DEFENSE TECHNICAL INFORMATION CENTER

Information for the Defense Community

DTIC® has determined on 07/29/2010 that this Technical Document has the Distribution Statement checked below. The current distribution for this document can be found in the DTIC® Technical Report Database.

☒ **DISTRIBUTION STATEMENT A.** Approved for public release; distribution is unlimited.

☐ **© COPYRIGHTED**; U.S. Government or Federal Rights License. All other rights and uses except those permitted by copyright law are reserved by the copyright owner.

☐ **DISTRIBUTION STATEMENT B.** Distribution authorized to U.S. Government agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)

☐ **DISTRIBUTION STATEMENT C.** Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)

☐ **DISTRIBUTION STATEMENT D.** Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

☐ **DISTRIBUTION STATEMENT E.** Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

☐ **DISTRIBUTION STATEMENT F.** Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority.

Distribution Statement F is also used when a document does not contain a distribution statement and no distribution statement can be determined.

☐ **DISTRIBUTION STATEMENT X.** Distribution authorized to U.S. Government Agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoDD 5230.25; (date of determination). DoD Controlling Office is (insert controlling DoD office).

Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at www.nrc.gov/NRC/ADAMS/index.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   P. O. Box 37082
   Washington, DC 20402–9328
   www.access.gpo.gov/su_docs
   202–512–1800
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–533–6847 or, locally, 703–805–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/NRC/NUREGS/indexnum.html are updated regularly and may differ from the last printed version.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

NUREG-1624, Rev. 1

Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)

Manuscript Completed: April 2000
Date Published: May 2000

Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

ABSTRACT

This report describes the most recent version of a second-generation human reliability analysis (HRA) method called "A Technique for Human Event Analysis," (ATHEANA), NUREG-1624, Rev.1. ATHEANA is the result of development efforts sponsored by the Probabilistic Risk Analysis Branch in the U.S. Nuclear Regulatory Commission's (NRC)'s Office of Nuclear Regulatory Research. ATHEANA was developed to address limitations identified in current HRA approaches by providing a structured search process for human failure events and unsafe acts, providing detailed search processes for error-forcing context, addressing errors of commission and dependencies, more realistically representing the human-system interactions that have played important roles in accident response, and integrating advances in psychology with engineering, human factors, and PRA disciplines. The report is divided into two parts. Part I introduces the concepts upon which ATHEANA is built and describes the motivation for following this approach. Part 2 provides the practical guidance for carrying out the method. Appendix A provides retrospective ATHEANA-based analyses of significant operating events. Appendices B-E provide sample ATHEANA prospective analyses (HRAs) for four specific human performance issues.

Table of Contents

ABSTRACT iii

EXECUTIVE SUMMARY xv

FOREWORD xxv

ACKNOWLEDGMENTS xxix

1 INTRODUCTION 1-1
- 1.1 Purpose and Organization of this Report 1-1
- 1.2 Background 1-3
- 1.3 Motivation for a New Approach to Human Reliability Analysis 1-6
- 1.4 Benefits from Using ATHEANA 1-9
  - 1.4.1 Overview of the Risk Management Benefits of Using ATHEANA 1-9
  - 1.4.2 Insights from ATHEANA Regarding Risk Management Using PRA 1-11
    - 1.4.2.1 Possible Plant-Specific Insights and Subsequent Improvements 1-12
    - 1.4.2.2 Insights of Possible Value to the NRC and Industry 1-13
    - 1.4.2.3 Insights Regarding Additional Qualitative Benefits from Using ATHEANA 1-14
  - 1.4.3 General Insights 1-14
- 1.5 Other Related HRA Developmental Work 1-15
- 1.6 References 1-17

2 GENERAL DESCRIPTION OF THE ATHEANA METHOD 2-1
- 2.1 The Multidisciplinary HRA Framework 2-1
  - 2.1.1 Error-Forcing Context 2-2
  - 2.1.2 "Human Error" 2-3
  - 2.1.3 The PRA Model 2-5
- 2.2 The Approach for Analysis using ATHEANA 2-6
- 2.3 References 2-8

3 THE IMPORTANCE OF PLANT CONDITIONS AND CONTEXT IN HUMAN PERFORMANCE 3-1
- 3.1 Current HRA and PRA Perspective 3-1
- 3.2 The Significance of Context 3-2
- 3.3 Examples of the Effects of Plant Conditions and Context on Operations 3-5
  - 3.3.1 ATHEANA Reviews of Events 3-5
  - 3.3.2 Other Analyses of Operational Events 3-8
- 3.4 References 3-8

Table of Contents (Cont.)

4 BEHAVIORAL SCIENCE PERSPECTIVE 4-1
4.1 Analysis of Operator Cognitive Performance 4-1
4.1.1 Situation Assessment 4-1
4.1.2 Monitoring and Detection 4-4
4.1.3 Response Planning 4-5
4.1.4 Response Implementation 4-6
4.2 Cognitive Factors Affecting Operator Performance 4-6
4.2.1 Knowledge Factors 4-7
4.2.2 Processing Resource Factors 4-7
4.2.3 Strategic Factors 4-9
4.3 Failures in Operator Cognitive Activity 4-10
4.3.1 Failures in Monitoring or Detection 4-10
4.3.2 Failures in Situation Assessment 4-11
4.3.3 Failures in Response Planning 4-14
4.3.4 Failures in Response Implementation 4-17
4.4 Contributing Elements of Error-Forcing Contexts in Power-Plant Operations .. 4-17
4.4.1 Characteristics of Parameters and Scenarios 4-18
4.4.1.1 Parametric Influences 4-19
4.4.1.2 Scenario Influences 4-20
4.5 Conclusions 4-20
4.6 References 4-21
4.7 Bibliography of Cognitive Psychology Literature Relevant to ATHEANA 4-22

5 OPERATIONAL EXPERIENCE ILLUSTRATING ATHEANA PRINCIPLES 5-1
5.1 Contributions of Humans and Error-Forcing Contexts in Past Operational Experience 5-2
5.1.1 Plant Conditions and PSFs 5-2
5.1.2 Failures in Information Processing Stages 5-3
5.2 Analysis of Error-Forcing Context 5-4
5.2.1 Error-Forcing Context and Unsafe Actions 5-5
5.2.1.1 Error-Forcing Context in Detection 5-5
5.2.1.2 Error-Forcing Context in Situation Assessment 5-6
5.2.1.3 Error-Forcing Context in Response Planning 5-10
5.2.1.4 Error-Forcing Context in Response Implementation 5-12
5.2.2 Performance-Shaping Factors 5-12
5.2.3 Important Lessons from Analyses of Events 5-14
5.3 An Operational Event Example Illustrating Dependency Effects 5-21
5.4 Summary 5-27
5.5 References 5-27

Table of Contents (Cont.)

6 OVERVIEW OF THE ATHEANA PROCESS 6-1
6.1 Road Map to Part 2 6-1
6.2 Summary of Retrospective ATHEANA Analysis 6-2
6.3 Summary of Prospective ATHEANA Analysis 6-3
6.4 The ATHEANA Prospective Process: An Evolutionary Extension of Existing HRA Methods 6-10
6.4.1 Summary 6-15
6.5 References 6-15

7 PREPARATION FOR APPLYING ATHEANA 7-1
7.1 Select the Analysis Activity 7-1
7.2 Assemble and Train the Multidisciplinary Team 7-1
7.3 Collect Background Information 7-3
7.3.1 Review and Collection of Anecdotal Experience 7-5
7.3.2 Additional Plant-Specific Information Needed for ATHEANA 7-10
7.3.3 Other Information Needed Later in ATHEANA 7-11
7.4 Prepare to Conduct Simulator Exercises 7-12
7.5 Conclusion 7-14
7.6 References 7-14

8 RETROSPECTIVE ANALYSIS 8-1
8.1 Overview 8-1
8.2 Identify and Describe the Undesired Event 8-3
8.3 Identify the Functional Failures, the HFEs, and the UAs 8-3
8.4 Identify the Causes of the UAs 8-5
8.4.1 Information Processing Failures 8-5
8.4.2 Performance-Shaping Factors 8-7
8.4.3 Significant Plant Conditions 8-7
8.5 Drawing Conclusions 8.8
8.6 Document the Results of the Analysis 8-8
8.7 References 8-8

9 DETAILED DESCRIPTION OF PROCESS 9-1
9.0 Introduction 9-1
9.1 Step 1: Define and Interpret the Issue 9-1
9.1.1 Guidance for Step 1 9-4
9.1.2 Products of Step 1 9-5
9.2 Step 2: Define the Scope of the Analysis 9-5
9.2.1 Guidance for Step 2 9-5
9.2.2 Products of Step 2 9-12
9.3 Step 3: Describe the Base Case Scenario 9-12
9.3.1 Overview of Step 3 9-13
9.3.2 Detailed Guidance for Step 3 9-17

Table of Contents (Cont.)

9.3.2.1 Identify and Describe the Consensus Operator Model 9-18
9.3.2.2 Identify and Describe Relevant Reference Analyses 9-18
9.3.2.3 Describe Modifications to Reference Analyses 9-18
9.3.2.4 Describe Possible Scenarios for the Selected Initiator (if no Reference Analysis) 9-19
9.3.2.5 Describe the Base Case Scenario 9-20
9.3.3 Product of Step 3 9-21
9.4 Step 4: Define HFE(s) and/or UAs 9-21
9.4.1 Guidance for Step 4 9-24
9.4.1.1 Defining HFEs 9-24
9.4.1.2 Defining Unsafe Actions 9-30
9.4.2 Products of Step 4 9-34
9.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base 9-34
9.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario 9-35
9.5.2 Time Frames of Interest 9-39
9.5.3 Operator Tendencies and Informal Rules 9-41
9.5.4 Evaluation of Formal Rules and Emergency Operating Procedures 9-41
9.5.5 Product of Step 5 9-46
9.6 Step 6: Search for Deviations from the Base Case Scenario 9-46
9.6.1 Overview of Step 6 9-47
9.6.2 Tools Underlying the Search Schemes 9-49
9.6.3 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario 9-50
9.6.4 Search of Relevant Rules 9-54
9.6.5 Search for Support System Dependencies 9-55
9.6.6 Search for Operator Tendencies and Error Types 9-56
9.6.7 Develop Descriptions of Deviation Scenarios 9-57
9.6.8 Products of Step 6 9-59
9.7 Identify and Evaluate Complicating Factors and Links to PSFs 9-59
9.7.1 PSFs 9-61
9.7.2 Additional Physical Conditions 9-63
9.7.3 Reintegration of the Deviation Scenario Description 9-64
9.7.4 Products of Step 7 9-65
9.8 Step 8: Evaluate the Potential for Recovery 9-65
9.8.1 Guidance for Step 8 9-66
9.8.2 Reintegration of the Deviation Scenario after Recovery 9-67
9.8.3 Product of Step 8 9-67
9.9 References 9-72

10 ISSUE RESOLUTION 10-1
10.1 Process for Issue Resolution 10-1
10.2 Guidance for Quantification 10-2
10.2.1 Formulation of Quantification 10-2

Table of Contents (Cont.)

