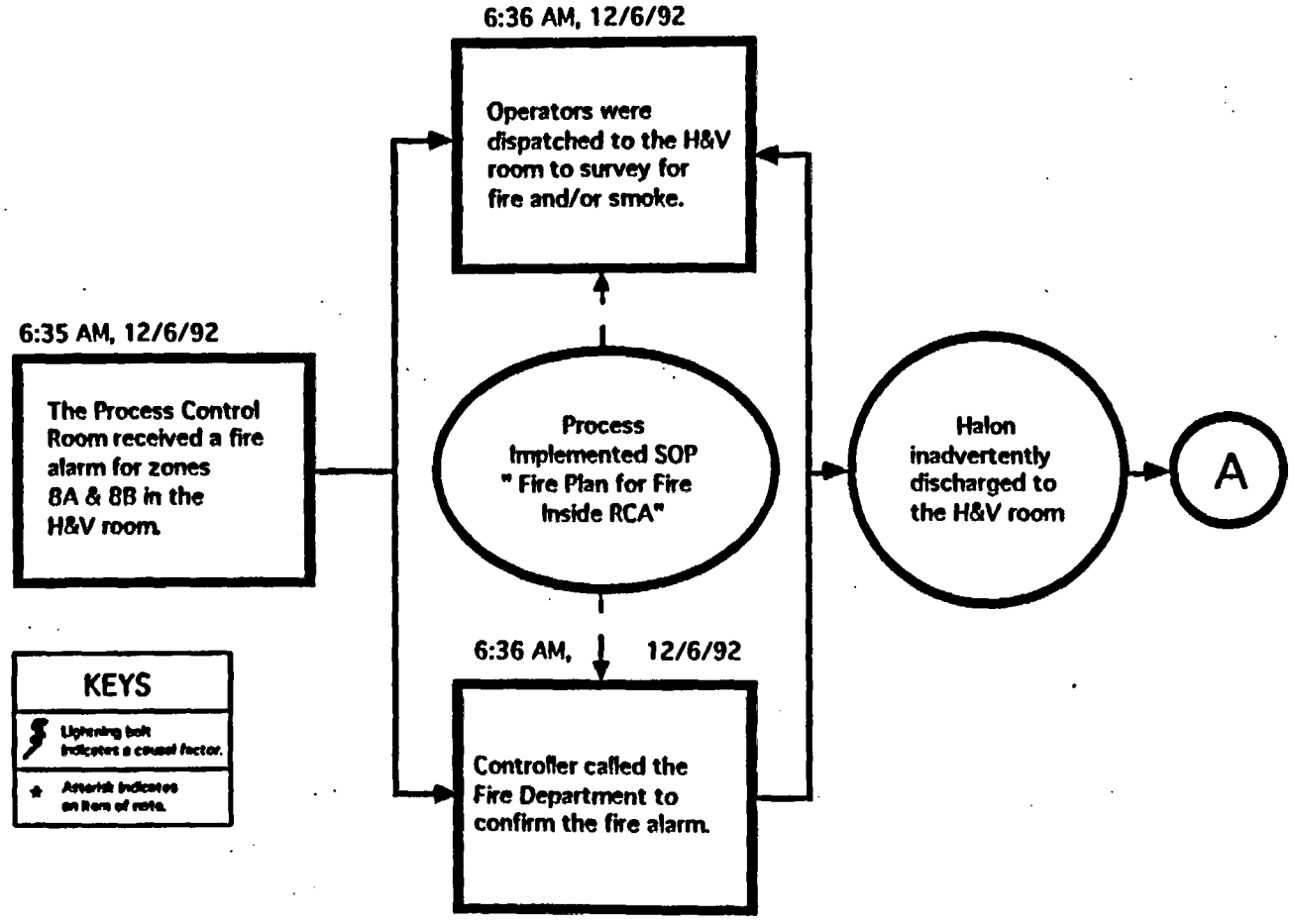
At approximately 6:40 AM on Sunday morning, a fire alarm signal was received in the Control Room. This signal indicated fire in the Zones 8A and 8B H&V Room. All interlocks functioned properly, and the Room Exhausters, Main Air Supply Fans, HVAAM Exhausters shut down automatically. All cabinet exhaust vacuum controllers switched to "Fire Mode". Halon discharged into the H&V Room.