10.2.2 Quantification Process 10-3
10.2.2.1 Quantification of EFCs 10-3
10.2.2.2 Quantification of Unsafe Actions 10-7
10.2.2.3 Quantification of Recovery 10-14
10.2.3 Representation of Uncertainties 10-17
10.3 Guidance for PRA Incorporation of HFEs 10-17
10.3.1 Overview of the Typical PRA Model 10-18
10.3.2 Treatment of Human Failure Events in Existing PRAs 10-18
10.3.2.1 Human-Induced Initiating Events 10-19
10.3.2.2 Human Failure Events in Event Trees 10-19
10.3.2.3 Human Failure Events in Fault Trees 10-19
10.3.2.4 Failures to Perform Specific Recovery Actions 10-22
10.3.3 Incorporating ATHEANA Human Failure Events in the PRA Model 10-22
10.3.3.1 Human-Induced Initiating Events 10-22
10.3.3.2 Human Failure Events in Event Trees 10-23
10.3.3.3 Human Failure Events in Fault Trees 10-24
10.3.3.4 Failures to Perform Specific Recovery Actions 10-25
10.3.3.5 Overall Sequence Quantification Considerations 10-26
10.4 References 10-26

11 PERSPECTIVE ON ATHEANA 11-1

APPENDIX A REPRESENTATIONS OF SELECTED OPERATIONAL EVENTS FROM AN ATHEANA PERSPECTIVE A-1

APPENDIX B ATHEANA EXAMPLE - DEGRADATION OF SECONDARY COOLING B-1

APPENDIX C ATHEANA EXAMPLE - LARGE LOSS OF COOLANT ACCIDENT (LLOCA); A "DIRECT INITIATOR SCENARIO" C-1

APPENDIX D ATHEANA EXAMPLE - LOSS OF SERVICE WATER EVENT D-1

APPENDIX E ATHEANA EXAMPLE - SMALL LOSS OF COOLANT ACCIDENT (SLOCA) A "DIRECT INITIATOR SCENARIO" E-1

APPENDIX F DISCUSSION OF COMMENTS FROM A PEER REVIEW OF A TECHNIQUE FOR HUMAN EVENT ANALYSIS (ATHEANA) F-1

APPENDIX G GLOSSARY OF GENERAL TERMS FOR ATHEANA G-1

List of Figures

Figure		Page
2.1	Multidisciplinary HRA Framework	2-2
4.1	Major Cognitive Activities Underlying NPP Operator Performance	4-2
5.1	Oconee 3 Loss of Cooling	5-23
5.2a	Event Information	5-24
5.2b	Summary of Human Actions	5-25
5.2c	Event Dependencies	5-26
6.1	ATHEANA Prospective Search Process	6-4
8.1	TMI-2 Represented in ATHEANA Framework	8-2
8.2	Crystal River Unit 1 Represented in ATHEANA Framework	8-6
9.1	ATHEANA Prospective Search Process	9-2
9.1a	Key for the Meaning of the Box Shapes in Figures 9.1 - 9.6	9-3
9.2	Step 2 - Describe the Scope of the Analysis	9-6
9.3	Step 3 - Describe Base Case Scenario	9-15
9.4	Step 5 - Identify Potential Vulnerabilities	9-35
9.5	Step 6 - Search for Deviations from Base Case Scenario	9-48
9.6	Step 7 - Evaluate Complicating Factors	9-60
10.1	Representation of Estimation of UA Probability	10-10
10.2	Overview of PRA Modeling	10-20
10.3	Overview of PRA Modeling with HFE Interfaces Shown	10-20
10.4	Illustration of HFEs in Event Trees	10-21
10.5	Illustration of HFEs in Fault Trees	10-21
10.6	Illustration of Failure-to-Recover Events in Cut Sets	10-23
10.7	Illustration of Incorporating an ATHEANA HFE in an Event Tree	10-25
B.1	Large LOCA Event Tree	B-3
B.2	Loss of Main Feedwater Event Tree	B-3
B.3	T_{avg} During Loss of Main Feed.	B-7
B.4	Pressurizer Volume During Loss of Main Feed.	B-7
B.5	Steam Generator Water Level During Loss of Main Feed.	B-7
B.6	Power Level vs. Time	B-9
B.7	Turbine Pressure vs. Time	B-9
B.8	Instrument Air Pressure vs. Time	B-9
B.9	Service Water Pressure vs. Time	B-9
B.10	RCS Conditions vs. Time	B-10
B.11	Steam Generator Status vs. Time	B-10
B.12	Containment Conditions vs. Time	B-10
B.13	EOP Highlights Related to Loss of Main Feed Scenario	B-17
B.14a	RCS Response vs. Time	B-34
B.14b	SG Response vs. Time	B-34
B-15	Plant Status After HFE Occurs	B-41
C.1	Core Power during LLOCA Reference Case	C-4
C.2	Break Flow Rate during LLOCA Reference Case	C-4

List of Figures (Cont.)

Figure		Page
C.3	Core Pressure during LLOCA Reference Case	C-4
C.4	Containment Pressure during LLOCA Reference Case	C-4
C.5	Safety Injection Flow during LLOCA Reference Case	C-4
C.6	Accumulator Flow (Blowdown) during LLOCA Reference Case	C-4
C.7	Reflood Rate during LLOCA Reference Case	C-5
C.8	Reflood Transient Water Level during LLOCA Reference Case	C-5
C.9	Peak and Average Clad Temperature during LLOCA Reference Case	C-5
C.10	Observable Parameters during LLOCA Reference Case	C-7
C.11	Large LOCA PRA Event Tree	C-8
C.12	Large LOCA Functional Event Tree	C-9
C.13	EOP Map for Base Case LLOCA (Sheet 1)	C-34
C.14	Observable Parameters during "No" LLOCA Deviation (<DBA) Case	C-16
C.15	"No" LLOCA Deviation (<DBA) Procedure Map (Sheet 1)	C-48
C.16	Observable Parameters during LLOCA "Switching" Deviation Case	C-21
D.1	Power Level vs. Time	D-6
D.2	Turbine Pressure vs. Time	D-6
D.3	Instrument Air Pressure vs. Time	D-6
D.4	Service Water Pressure vs. Time	D-6
D.5	RPV Level vs. Time	D-7
D.6	Containment Conditions vs. Time	D-7
D.7	Four Loss of Service Water Procedures	D-14
D.8	EOP EP-2	D-15
D.9	EOP EP-3	D-16
D.10	Loss of Service Water Event Tree	D-28
E.1	RCS Depressurization Transient during 3-inch SLOCA Reference Case	E-8
E.2	Pumped Safety Injection Flow during 3-inch SLOCA Reference Case	E-8
E.3	Core Mixture Height during 3-inch SLOCA Reference Case	E-8
E.4	Clad Temperatures Transient during 3-inch SLOCA Reference Case	E-8
E.5	Core Steam Flow during 3-inch SLOCA Reference Case	E-8
E.6	Hot Spot Fluid Temperature during 3-inch SLOCA Reference Case	E-8
E.7	Core Power during 3-inch SLOCA Reference Case	E-9
E.8	Comparison of Depressurization Transients for Three SBLOCA Sizes	E-10
E.9	Observable Parameters during SLOCA Reference Case	E-11
E-10	Small LOCA PRA Event Tree	E-13
E.11	Small LOCA Functional Event Tree	E-15
E.12	EOP Map of Base Case SLOCA (Sheet 1)	E-60
E.13	Observable Parameters during Pressurizer Steam Space SLOCA Deviation Case	E-29
E.14	"Growing" SLOCA Deviation Case	E-34

List of Tables

Table		Page
5.1	Examples of Detection Failures	5-6
5.2	Examples of Situation Assessment Failures	5-7
5.3	Examples of Response Planning Failures	5-11
5.4	Examples of Response Implementation Failures	5-13
5.5	Examples of PSFs on Cognitive and Physical Abilities	5-15
5.6	Characteristics of Serious Accidents and Event Precursors	5-18
5.7	Factors Not Normally Considered in PRAs	5-19
9.1	Generic List of Initiating Event Classes and Associated Initiators	9-8
9.2	ATHEANA-Suggested Characteristics of High-Priority Initiators or Accident Sequences	9-10
9.3	ATHEANA-Suggested Characteristics of High Priority Systems and Functions	9-11
9.4	Development of the Base Case Scenario	9-16
9.5	Examples of Base Case Scenario Development	9-22
9.6	Functional Failure Modes Based upon PRA Requirements	9-26
9.7	Examples of Likely Human Failures and Human Failure Modes by PRA Functional Failure Mode	9-28
9.8	Example Unsafe Actions for Generalized Equipment Functional Failure Modes	9-31
9.9a	Possible EOCs for Systems or Equipment that Automatically Start or Stop	9-73
9.9b	Possible EOCs for Continuation of Operation or No Operation of Systems and Equipment	9-74
9.9c	Possible EOCs or EOOs for Manual Actuation and Control of Systems and Equipment	9-75
9.9d	Possible EOOs for Backup (i.e., Recovery) of Failed Systems and Equipment	9-76
9.9e	Possible EOCs or EOOs for Failures of Passive Systems and Components	9-76
9.10	Event Characteristics and Potential Vulnerabilities	9-38
9.11	Relevant Time Frames for the Examples of Appendices B and C	9-40
9.12a	Summary of Operator Action Tendencies (PWRs)	9-42
9.12b	Summary of Operator Action Tendencies (BWRs)	9-43
9.13	Examples of Informal "Rules" Used by Operators	9-45
9.14	Failures in Response Implementation	9-52
9.15a	Scenario Characteristics and Description	9-77
9.15b	Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors	9-79
9.16a	Questions to Identify Scenario Relevant Parameter Characteristics (Table to be used with Table 9.16b)	9-87
9.16b	Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Table to be used following Table 9.16a)	9-93
9.17	Examples of Hardware Failures, Configuration Problems, or Unavailabilities	9-64
9.18	Examples of Information (i.e., Transmit) Problems	9-68
9.19	Physics Algorithms in Instruments that Can Confuse Operators	9-69

List of Tables (Cont.)