OPERATING CONDITIONS OF FACILITY AT TIME OF OCCURRENCE

The facility was in the operating mode; however, no materials processing was in progress. Shift turnover was in progress.

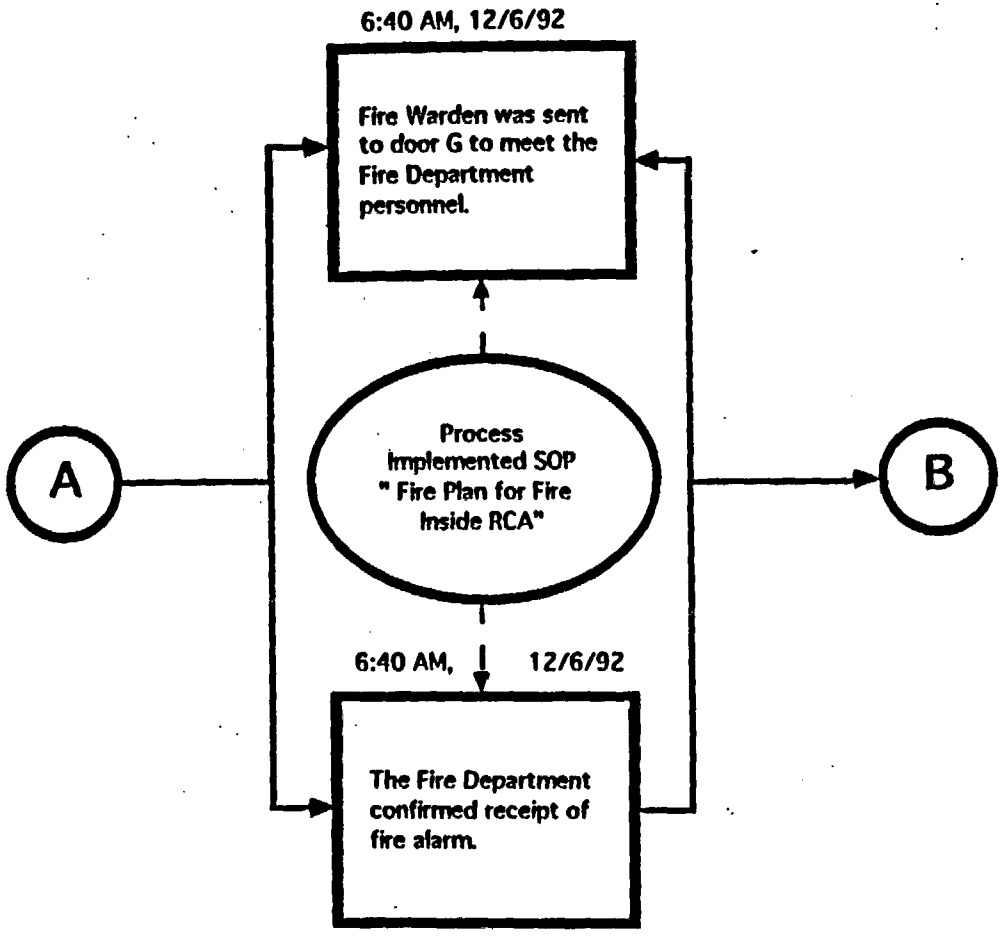
IMMEDIATE ACTIONS TAKEN AND RESULTS:

Upon receipt of the alarm, operators were dispatched to the H&V Room to check for fire and/or smoke. Additional operator were sent to survey the building for any possible cause of the fire alarm. The Fire Warden went to meet Fire Department personnel responding to the alarm. On contacting the Fire Department personnel, the Fire Warden confirmed receipt of a fire alarm and was toldthat the fire truck was on the way. When it was determined that there was no fire, an operator went to the HP Count Room and placed the HVAAM Halon Bypass switch into bypass mode and restarted the HVAAM exhausters. Fire Department personnel confirmed that there was no fire. Fire Department Systems personnel and DC&S were called in to initiate an investigation as to the possible cause of this alarm. During the course of the investigation, it was found that the Halon cylinders which provide coverage to the H&V Room had discharged 583 lbs of Halon into the room.