Table		Page
9.20	Examples of Plant Conditions in Which the Plant Physics or Behavior Can Confuse Operators	9-70
9.21	Other Plant Conditions that Can Confuse Operators	9-71
10.1	HEART Generic Task Failure Probabilities	10-11
10.2	HEART Performance-Shaping Factors	10-11
10.3	Potential Recovery Opportunities, Oconee, 1991	10-15
10.4	Recovery Opportunities vs. Actions Taken	10-16
B.1	Characteristics of Base Case Scenario	B-4
B.2	Relevant Time Frames for the Loss of MFW Scenario	B-14
B.3	Loss of MFW Initiating Event / Scenario Deviation Considerations	B-21
B.4	Results of the Loss of Main Feed Initiating Event: Scenario Deviation Analysis	B-23
B.5	Results of Relevant Rule Deviation Analysis	B-27
B.6	Results of the System Dependency Deviation Analysis	B-31
B.7	Summary of Deviations Involving Operator Tendencies	B-34
B.8	Deviation Scenarios	B-37
B.9	Scenario Progression Log Regarding Possible Recovery from HFEs	B-42
C.1	Characteristics of the Base Case Scenario	C-2
C.2	Time Frames for the Base Case Large LOCA	C-11
C.3	Summary of Potential Vulnerabilities for LLOCA	C-14
C.4	Application of Guide Words to LLOCA Deviation Analysis	C-26
C.5	Results of LLOCA Deviation Analysis	C-27
C.6	"Switching" LLOCA Deviation Scenario	C-30
D.1	Base Case Scenario Characteristics	D-3
D.2	Relevant Time Frames for the Loss of Service Water Scenario	D-12
D.3	Summary of Potential Vulnerabilities for Loss of Service Water	D-19
D.4	Loss of Service Water Initiating Event / Scenario Deviation Considerations	D-20
D.5	Results of the Loss of Service Water Initiating Event/Scenario Deviation Analysis	D-21
D.6	Loss of Service Water Scenario Summary	D-25
E.1	Probability of k Failures in Systems of Various Size (p=0.001)	E-2
E.2	Step 3: Describe the Base Case Scenario	E-5
E.3	Time Frames for the Base Case SLOCA	E-19
E.4	Summary of Potential Vulnerabilities for SLOCA	E-23
E.5	Application of Guide Words to SLOCA Deviation Analysis	E-39
E.6	Results of SLOCA Deviation Analysis	E-40
E.7	Results of the EOP/Informal Rule Deviation Analysis	E-45
E.8	Results of System Dependency Deviation Analysis	E-49
E.9	Deviation Scenarios	E-51

EXECUTIVE SUMMARY

This report describes the most recent version of a second-generation human reliability analysis (HRA) method called "A Technique for Human Event Analysis" (ATHEANA). ATHEANA is the result of development efforts sponsored by the Probabilistic Risk Analysis (PRA) Branch in the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research (RES).

ATHEANA was developed to increase the degree to which an HRA can represent the kinds of human behaviors seen in accidents and near-miss events at nuclear power plants and at facilities in other industries that involve broadly similar kinds of human/system interactions. In particular, ATHEANA provides this improved capability by:

- more realistically searching for the kinds of human/system interactions that have played important roles in accident responses, including the identification and modeling of errors of commission and dependencies

- taking advantage of, and integrating, advances in psychology, engineering, plant operations, human factors, and probabilistic risk assessment (PRA) disciplines in its modeling

ATHEANA: An HRA Method and an Event Analysis Tool

In general, ATHEANA provides a useful structure for understanding and improving human performance in operational events. As described in this report, ATHEANA originates from a study of operational events and from an attempt to reconcile observed human performance in the most serious of these events with existing theories of human cognition and human reliability models, within the context of plant design, operation, and safety.

More specifically, ATHEANA provides the following:

- An improved process for performing HRA/PRA, providing further rigor and structure to HRA/PRA tasks. Some of these tasks are already performed (e.g., identification of human failure events (HFEs) to include in PRA models), but not as explicitly or thoroughly as ATHEANA specifies.

- A method for obtaining qualitative and quantitative HRA results. The premise of the ATHEANA HRA method is that significant human errors occur as a result of "error-forcing contexts" (EFCs), defined as combinations of plant conditions and other influences that make operator error very likely. ATHEANA is distinctly different in that it provides structured search schemes for finding such EFCs, by using and integrating knowledge and experience in engineering, PRA, human factors, and psychology with plant-specific information and insights from the analysis of serious accidents.

- An event analysis perspective and a tool for event analysis that can support the ATHEANA HRA process, or can be an end to itself. The ATHEANA event analysis perspective and tool is also

based upon the integration of multiple disciplines and feedback from the analyses of many events, both nuclear power plant (NPP) and non-NPP events. (Event analyses performed for NPP events have included full-power, startup, and low-power and shutdown conditions.)

This report provides guidance on how to apply the ATHEANA retrospective (i.e., event analysis) and prospective (i.e., HRA) approaches, and describes an overall process that includes analyst preparatory tasks and the retrospective and prospective analyses. This report also provides examples of retrospective and prospective analyses in the appendices.

Motivation for Developing an Improved Human Reliability Analysis Capability

There were several motivators for developing ATHEANA, but the most compelling were that:

- the human events modeled in previous HRA/PRA models are not consistent with the significant roles that operators have played in actual operational events
- the accident record and advances in behavioral sciences both support a stronger focus on contextual factors, especially plant conditions, in understanding human error
- recent advances in psychology ought to be used and integrated with the disciplines of engineering, human factors, and PRA in modeling human failure events

Lessons Learned from Serious Accidents

The record of significant incidents in nuclear power plant NPP operations shows a substantially different picture of human performance than that represented by human failure events typically modeled in PRAs. The latter often focus on failures to perform required steps in a procedure. In contrast, human performance problems identified in real operational events often involve operators performing actions that are not required for an accident response and, in fact, worsen the plant's condition (i.e., errors of commission). In addition, accounts of the role of operators in serious accidents, such as those that occurred at Chernobyl 4 and Three Mile Island, Unit 2 (TMI-2) frequently leave the impression that the operator's actions were illogical and incredible. Consequently, the lessons learned from such events often are discounted as being very plant- or event-specific.

As a result of the TMI-2 event, numerous modifications and backfits were implemented by all NPPs in the United States, including symptom-based procedures, new training, and new hardware. However, after these modifications and backfits, the types of problems that occurred in this accident continue to occur. These problems are a result of errors of commission involving the intentional operator bypass of engineered safety features (ESFs). In the TMI-2 event, operators inappropriately terminated high-pressure injection, resulting in reactor core undercooling and eventual fuel damage. In 1995, NRC's Office of Analysis and Evaluation of Operation Data (AEOD) published a report entitled "Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features" that identified 14 events over the previous 41 months in which an ESF was inappropriately bypassed.

The AEOD report concluded that these events, and other similar events, show that this type of "human intervention may be an important failure mode." Event analyses performed to support the ATHEANA development (including examples given in Appendix A of this report) identified several errors of commission that resulted in the inappropriate bypass of ESFs.

In addition, event analyses of power plant accidents and incidents performed for this project show that real operational events typically involve a combination of complicating factors that are not addressed in current PRAs. The following examples illustrate the factors that may complicate operators' responses to events:

- scenarios that deviate from operators' expectations, based on their training and experience
- multiple equipment failures and unavailabilities (especially those that are dependent or human-caused) that go beyond those represented in operator training in simulators and assumed in safety analyses
- instrumentation problems for which the operators are not fully prepared and which can cause misunderstandings about the event (this may also be the case for digital-based instrumentation systems)
- plant conditions not addressed by procedures

Unfortunately, events involving such complicating factors frequently are interpreted only as an indication of plant-specific operational problems, rather than a general cause for concern for all plants.

The Significance of Context

Recent work in the behavioral sciences has contributed to the understanding of the interactive nature of human errors and plant behavior that characterize accidents in high-technology industries. This understanding suggests that it is essential to analyze both the human–centered factors (e.g., performance shaping factors (PSFs) such as human–machine interface design, the content and format of plant procedures, and training) and the conditions of the plant that call for actions and create the operational causes for human–system interactions (e.g., misleading indicators, equipment unavailabilities, and other unusual configurations or operational circumstances).

The human-centered factors and the influence of plant conditions are not independent of each other. In many major accidents, particularly unusual plant conditions create the need for operator actions and, under those unusual plant conditions, deficiencies in the human-centered factors lead people to make errors in responding to the incident. This observation has been supported by retrospective analysis of real operating event histories (e.g., see Appendix A of this report). These retrospective analyses have identified the context in which severe events can occur; specifically, the plant conditions, significant PSFs, and dependencies that set up operators for failure. Serious events appear to involve both unexpected plant conditions and unfavorable PSFs (e.g., situational factors) that comprise an EFC. Plant conditions include the physical condition of the NPP and its

instruments. Plant conditions, as interpreted by the instruments (which may or may not be functioning as expected), are fed to the plant display system. Finally, the operators receive information from the display system and interpret that information (i.e., make a situation assessment) using their mental model and current situation model. The operator and display system form the human-machine interface (HMI).

On the basis of the operating events analyzed, the EFC typically involves an unanalyzed plant condition that is beyond normal operator training and procedure-related PSFs. For example, this error-forcing condition can activate a human error mechanism related to an inappropriate assessment of the situation (e.g., a misdiagnosis). This can lead to the refusal to believe or recognize evidence that runs counter to the initial misdiagnosis. Consequently, mistakes (e.g., errors of commission), and ultimately, an accident with serious consequences, can result. These ideas lead to another way to frame the observations of serious events that have been reviewed:

- The plant behavior is outside the expected range.
- The plant's behavior is not understood.
- Indications of the actual plant state and behavior are not recognized.
- Prepared plans or procedures are not applicable nor helpful.