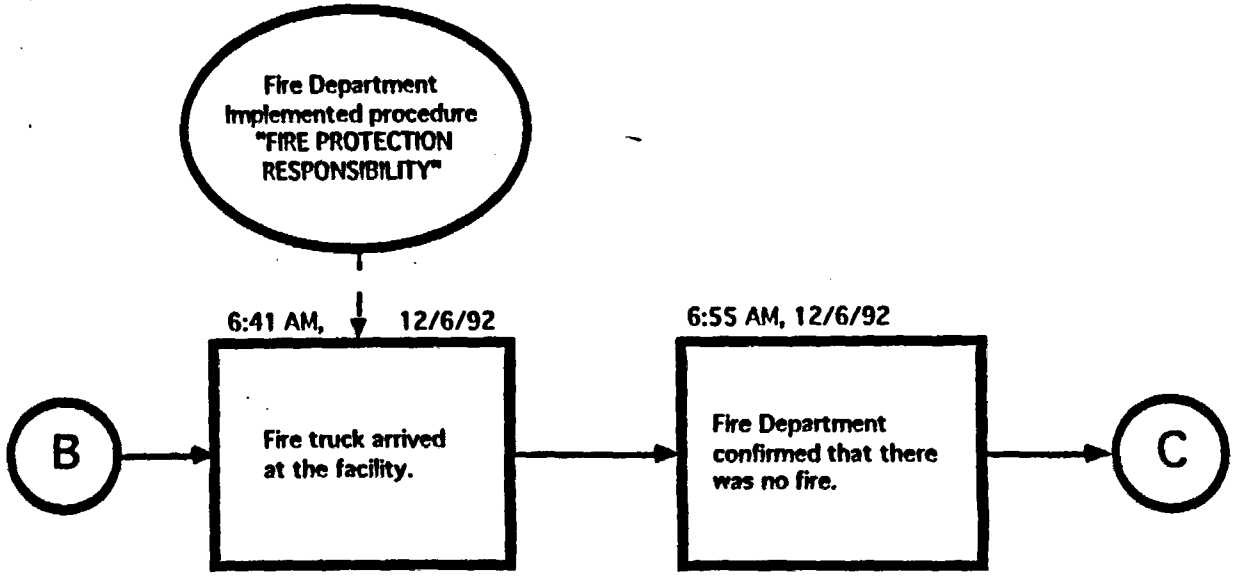
Events and Causal Factors Chart / Page 1 of 7