From this point of view, it is clear that key factors in these events have not been within the scope of existing PRAs/HRAs. If these events are the contributors to severe accidents that can actually occur, then expansion of the PRA/HRA to model them is essential. Otherwise a PRA may not include the dominant contributors to risk.

The significance of unusual contexts derived from incident analyses also is consistent with experience described by training personnel. They have observed that operators can be "made to fail" in simulator exercises by creating particular combinations of plant conditions and operator mindset.

Integration of Multiple Disciplines in ATHEANA

ATHEANA uses and integrates the knowledge and experience from multiple disciplines (e.g., plant operations and engineering, PRAs, human factors, and behavioral sciences) through an underlying, multidisciplinary HRA framework and through the systematic structuring of tasks and information in the ATHEANA HRA process.

On the basis of observations of serious events in the operating history of the commercial nuclear power industry, as well as experience in other technologically complex industries, the underlying premise of ATHEANA, both its HRA framework and process, is that significant human errors occur

as a result of a combination of influences associated with plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel.

In most cases, these error mechanisms are often not inherently "bad" behaviors, but are usually mechanisms that allow humans to perform skilled and speedy operations. For example, people often

diagnose the cause of an occurrence on the basis of pattern matching. This is in many cases an efficient and speedy way to respond to some event. However, when an event actually taking place is subtly different from a routine event, there is a tendency for people to quickly recall and select the nearest similar pattern and act as if the event was the routine one. In the routine circumstance, this rapid pattern matching allows for very efficient and timely responses. However, the same process can lead to an inappropriate response in a nonroutine situation.

Given this assessment of the causes of inappropriate actions, a process is needed that can search for likely opportunities for inappropriately triggered mechanisms to cause unsafe actions. The starting point for this search is a framework (presented and described in Section 2.1) that describes the interrelationships among error mechanisms, the plant conditions and performance-shaping factors that set them up, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe. The framework also includes elements from plant operations and engineering, PRAs, human factors engineering, and behavioral sciences. All of these elements contribute to the understanding of human reliability and its associated influences, and have emerged from the review of significant operational events at NPPs by a multidisciplinary project team representing all of these disciplines. The elements included are the minimum necessary to describe the causes and contributions of human errors in, for example, major NPP events.

The human performance-related elements of the framework (i.e., those requiring the expertise of the human factors, behavioral science, and plant engineering disciplines) are performance-shaping factors (PSFs), plant conditions, and error mechanisms. These elements are representative of the level of understanding needed to describe the underlying causes of unsafe actions and explain why a person may perform an unsafe action. The elements relating to the PRA perspective, namely the human failure events and the scenario definition, represent the PRA model itself. The unsafe action and HFE elements represent the point of integration between the HRA and PRA model. A PRA traditionally focuses on the consequences of an unsafe action, which it describes as a human error that is represented by an HFE. The HFE is included in the PRA model associated with a particular plant state that defines the specific accident scenarios that the PRA model represents.

The structure of ATHEANA's multidisciplinary HRA framework ultimately leads to the systematic structuring of the different dimensions influencing human/system interactions that is incorporated into the ATHEANA HRA process, especially the search for EFC. This systematic structuring in the ATHEANA HRA process brings a degree of clarity and completeness to the process of modeling human errors in the PRA process. The absence of this systematic approach in earlier HRA methods has limited the ability to incorporate human errors in PRAs in a way that could satisfy both the engineering and the behavioral sciences. The consequence has been that PRA results are not seen as accurate representations of the contribution of human errors to power-plant safety, particularly when compared with the experience of major NPP accidents and incidents.

Overview of ATHEANA

As noted above, ATHEANA consists of:

- a retrospective process
- a prospective process (including an HRA method)

Both of these processes are briefly described below.

The ATHEANA Retrospective Analysis Process

The ATHEANA retrospective analysis process initially was developed to support the development of the prospective (or HRA) ATHEANA analysis process. However, as the retrospective analysis matured, it became evident that this approach was useful beyond the mere development of the ATHEANA prospective approach. The results of retrospective analyses are powerful tools in illustrating and explaining ATHEANA principles and concepts. Also, the ATHEANA approach for retrospective analysis was used to train third-party users of ATHEANA in an earlier demonstration of the method. In this training, not only reviewing example event analyses, but actual experience in performing such analyses, helped new users develop the perspective required to apply the prospective ATHEANA process. Finally, event analyses using the ATHEANA approach are useful in themselves. Among other things, they can be used to help understand why specific events occurred and what could be done to prevent them from occurring again.

The retrospective approach can be applied broadly, using the ATHEANA HRA framework mentioned above. Both nuclear and non-nuclear events can be easily analyzed using this framework and its underlying concepts. A more detailed approach has been developed for nuclear power plant events, although it can be generalized for other technologies. This more detailed approach is more closely tied to the ATHEANA prospective analysis than general use of the framework. This report provides examples of event analyses using the framework approach and guidance for performing the more detailed analyses.

The ATHEANA HRA Process

The ATHEANA prospective process (or HRA) consists of ten major steps (following preparatory tasks, such as assembling and training the analysis team). This report provides detailed guidance on how to perform Steps 1 through 10. Illustrative examples of how to apply all ten of the process steps are given in Appendices B through E.

The essential elements of the ATHEANA HRA process are:

- integration of the issues of concern into the ATHEANA HRA/PRA perspective

- identification of human failure events and unsafe actions that are relevant to the issue of concern

- for each human failure event or unsafe action, identification of (through a structured and controlled approach) the reasons why such events occurs (i.e., elements of an EFC - plant conditions and performance shaping factors)

- quantification of the EFCs and the probability of each unsafe action, given its context

- evaluation of the results of the analysis in terms of the issue for which the analysis was performed

As noted earlier, ATHEANA's search for EFCs and its associated quantification approach (which some may term the "HRA method") are especially unique. The ATHEANA search for EFC has been structured to seek, among other things, plant conditions that could mislead operators so that they develop an incorrect situation assessment or response plan, and take an unsafe action. ATHEANA assumes that significant unsafe actions occur as a result of the combination of influences associated with such plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel. In ATHEANA, EFCs are identified using four related search schemes:

(1) A search [with characteristics similar to a hazards and operability analysis ("HAZOP")] for physical deviations from the expected plant response. This search also involves the identification of potential operator tendencies given the physical deviation and the identification of error types and mechanisms that could become operative given the characteristics of the physical deviation. This search for human-centered factors is also conducted as integral parts of searches 2 and 3 described below.

(2) A search of formal procedures that apply normally or that might apply under the deviation scenario identified in the first search

(3) A search for support system dependencies and dependent effects of pre-initiating event human actions.

(4) A "reverse" search for operator tendencies and error types. The first three searches identify plant conditions and rules that involve deviations from some base case. In this search, a catalog of error types and operator tendencies is examined to identify those that could cause human failure events or unsafe actions of interest. Then plant conditions and rules associated with such inappropriate response are identified. Consequently, this search serves as a catch-all to see if any reasonable cases were missed in the earlier searches.

In order to address the elements of EFC (which go beyond the types and scope of context addressed in previous HRA methods), ATHEANA required a new quantification model. In particular, quantification of the probabilities of corresponding HFEs is based upon estimates of how likely or frequently the plant conditions and PSFs comprising the EFCs occur, rather than upon assumptions of randomly occurring human failures. This approach involves an approach that blends systems analysis techniques with judgment by operators and experienced analysts to quantify the probability of a specific class of error-forcing context and the probability of the unsafe act, given that context.

In the end, the overall approach must be an iterative one (i.e., define an error-forcing context and unsafe act, attempt quantification considering recovery, refine the context, etc.).

Benefits of Applying ATHEANA

ATHEANA method has been developed to better understand and model the kinds of human behavior seen in serious accidents and near-misses in the nuclear and other industries. Both the prospective and retrospective ATHEANA processes can provide useful insights and suggest improvements regarding human performance and its contribution to safety.

Plant-specific PRA studies using ATHEANA prospective process (both qualitative and quantitative results) should provide new insights into the significant factors affecting risk, allowing, for example:

- identification of more effectively crafted risk management options (due to the better understanding of the underlying causes of human error that ATHEANA can provide)
- identification of previously undiscovered vulnerabilities in operator aids (e.g., procedures, human-machine interfaces) for specific contexts
- identification of previously undiscovered weaknesses in current training program requirements and identification of new paradigms for training
- development of new scenarios for simulator training exercises
- identification of changes in operator qualification exams
- identification of areas where the risk from human failure events are low (not risk significant from both ATHEANA and previous HRA perspectives); thereby, providing potential for regulatory relief

The ATHEANA retrospective process also is a useful tool for understanding and improving human performance. The ATHEANA retrospective process can be used to accomplish several tasks associated with the analysis of human performance, including:

- development of generic or plant-specific insights and recommendations for potential improvements,
- development of supporting information for performing HRA/PRA,
- performance of incident investigations, and
- performance of root cause analysis.

When is it Necessary to apply ATHEANA to an HRA Problem?

As stated earlier, some of the ten steps in the ATHEANA HRA process are similar to those that are performed with other HRA methods. However, ATHEANA is a more thorough process for identifying, analyzing, and documenting human failure events and contexts that make them more likely. PRA and HRA practitioners may ask: when is it necessary or proper to apply ATHEANA to an HRA problem? Structured this way, the question fails to recognize that, at a high level, the ATHEANA steps are required by all approaches to HRA and involve four areas: specification of the problem, search for HFEs, search for (or identification of) context, and quantification. In some areas ATHEANA bolsters existing methods by providing clear guidance and providing control of the PRA/HRA project. ATHEANA's detailed process description is more rigorous and systematic, as well as more explicit, than that for previous HRA processes and methods. It will lead to more consistency among analyses and increased efficiency, in the long run. In the area of context, ATHEANA breaks new ground. The searches for EFC go well beyond simple the PSF identification of previous methods. They identify unexpected plant conditions that, coupled with relevant PSFs, can have significant impact on human information processing, enabling a wide range of error mechanisms and error types. The result of this change is that quantification becomes more an issue of calculating the likelihood of specific plant conditions, for which unsafe actions are much more likely than would be true under anticipated conditions.

Consequently, the question for practitioners becomes, when to apply the full detail of ATHEANA. This is really a project management decision that depends on the intended use of the HRA/PRA and the potential impact on risk. Simplifications may be reasonable, but the consequences of the loss of information caused by such simplifications, on the evaluation of risk and on risk management capabilities, should be consciously recognized.

FOREWORD

It is widely recognized that human errors, i.e., acts (or failures to act) that depart from or fail to achieve what should be done,[1] can be important contributors to the risk associated with the operation of nuclear power plants. This recognition is based upon substantial empirical and analytical evidence. For example, key human failure events at Three Mile Island (TMI) 2 and Chernobyl 4 contributed directly to the occurrence and severity of those accidents. Numerous probabilistic risk assessment (PRA) studies, including the recent Individual Plant Examinations, have shown that a number of specific failures to correctly perform required actions (during an accident) are important risk contributors across a wide number of plants. The importance of human actions (both positive and negative) is reflected in a number of the U.S. Nuclear Regulatory Commission's (NRC's) activities and initiatives, including those aimed at making the agency's decision making more risk informed. For example, Regulatory Guide 1.174, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, specifically mentions the need for identifying "the operator actions modeled in the PRA that impact the [licensee's] application."

It is also widely recognized that current human reliability analysis (HRA) methods for identifying potentially important human failure events and determining their likelihood have significant limitations. These limitations include the inability to credibly treat events of the type that led to the TMI and Chernobyl accidents, namely mistakes involving conscious but incorrect choices of actions by plant operators in response to an accident. These failures, commonly referred to as "errors of commission," are difficult to address because they require a prediction of the circumstances under which the failures, which on the surface may appear to be illogical and incredible, actually become plausible.

In order to improve the current HRA state-of-the-art, especially regarding the treatment of errors of commission, the NRC funded the development of ATHEANA (A Technique for Human Event Analysis). ATHEANA is an approach which incorporates in an HRA methodology the current understanding of why errors occur. Its underlying premise, following the work of earlier pioneers (including Reason and Woods) and substantiated by reviews of a number of significant accidents both within and without the nuclear industry, is that significant human errors occur as a result of a combination of influences associated with plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel. This premise requires the identification of these combinations of influences, called the "error-forcing contexts" (EFCs), and the assessment of their influence. Much of the recent effort in developing ATHEANA has centered on developing methods to systematically search for EFCs.

In May 1998, a technical basis and implementation guidance document for ATHEANA was issued as a draft report for public comment. In conjunction with the release of this document, a peer review

---

[1]This general definition is from Webster's. Section 2 of this report provides a definition more targeted for human reliability analysis applications. It also establishes alternative terminology, including "human failure events," used to: a) reduce potential confusion between the probabilistic risk assessment (PRA) and behavioral science communities, and b) reduce the connotation of blame typically associated with the term "error."

of the method, its documentation, and the results of an initial test of the method was held. The numerous in-depth comments and lessons learned from these activities were used to improve ATHEANA, resulting in the version documented in this report.

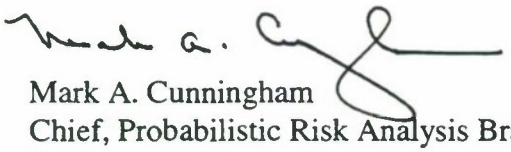
The NRC staff believes that ATHEANA has reached an important stage in its development. ATHEANA is now a thorough process for identifying, analyzing, and documenting human failure events and the contexts that make them more likely. ATHEANA shares a number of elements with current HRA methods (e.g., the collection of information on operator tasks, training, and procedures). However, it provides an increased focus on plant conditions as issues of importance when addressing the causes of human failure events. It goes beyond current HRA methods in its structured and reasonably straightforward searches for error-forcing context; these searches are designed to root out unexpected plant conditions that, coupled with relevant performance shaping factors, can have significant impact on human information processing. The fundamental result of this approach is that the process of estimating human failure event probabilities intrinsically requires the analyst to calculate the likelihood of specific plant conditions under which failures are much more likely than would be true under expected conditions.

In the next few months, NRC intends to use ATHEANA in support of regulatory activities regarding pressurized thermal shock and fire risk assessment. These applications are not only important to the agency, they also represent difficult technical challenges to conventional HRA. The staff recognizes that some aspects of ATHEANA (e.g., how to screen scenarios prior to detailed analysis, how best to perform the quantification process) need improvement to increase the methodology's efficiency and repeatability of results. Through the tests provided by real applications, we expect to develop working solutions to these technical challenges. These applications should be useful in identifying and prioritizing the NRC's future HRA development activities.

The NRC, of course, is not alone in its efforts to develop an improved HRA methodology. A number of organizations are active internationally in developing methodologies and collecting information (e.g., through actual event experience and simulator experiments) to support the implementation of these methodologies. The NRC is interacting with many of these organizations to better understand methodological similarities and differences, and hopes that these interactions will establish common grounds for future collaborations.

In closing, this report documents the current status of ATHEANA. It is expected that the methodology will continue to evolve over time, and that the report will be updated at a suitable point in the future. The staff believes the general ATHEANA framework and process are applicable to most of the HRA problems NRC is currently facing. However, details of the process have been developed with a focus on treating operator responses to nuclear power plant transients. Furthermore, the ATHEANA-unique elements of the process are aimed at addressing issues at a level of detail that may be beyond the requirements of a given HRA problem. The staff therefore does not expect that ATHEANA will be needed for all HRA problems, nor does it expect that ATHEANA will replace all other current HRA methods. With early lessons from ATHEANA applications and interactions with other organizations, the staff intends to take a broad look at the

HRA method and data needs of the agency and to define and implement the research activities needed to meet these needs.



Mark A. Cunningham
Chief, Probabilistic Risk Analysis Branch
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research

ACKNOWLEDGMENTS

Seldom is the development of an answer to a difficult problem the work of any single individual. Such is the case with development of ATHEANA. The authors especially wish to express their appreciation to:

- NRC managers (past and present) **Warren Minners**, **Joseph Murphy**, and **Mark Cunningham** for having the courage and vision to support an effort to predict errors of commission when conventional wisdom said it could not be done;

- our colleagues in the U.S. and the international community who offered debate, criticism, advice, wisdom, suggestions, encouragement, and perspectives that are such an important part of any development effort;

- industry representatives who helped with the development of ATHEANA, especially **Kenneth Kiper**, **Joseph Dalton**, **Steven Kessinger**, and **Edward Spader**, whose expertise and cooperation were vital to the successful conduct of the pilot application of ATHEANA; and,

- the many other contributors to the program, especially **John Taylor**, Brookhaven National Laboratory (BNL), **Allen Camp** (Sandia National Laboratories), **James Reason** (University of Manchester), and **Emilie Roth** (Westinghouse).

The ATHEANA team:

Michael Barriere, formerly at Brookhaven National Laboratory
Dennis Bley, Buttonwood Consulting, Inc.
Susan Cooper, Science Applications International Corp.
John Forester, Sandia National Laboratories
Alan Kolaczkowski, Science Applications International Corp.
William Luckas, Brookhaven National Laboratory
Gareth Parry, formerly at NUS-Haliburton
Ann Ramey-Smith, Nuclear Regulatory Commission
Catherine Thompson, Nuclear Regulatory Commission
Donnie Whitehead, Sandia National Laboratories
John Wreathall, John Wreathall & Company, Inc.

1 INTRODUCTION

1.1 Purpose and Organization of this Report

This report presents a human reliability analysis (HRA) method called "a technique for human event analysis" (ATHEANA). ATHEANA is the result of development efforts sponsored by the Probabilistic Risk Analysis (PRA) Branch in the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research (RES). ATHEANA was developed to increase the degree to which an HRA can represent the kinds of human behaviors seen in accidents and near-miss events at nuclear power plants and at facilities in other industries that involve broadly similar kinds of human/system interactions. In particular, ATHEANA provides this improved capability by:

- more realistically searching for the kinds of human/system interactions that have played important roles in accident responses, including the identification and modeling of errors of commission and dependencies

- taking advantage of, and integrating, advances in psychology, engineering, human factors, and PRA disciplines in its modeling

This report describes the background and process for implementing ATHEANA, which can be used to perform retrospective analyses of events to identify key human interactions and their effects. It can also be used prospectively to identify potentially significant human-related events and their likely effects on safety. It is expected that in most cases, though it is not a requirement, ATHEANA prospective analyses will be performed within the context of a PRA. The key steps in performing a retrospective analysis are:

- identify the framework of safety and the key failures that occurred to challenge the safety barriers (including "near misses" that may have reduced the margins of safety)

- identify the specific actions taken by people that caused the key failures and the contexts that led to the actions being taken

It is recognized that new analyses in the nuclear industry using ATHEANA will probably be aimed at resolving issues related to human performance; wholesale requantification of existing PRAs or the widespread performance of new PRAs for existing nuclear plants is unlikely. Therefore the development of ATHEANA has included the creation of steps to identify and interpret human-performance issues within the ATHEANA process. The identification of these issues will come from persons within NRC and the utilities, and others raising questions about human performance, but the application of ATHEANA involves the integration of the issues of concern into the ATHEANA process.

The basic steps in the prospective analysis are:

- integrate the issues of concern into the ATHEANA methodology

- perform and control the structured processes for identifying human failure events and unsafe acts and determine the reasons why such events occur (i.e., the elements of an error-forcing context)

- identify how potential conditions can arise that may set up the operators to take inappropriate actions or fail to take needed actions

- quantify the error-forcing contexts and the probability of each unsafe act, given its context (if performed within a PRA framework)

- evaluate the results of the analysis in terms of the issue for which the analysis was performed

This report provides step-by-step guidance for applying the ATHEANA method. It is anticipated that practitioners will be most concerned with the guidelines for applying ATHEANA principles and concepts provided in Part 2 of this report. However, the analysis team must include members who are thoroughly familiar with the knowledge base of theoretical material and operational events described in Part 1 of this report. Thus, this report also summarizes the technical bases of ATHEANA. Theoretical material from the behavioral sciences explains the factors involved in human error. Application of theoretical models to real nuclear power plant events clarifies which factors are most often involved in significant events. Together, these expositions lead to formalisms for retrospective analysis of events and prospective analysis of human reliability.