HALON DISCHARGE



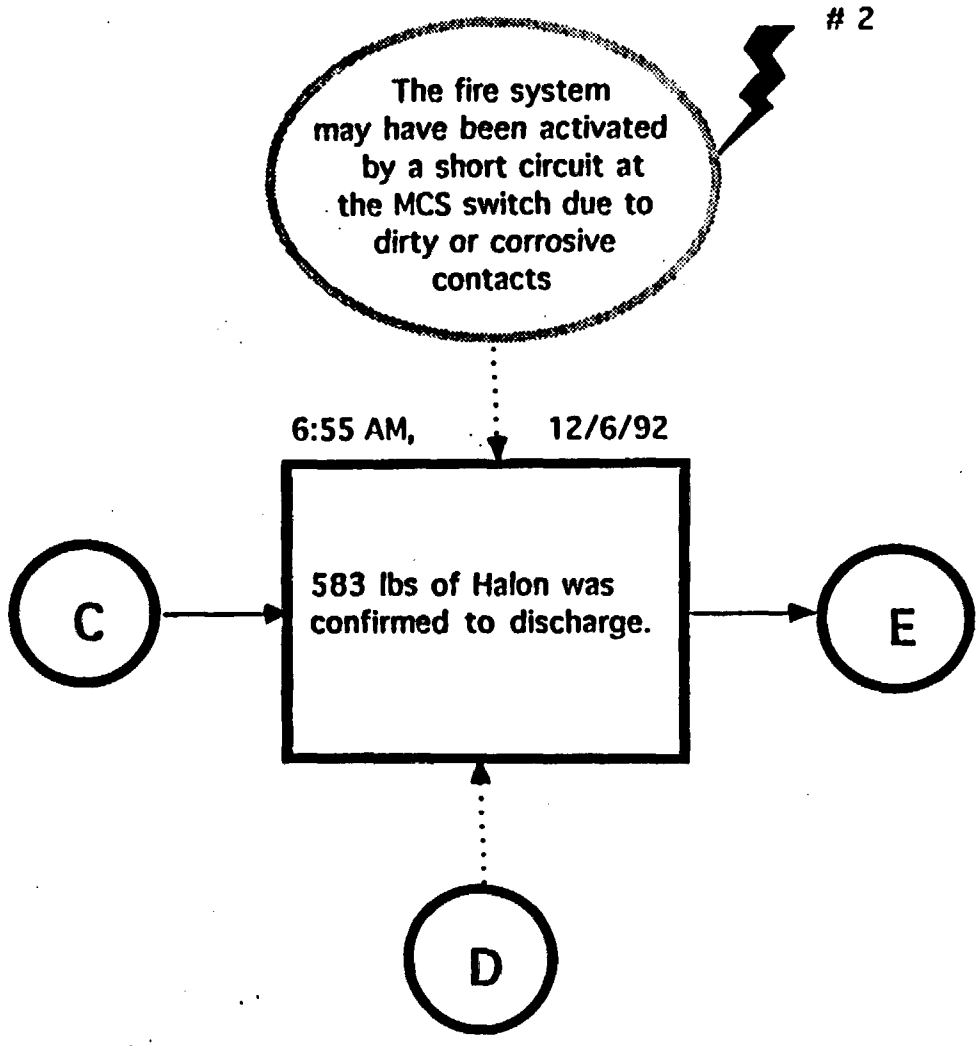
Events and Causal Factors Chart / Page 2 of 7

HALON DISCHARGE

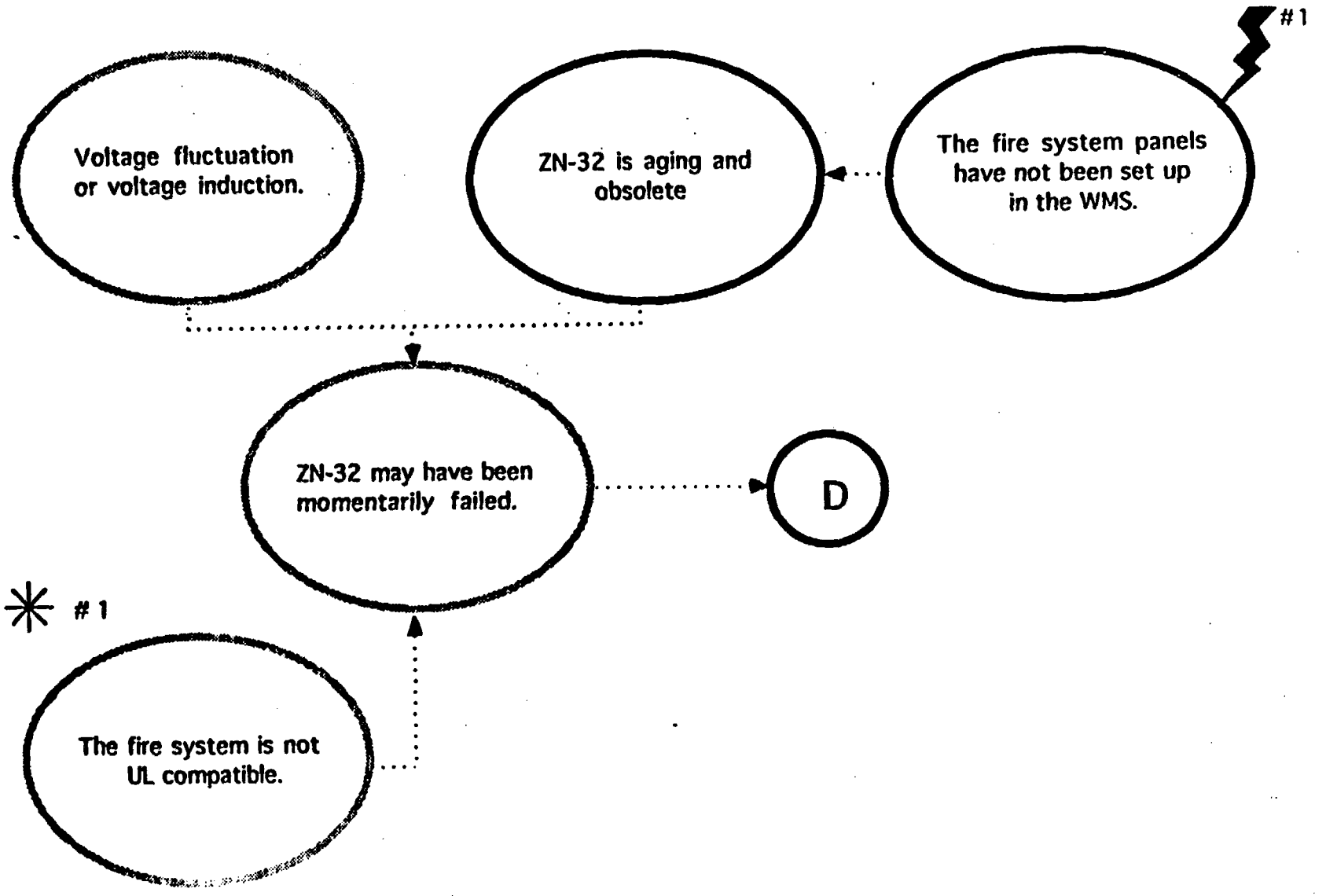


Events and Causal Factors Chart / Page 3 of 7

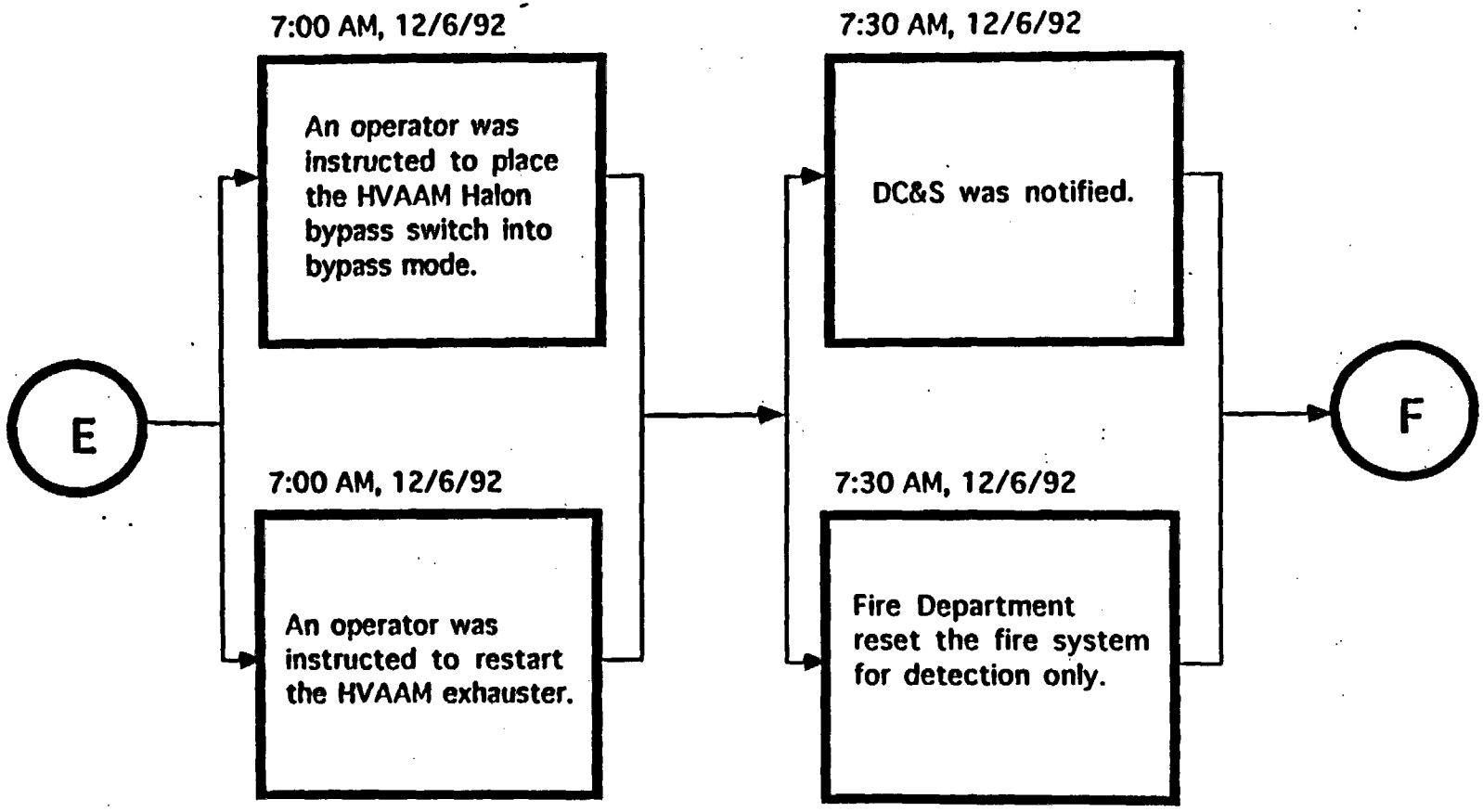