This report is organized in two parts:

Part 1, Principles and Concepts Underlying the ATHEANA HRA Method. This part begins with Section 2, which provides a general description of the ATHEANA method. Section 3 discusses the importance of context in influencing operator performance. Section 4 discusses the behavioral sciences principles on which ATHEANA is based (i.e., the lessons of the "real world" and the theoretical knowledge developed through analysis and experimentation). Part 1 closes with Section 5, which returns to operational experience to illustrate the ATHEANA concepts previously presented.

Part 2, Application of Principles and Concepts to ATHEANA. This part begins with Section 6, which provides a summary of the process. Section 7 discusses the preparation required to use the ATHEANA method. Section 8 provides the guidance for using ATHEANA for retrospective analyses, and Section 9 provides step-by-step guidelines for prospectively using the ATHEANA method to identify potentially significant new unsafe actions and the contexts in which they could occur. Section 10 provides guidance on interpreting the results in terms of resolving the issues for which the analysis was performed, including quantifying the frequencies of, and incorporating the accident scenarios that would be used in a PRA, if appropriate. Section 11 closes Part 2 by summarizing the purpose and capability of ATHEANA.

This report also includes five appendices:

Appendix A, Representation of Selected Operational Events from an ATHEANA Perspective. This describes the results of retrospective analyses using ATHEANA for six events at nuclear power plants.

Appendices B-E illustrate the prospective application of ATHEANA for the following types of event:
Appendix B, Loss of Main Feedwater
Appendix C, Large Loss-of-Coolant Accident (LOCA)
Appendix D, Loss of Service Water
Appendix E, Small LOCA

Appendix F, Summary of Comments and Responses. This discusses the comments received from a peer-review panel convened to discuss the previous version of ATHEANA.

Appendix G, Glossary of General Terms for ATHEANA. This provides definitions of important ATHEANA terms.

1.2 Background

PRA has become an important tool in nuclear power plant (NPP) operations and regulation. For over two decades, the NRC has been using PRA methods as a basis for regulatory programs and analyses. The NRC published SECY-95-126 (Ref. 1.1), providing the final policy statement on the use of PRA in NRC regulatory activities. In June 1994, a memorandum from the NRC Executive Director for Operations to the Commissioners (Ref. 1.2), identified at least 12 major licensing and regulatory programs that are strongly influenced by PRA studies. These programs include the following activities:

- licensing reviews of advanced reactors
- screening and analysis of operational events
- inspections of facilities
- analysis of generic safety issues
- facility analyses
- reviews of high-level waste repositories

HRA is a critical element of PRAs since it is the tool used to assess the implications of various aspects of human performance on risk. Although all of these current programs require an understanding of the human contribution to risk, current HRA methods are limited in their ability to represent all of the important aspects of human performance, constraining the extent to which NRC can rely on the results of PRA studies for decision-making processes.

Limitations in the analysis of human actions in PRAs are always recognized as a constraint in the application of PRA results. For example, in its review of the first comprehensive nuclear plant PRA, the Reactor Safety Study (WASH-1400, Ref. 1.3), the Lewis Commission (NUREG/CR-0400, Ref. 1.4) identified four fundamental limitations in the methods used in the evaluation of "human factors" just 6 months before the Three Mile Island accident (Ref. 1.5). The four fundamental limitations are as follows:

- insufficient data
- methodological limitations related to the treatment of time-scale limitations
- omission of the possibility that operators may perform recovery actions
- uncertainty concerning the actual behavior of people during accident conditions

In 1984, NRC again reviewed the methodology of PRAs, in NUREG-1050 (Ref. 1.6), and recognized that several of the HRA limitations listed above were still relevant. This review led to the following conclusion:

> the depth of the [HRA] techniques must be expanded so that the impact of changes in design, procedures, operations, training, etc., can be measured in terms of a change in a risk parameter such as the core-melt frequency. Then tradeoffs or options for changing the risk profile can be identified. To do this, the methods for identifying the key human interactions, for developing logic structures to integrate human interactions with the system-failure logic, and for collecting data suitable for their quantification must be strengthened.

Most of these deficiencies continue to persist in HRA methods today. For example, in the NRC's final policy statement on the use of probabilistic risk assessment methods in nuclear regulatory activities (SECY-95-126, Ref. 1.1), errors of commission (EOCs) are specifically identified as an example of a human performance issue for which HRA and PRA methods are not fully developed. In addition, NRC's final policy statement asserts that "PRA evaluations in support of regulatory decisions should be as realistic as practicable." Without incorporating the aspects of human performance seen in serious accidents and incidents, a PRA's omission of context-driven human failures cannot be considered "realistic."

Previous efforts in this project examined human performance issues specific to shutdown operations (NUREG/CR-6093, Ref. 1.7), and developed a multidisciplinary HRA framework to investigate errors of commission and human dependencies in full-power and shutdown operations (NUREG/CR-6265, Ref. 1.8). To support ATHEANA, the human/system event classification scheme (HSECS) database (Ref. 1.9) has been developed as a more comprehensive data analysis approach and database for the review of operating experience. Most recently, NUREG/CR-6350 (Ref. 1.10) presented the preliminary technical basis and methodological description of ATHEANA.

The ATHEANA method is concerned with identifying and estimating the likelihoods of situations in which operators take actions that render a plant unsafe. As discussed in later sections, the principal focus of ATHEANA is to identify how human failure events (HFEs) can occur as a result

of unsafe actions (UAs), and what types of error-forcing contexts (EFCs) can set up the opportunities to make such HFEs and UAs potentially significant. While these terms are discussed more formally later, HFEs are expressed as the effect of an action on plant systems (such as loss of high-pressure injection cooling resulting from operator action). UAs are expressed as particular human actions that can lead to an HFE; an example would be "Operators prematurely terminate operation of safety injection pumps A and B." The term "error-forcing context" is used in ATHEANA to describe those conditions that set up the opportunity for the unsafe action and possibly the HFE to occur. It should be noted that the term EFC adopted at the beginning of the development of ATHEANA, does not imply that the unsafe action and HFE are guaranteed to occur; rather, it leads to an increased likelihood of such events occurring. In addition, the term "error" in the broader sense is not used in ATHEANA because of some people's assumption that an "error" implies blame on the part of the person making the "error." That is not the intention in ATHEANA, where we believe that in most cases the unsafe actions are the likely consequences of a situation in which operators are placed.

ATHEANA is intended to be used as a tool in addressing and resolving issues associated with the risks of human/system interactions in the nuclear power and other industries. That is to say, the process includes guidance for identifying and structuring the analysis around answering questions, rather than simply being just one step in a PRA. This emphasis is deliberate because in the immediate future, it is unlikely that nuclear plants will perform new PRAs. In most cases, plants are likely to adapt their existing individual plant examinations (IPEs) to address any new issues. The ATHEANA process accommodates this reality.

Some issues may be explicitly stated in terms of an overall PRA framework; for example, "What is the change in the core-damage frequency associated with some specific new operator actions?" Other issues may not be expressed in a way that is explicitly tied to a PRA framework; for example, "What is the effect of cable-aging issues on safety, with respect to operator actions?" In the NRC environment of risk-informed regulatory practice, even such loosely expressed issues will be related to a PRA. The process includes explicit guidance for including these issues in the ATHEANA method.

The human behaviors associated with accidents and near misses in the nuclear and other industries seem broadly similar, and initial conversations with human-performance analysts in other industries (e.g., aviation) suggest that ATHEANA may be useful in these other industries. Therefore, while many of the descriptions and examples of ATHEANA are associated with nuclear power, analogous descriptions can be seen in other industries. For example, in nuclear power, the events of concern are usually thought of as the occurrence of core damage, failure of the containment, and release of radiation to the public. In the case of aviation, the primary events of concern are hull-loss accidents (those involving the write-off of the aircraft), injuries and fatalities among the passengers and crew, and financial loss. Similarly with the chemical process industry, the primary events of concern include losses or damage to the facility, injuries and fatalities to the members of the workforce and the public, and toxic releases to the environment. In addition, the kinds of human/system interactions will be specific to these domains (flight control, air traffic control, process operations, etc.) The tools, performance-shaping factors, and work environments will be different. However, we believe that analysts working in these other environments will be able to infer how the process

could be used from our descriptions and examples, even though they are principally associated with nuclear power.

The summary material presented in the following sections introduces the reader to ATHEANA and answers the following relevant questions when considering ATHEANA for the first time:

- Why is a new method needed for human reliability analysis?
- In what ways can the use of ATHEANA improve the analysis of human performance and risk management?

1.3 Motivation for a New Approach to Human Reliability Analysis

The record of significant incidents in NPP operations shows a substantially different picture of human performance than that represented by human failure events typically modeled in PRAs. The latter often focus on failures to perform required steps in a procedure. In contrast, human performance problems identified in real operational events often involve operators performing actions that are not required for an accident response and, in fact, worsen the plant's condition (i.e., EOCs). In addition, accounts of the role of operators in serious accidents, such as those that occurred at Chernobyl 4 (NUREG-1250, Ref. 1.11 and NUREG-1251, Ref. 1.12), and Three Mile Island, Unit 2 (TMI-2, Ref. 1.5), frequently leave the impression that the operator's actions were illogical and incredible. Consequently, the lessons learned from such events often are discounted as being very plant- or event-specific.

As a result of the TMI-2 event, numerous modifications and backfits were implemented by all nuclear power plants in the United States, including symptom-based procedures, new training, and new hardware. However, after these modifications and backfits, the types of problems that occurred in this accident continue to occur. These problems are a result of errors of commission involving the intentional operator bypass of engineered safety features (ESFs). In the TMI-2 event, operators inappropriately terminated high-pressure injection, resulting in reactor core undercooling and eventual fuel damage. NRC's Office of Analysis and Evaluation of Operation Data (AEOD) published "Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features," AEOD/E95-01, July 1995 (Ref. 1.13), identifying 14 events over the previous 41 months in which an ESF was inappropriately bypassed. The AEOD/E95-01 report concluded that these events, and other similar events, show that this type of "human intervention may be an important failure mode." Events analyses performed to support the ATHEANA development (NUREG/CR-6265, Ref. 1.8) and the HSECS database (Ref. 1.9) also have identified several errors of commission that result in the inappropriate bypass of ESFs.