HALON DISCHARGE



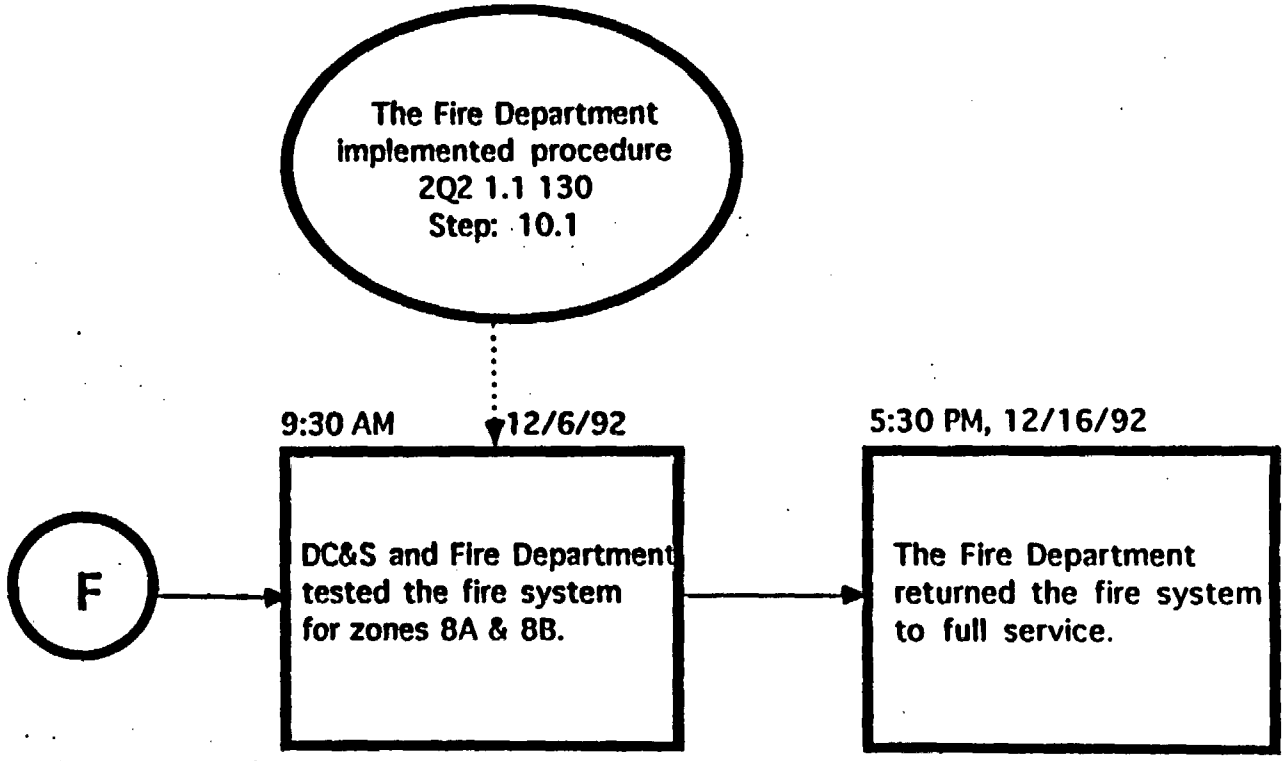
Events and Causal Factors Chart / Page 4 of 7
HALON DISCHARGE