In addition, event analyses of power plant accidents and incidents performed for this project show that real operational events typically involve a combination of complicating factors that are not addressed in current PRAs. The following examples illustrate the factors that may complicate operators' responses to events:

- scenarios that deviate from operators' expectations, based on their training and experience
- multiple equipment failures and unavailabilities (especially those that are dependent or human-caused) that go beyond those represented in operator training in simulators and assumed in safety analyses
- instrumentation problems for which the operators are not fully prepared and which can cause misunderstandings about the event (this may also be the case for digital-based instrumentation systems)
- plant conditions not addressed by procedures

Unfortunately, events involving such complicated factors frequently are interpreted only as an indication of plant-specific operational problems, rather than a general cause for concern for all plants.

The purpose of ATHEANA is to provide an HRA modeling process that can accommodate and represent the human performance found in real NPP events, and that can be used with PRAs or other safety perspectives to resolve safety questions. On the basis of observations of serious events in the operating history of the commercial nuclear power industry, as well as experience in other technologically complex industries, the underlying premise of ATHEANA is that significant human errors occur as a result of a combination of influences associated with plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel.

In most cases, these error mechanisms are often not inherently "bad" behaviors, but are usually mechanisms that allow humans to perform skilled and speedy operations. For example, people often diagnose the cause of an occurrence on the basis of pattern matching. This is in many cases an efficient and speedy way to respond to some event. However, when an event actually taking place is subtly different from a routine event, there is a tendency for people to quickly recall and select the nearest similar pattern and act as if the event was the routine one. In the routine circumstance, this rapid pattern matching allows for very efficient and timely responses. However, the same process can lead to an inappropriate response in a nonroutine situation. Other examples of such error mechanisms are discussed in Sections 4 and 9.

Given this assessment of the causes of inappropriate actions, a process is needed that can search for likely opportunities for inappropriately triggered mechanisms to cause unsafe actions. The starting point for this search is a framework (described in Section 2) that describes the interrelationships among error mechanisms, the plant conditions and performance-shaping factors that set them up, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe. The framework also includes elements from plant operations and engineering, PRAs, human factors engineering, and behavioral sciences. All of these elements contribute to the understanding of human reliability and its associated influences, and have emerged from the review of significant operational events at NPPs by a multidisciplinary project team representing all of these disciplines.

The elements included are the minimum necessary to describe the causes and contributions of human errors in, for example, major NPP events.

The human performance-related elements of the framework (i.e., those requiring the expertise of the human factors, behavioral science, and plant engineering disciplines) are performance-shaping factors, plant conditions, and error mechanisms. These elements are representative of the level of understanding needed to describe the underlying causes of unsafe actions and explain why a person may perform an unsafe action. The elements relating to the PRA perspective, namely the human failure events and the scenario definition, represent the PRA model itself. The unsafe action and HFE elements represent the point of integration between the HRA and PRA model. A PRA traditionally focuses on the consequences of an unsafe action, which it describes as a human error that is represented by an HFE. The HFE is included in the PRA model associated with a particular plant state that defines the specific accident scenarios that the PRA model represents.

The framework has served as the basis for the retrospective analysis of real operating event histories (NUREG/CR-6903 (Ref. 1.7), NUREG/CR-6265 (Ref. 1.8), the HSECS database (Ref. 1.9), and NUREG/CR-6350 (Ref. 1.10)). That retrospective analysis has identified the context in which severe events can occur; specifically, the plant conditions, significant performance-shaping factors (PSF), and dependencies that set up operators for failure. Serious events appear to involve both unexpected plant conditions and unfavorable PSFs (e.g., situational factors) that comprise an error-forcing context. Section 3.2 clarifies the term "plant conditions" and depicts the relationship between plant conditions and the operator. Plant conditions include the physical condition of the NPP and its instruments. Plant conditions, as interpreted by the instruments (which may or may not be functioning as expected), are fed to the plant display system. Finally, the operators receive information from the display system and interpret that information (i.e., make a situation assessment) using their mental model and current situation model. The operator and display system form the human-machine interface (HMI).

On the basis of the operating events analyzed, the error-forcing context typically involves an unanalyzed plant condition that is beyond normal operator training and procedure-related PSFs. For example, this error-forcing condition can activate a human error mechanism related to an inappropriate assessment of the situation (e.g., a misdiagnosis). This can lead to the refusal to believe or recognize evidence that runs counter to the initial misdiagnosis. Consequently, mistakes (e.g., errors of commission), and ultimately, an accident with serious consequences, can result. These ideas lead to another way to frame the observations of serious events that have been reviewed:

- The plant behavior is outside the expected range.
- The plant's behavior is not understood.
- Indications of the actual plant state and behavior are not recognized.
- Prepared plans or procedures are not applicable nor helpful.

From this point of view, it is clear that key factors in these events have not been within the scope of existing PRAs/HRAs. If these events are the contributors to severe accidents that can actually occur, then expansion of the PRA/HRA to model them is essential. Otherwise a PRA may not include the dominant contributors to risk.

Previous HRA methods have implicitly focused on addressing the question, "What is the chance of random operator error (e.g., operator fails to...) under nominal accident conditions?" Even when performance-shaping factors are included, they are typically evaluated for the nominal event sequence or, at best, for particular cut sets. The analyses have not looked beyond the hardware modeled in the PRA for specific conditions that could complicate operator response. On the basis of review of the operating experience in several industries, a more appropriate question to pursue is, "What is the chance of an error-forcing-context occurring so that operator error is very likely?"

The systematic structuring of the different dimensions influencing human/system interactions that is provided by the multidisciplinary HRA framework, along with the search for cognitively demanding context that is driven by consideration of the elements of cognitive information processing, brings a degree of clarity and completeness to the process of modeling human errors in the PRA process. The absence of this systematic approach in existing HRA methods has limited the ability to incorporate human errors in PRAs in a way that could satisfy both the engineering and the behavioral sciences. The consequence has been that PRA results are not seen as accurate representations of the contribution of human errors to power-plant safety, particularly when compared with the experience of major NPP accidents and incidents.

1.4 Benefits from Using ATHEANA

The primary purpose of any nuclear plant probabilistic risk assessment is to provide a means to understand and manage risk at these plants. Three steps must be carried out for risk management to be effective. First, the risks must be identified and ranked so that resources can be applied most effectively in managing them. Second, there must be a well-defined understanding of the underlying reasons the risks exist. Third, cost-effective solutions must be identified and implemented to ensure adequate management of the most significant risks (i.e., lessened to the extent feasible and justifiable). To have an effective risk-management program, the risk-analysis technique must be able to supply the first two results so that appropriate risk management solutions can be identified and implemented. However for risk management to be fully effective, it is important that the models be realistic. As discussed earlier, many current PRAs do not include the types of human actions seen in many major accidents and near misses. The use of ATHEANA is intended to remedy this deficiency, as discussed in the following sections.

1.4.1 Overview of the Risk Management Benefits of Using ATHEANA

The results of the ATHEANA process can be viewed from a variety of perspectives. One level is the determination of whether there are additional risk-significant human failure events not currently captured in existing PRA/human reliability analyses. In particular, a focus of the ATHEANA

process is to identify errors of commission that may be risk significant and not currently modeled in the existing PRAs for the plants. In addition, use of the ATHEANA approach and its focus on error-forcing context may identify new errors of omission, or at least a reevaluation of the probability and risk importance of already identified errors of omission. Collectively, this information provides insights into additional human failure events that may be risk-significant, and through the PRA quantification process updates the results of the PRA (revised core damage frequency, revised ordering of the dominant accident sequences, etc.), thereby providing a more complete quantitative assessment of nuclear power plant risk. This level of results addresses the first step when implementing a risk management program.

At another level, through its investigative nature, the ATHEANA process attempts to identify the underlying causal factors for these risk-important HFEs. The process requires the identification of conditions that may significantly increase the potential for HFEs (i.e., error-forcing contexts) in order to identify these risk-significant HFEs and quantify their likelihood. This aspect of the ATHEANA process addresses the second step mentioned above when implementing a risk management program.

The third step, risk management, can then be effectively carried out using both levels of results. Once the results are understood in the full context of the PRA, risk management is carried out in several steps:

(1) *Suggest possible changes to reduce risk, cost, or both.* Risk can be reduced through effective changes of equipment, activities of plant personnel, and emergency response capabilities. A better understanding of the factors affecting risk can reduce the uncertainties in calculated risks. From the viewpoint of traditional PRA results, this means applying seasoned knowledge, in light of the PRA results, to envision possible changes. Some examples of risk reduction alternatives follow:

- Changes to plant hardware. These are the obvious responses to risks involving plant equipment. These changes are often costly, however, and may involve retraining workers; therefore other alternatives should also be considered, which may turn out to be more effective.

- Changes to plant procedures. Operating, maintenance, and emergency procedures, as well as off-site emergency response procedures, can be effectively modified and improved to reduce risk. Care must be taken to ensure that neither the training of personnel nor the level of performance is adversely affected by frequent or poorly analyzed procedural changes.

- Changes to plant training. Training programs can be expanded to improve performance in the scenarios found to be the most significant contributors to risk. In particular, new training techniques based on psychological understanding of significant HFE-EFC combinations can be developed. Most operational training is technology based, i.e., organized to teach facts about the plant, its operation, and its procedures, rather than to modify human behavior under cognitively demanding circumstances. There are exceptions such as fire-fighting

schools and the U.S. Navy's damage control school, where the focus includes intense indoctrination under physically and mentally demanding environments. Most simulator training is demanding, but focuses on programmed responses to somewhat standardized accident sequences. However, some recent nuclear power plant simulator training is stressing paradigms to improve the likelihood of successful communication among operators (misunderstood, misinterpreted, and partially completed verbal interactions are common sources of improper situation assessment and response in industrial accidents) and to force periodic team reassessment of past and future events (to break mindset and to test situation assessment).

- Improvement in underlying knowledge. Improvement in underlying knowledge[1] can affect risk. Reducing uncertainties often has a tendency to reduce calculated average risks because the average is strongly affected by possibilities associated with upper uncertainty bounds. There are several appropriate target areas:

  - research
  - more accurate mechanistic calculations
  - experiments to determine new physical knowledge
  - experiments to determine new knowledge of behavior and of the interaction between plant conditions and human influences
  - improvements in PRA and HRA modeling; for example, more precise modeling of success criteria–risk models necessarily involves simplifications, approximations, and assumptions. Improvements in risk modeling are usually possible if analysts can refine their models by replacing conservative assumptions with more realistic if detailed analyses.