Events and Causal Factors Chart / Page 5 of 7
HALON DISCHARGE



Events and Causal Factors Chart / Page 6 of 7
HALON DISCHARGE



Events and Causal Factors Chart / Page 7 of 7
HALON DISCHARGE

HALON DISCHARGE		
Causal Factor # 1	Paths Through Root Cause Tree	Recommendations
The fire system panels have not been set up in the Work Management System (WMS). **BACKGROUND** During the course of the investigation as to the cause of the Halon release, System Engineer notes that the input module may have been in service for approximately 11 years. Per vendor recommendation, the module should be replaced around 10 years under normal operating condition to maintain its reliability, thereby minimizing the false alarm leading to the activation of Halon release. However, the fire system panels have not been set up in the WMS for routine preventive maintenance.	• Equipment difficulty • Equipment reliability design • Equipment reliability program • Maintenance task requirement • Preventive maintenance for equipment L.T.A. Preventive maintenance program (WMS) was in place. However, the fire system panels were not registered in the program.	This is a presumptive cause of the incident. And it is also a single isolated cause, therefore, System Engineer recommends adding all fire system panels to the WMS, and replacement of the input module for zones 8A and 8B with the new input module ZU-35.

HALON DISCHARGE		
Causal Factor # 2	Paths Through Root Cause Tree	Recommendations
The Manual Control Station (MCS) switch may have short-circuited. **BACKGROUND** This fire suppression system has been installed for approximately 11 yrs, therefore, the MCS switch may be corrosive or dirty due to the ambient humidity and particles.	• Equipment difficulty • Equipment reliability design • Equipment reliability program • Maintenance task requirement • Preventive maintenance for equipment L.T.A. This MCS switch has been installed for approximate 11 yrs based on the print W-721079.	This is a presumptive cause of the incident. And it is also a single isolated cause, therefore, System Engineer recommends cleaning the MCS switch for zones 8A and 8B.

HALON DISCHARGE		
Item of Note #1	Paths Through Root Cause Tree	Recommendations
CP-35 control panel and ZN-32 input module are not UL compatible.. **BACKGROUND** During the course of the investigation as to the cause of Halon release, it was discovered that the fire protection panels in consists of CP-35's and ZN-32's, according to vendor compatibility documents, they are not UL compatible. Per vendor compatibility documents, the current fire protection system does not have an alarm overriding trouble feature, and the module will not supervise while the fire panel is operating on battery during an outage.	• Equipment difficulty • Equipment reliability design • Design • Design review verification • Incomplete review/verification The current fire protection system violates the Functional Performance Requirements 2Q section 4.0 (4.1.a).	System Engineer recommends upgrading all current input modules (ZN-32) to ZU-35 DS.