(2) *Evaluate the impact of each proposed change on risk and cost.* The new, after change, plant-operator system is analyzed using the same tools, under the assumption that the change is in place and functioning in a realistic fashion. That is, do not assume that a fix is perfect; it will generally have some possibility of actually making things worse.

(3) *Decide among the options.* In addition to changes, it is usually appropriate to include the option, "make no change." There are formal tools for evaluating alternative strategies such as multiattribute decision analysis. However, in practical applications, once the risk and cost (and their uncertainty) are well formulated, the selection of the best option is often obvious.

1.4.2 Insights from ATHEANA Regarding Risk Management Using PRA

The following sections discuss insights that are anticipated from the application of ATHEANA to plant-specific PRAs. Current HRA-related results identify *for the risk-significant HFEs identified*

[1] An efficient way to gather and format knowledge from any of the listed sources is to convene a panel whose members are experts in the area of knowledge sought, and conduct a formal elicitation process.

thus far such recommendations as procedure improvements, revised training focus, changes to plant status indications/alarms and improvements in ergonomic aspects of the plant design. The expectation is that a better understanding of the underlying causes of human errors anticipated from ATHEANA will result in more effectively crafted risk management options. The net result should be:

- a more complete assessment of potentially risk-dominant HFEs
- a more effective management of the total risk represented by inappropriate human actions, and hence
- a greater level of safety by further reducing the potential for HFEs

1.4.2.1 Possible Plant-Specific Insights and Subsequent Improvements

ATHEANA, with its first-generation documentation and guidance, was tested using a sampling of event sequences identified in a PRA for a PWR nuclear power plant. A team that includes PRA and operations specialists from the plant performed this first test application. Based on the findings from this first application and their fidelity to previous expectations, as well as some unexpected results, the kinds of plant-specific insights that can be expected from widespread application of ATHEANA to other plants include:

- *Instrumentation.* Recommended changes can be expected in instrument design (redundancy, diversity, vulnerability to common-cause failure) and in plant-status indications (more effective layout, better labeling, adding/subtracting indications and alarms, accessability).
- *Procedures.* Recommended changes can be expected in specific emergency procedures (eliminating points of ambiguity, providing additional cautionary notes, revisiting decision points if sequence timing is other than expected for the anticipated case) and in administrative procedures to enhance communication and situation assessment.
- *Training.* Recommended changes can be expected in some technical areas to provide operators with a better mental model of plant performance under particular degraded states and in developing specific cognitive skills. Particular focus should be in changing specific training to make operators aware of any identified error-forcing contexts, including new paradigms for breaking out of flawed situation models. New simulator exercises will be identified that can extend training into previously unexamined areas.
- *Maintenance.* Recommended changes can be expected in maintenance frequency and practices for particular equipment, to lessen the chances of some error-forcing contexts (i.e., those contexts that are induced in part by current maintenance practices). Analysis of ATHEANA results has indicated that certain practices can lead to special kinds of EFCs that can have a strong influence

on operator performance. In particular, the following practices significantly increase the likelihood of UAs when unfamiliar event sequences occur:

- allowing instruments and standby equipment to remain out of service for long time periods; operators learn to rely on alternative indications that may not be reliable under all conditions

- allowing repeated occurrences of severe out-of-calibration instrumentation or failures of instruments; operators learn to mistrust their instruments

- allowing routine bypassing of interlocks and ESFs, or jumpering of interlocks

- *Corrective Actions*. Because ATHEANA focuses on explicit causal factors, the retrospective analysis of plant events using the ATHEANA framework and information processing model can help plant management identify more effective corrective actions for events involving human performance problems.

1.4.2.2 Insights of Possible Value to the NRC and Industry

As plant-specific PRA studies using ATHEANA are completed and analyzed, new insights into the significant factors affecting risk should allow the following objectives to be fulfilled:

- identification of any new vulnerabilities not found by previous methods

- identification of weaknesses in current training program requirements and identification of new paradigms for training

- identification of potential changes in operator qualification exams

- identification of additional factors to be considered when evaluating the significance of actual events (i.e., considering those factors that relate to human performance and inducing possible error-forcing contexts)

- development of input to the NRC's maintenance rule identifying instruments for high-priority maintenance (i.e., high-reliability requirements and prompt corrective action, because of their importance to human reliability)

- identification of areas where the risks from HFEs are low (not risk significant from both ATHEANA and previous HRA perspectives), thereby providing potential for regulatory relief

1.4.2.3 Insights Regarding Additional Qualitative Benefits from Using ATHEANA

Many qualitative applications of parts of ATHEANA can be useful long before final ATHEANA HRA and PRA results are completed. These arise in many areas. A few examples are provided below:

- *Event analysis.* The ATHEANA framework provides a multidisciplinary structure for the retrospective analysis of operational events. Section 8 discusses the process for performing these event analyses. The ATHEANA point of view emphasizes the interrelationships that define error-forcing context. It can expose immediately useful information on the causes of the events so that more effective barriers can be erected to prevent the recurrence of identical and related types of events in the future. It will encourage updating of the plant-specific knowledge base with new information to help in future HRA work.

- *Internal communications.* The structured approach of ATHEANA and the recommended team structure bring together individuals from different groups within the licensee's organization to work more closely toward the common goal of improving human performance. In fact, the use of ATHEANA may lead to interaction among groups that heretofore has been minimal.

- *Root-cause analysis.* When it is incorporated into the root-cause analysis process, the ATHEANA framework provides a structure for examining the human contribution to significant plant problems and the underlying causes for that contribution.

1.4.3 General Insights

ATHEANA provides a useful structure for understanding and improving human performance in operational events. As described elsewhere in this report, it originates from a study of operational events and from an attempt to reconcile human performance observed in the most serious of these events with existing theories of human cognition and human reliability models, within the context of plant design, operation, and safety. ATHEANA provides a useful approach for accomplishing several tasks associated with the analysis of human performance, including:

- retrospective analysis of operational events
- prospective search for HFEs, UAs, and EFCs
- root-cause analysis
- incident analyses

Although the qualitative benefits are of considerable value, it is the quantitative use of the ATHEANA process in PRAs that can bring clarity to the complex question of overall benefit. This integrated view of plant operation is a necessary foundation for ranking risk insights for decision-making and for identifying the most cost-effective improvements.

1.5 Other Related HRA Developmental Work

The development of the ATHEANA method has not occurred in isolation. Rather, it has progressed in parallel with other projects that have related aims. Indeed, the goal of having HRA methods become more sensitive to the situations in which operators are placed and which can disrupt their cognition has long been an aim of the HRA development community. As early as 1982, NUREG/CR-3010, in describing the operator action tree (OAT) HRA method, stated that the OAT method "was developed to be an interim tool until more soundly based models [of the cognitive behavior of operators] become available" (Ref. 1.14). As discussed below, it has taken until the early to mid 1990s for the development of such models to emerge to the point of being usable in HRAs.

Practically speaking, information on the relationships among cognitive processes, "human error," and accidents coalesced and became more readily accessible to the engineering community through a series of multidisciplinary workshops and publications in the 1980s and early 1990s. One of the first significant steps was the publication of "Man-Made Disasters" in 1978 (Ref. 1.15) which made a first cut at systematically looking for common patterns of human activities in major accidents. Beginning in the early 1980s, there were a series of NATO-sponsored workshops dealing with such topics as human error (Ref. 1.16) and human detection and diagnosis of system failures (Ref. 1.17). These meetings brought together a wide spectrum of disciplines interested in human error, from attorneys and regulators to psychologists, sociologists, human factors engineers and PRA engineers. In addition, meetings sponsored by the World Bank, the IEEE series of conferences associated with human factors and nuclear safety (the series of meetings most frequently held at Myrtle Beach, SC, and Monterey, CA), and the Probabilistic Safety Assessment and Management (PSAM) conferences have all provided significant opportunities for continuing of the multidisciplinary discussions.

The exchanges of ideas and viewpoints at these meetings were very influential in creating the multidisciplinary perspective that has led to many of the new HRA developments in recent times, including ATHEANA. In other words, many of the recent developments have common roots in these discussions. One commonly identified specific source of information for these developments is *Human Error* (Ref. 1.18), which draws together work in different disciplines using a cognitive-psychology perspective to describe how people can be set up to take the kinds of unsafe actions seen in major technological accidents.

Several activities have aimed at developing methods to model errors of commission. As discussed earlier, these inappropriate interventions with automatically initiated systems have been seen as a recurring problem in operational problems (as discussed in Ref. 1.13), yet have typically not been included in current HRA methods. Of particular note, methods developed to analyze such errors include those developed by Julius, Jorgenson et al, (Refs. 1.19 and 1.20) and the Human Interaction Timeline (HITLINE) method developed by Macwan and Mosleh (Ref. 1.21). The first set of methods focuses on how operators may inappropriately follow and act upon incorrect paths in procedures, for example, because they misinterpret indications. HITLINE similarly seeks to identify opportunities for misdiagnosis or other cognitive errors in which operators take actions that

are not needed. The likelihood of such errors is based on assessments of various time-independent and time-dependent factors. The time-independent factors include crew training and experience, crew confidence, etc.; and the time-dependent factors are related to the plant, the procedures, and the operator actions in the event.

In addition to these methods aimed specifically at errors of commission, other work has continued in the development of HRA methods to take better account of developments in the understanding of the mechanisms giving rise to erroneous actions and the recognition that human errors are not random occurrences. One of the first and most influential was the pioneering work by Woods, Roth, and others in the development of a simulation-based model of nuclear power plant operators' cognition in the NRC-sponsored cognitive environment simulation (CES) (Ref. 1.22).

Some of the principal developments have been the Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté (MERMOS) developed by Electricité de France (Ref. 1.23); the Connectionism Assessment of Human Reliability (CAHR) method by Sträter and Bubb (Ref. 1.24); the Cognition Simulation Model (COSIMO) (Ref. 1.25) and its implementation in the Human Error Reliability Methods for Event Sequences (HERMES) (Ref. 1.26) by Cacciabue et al, INTENT by Gertman, Blackman et al, (Ref. 1.27); the two methods developed by Julius, Jorgenson, et al, (Refs. 1.19 and 1.20); the HITLINE method developed by Macwan and Mosleh (Ref. 1.21); and the Cognitive Reliability and Error Analysis Method (CREAM) by Hollnagel (Ref. 1.28). Each of these methods in one way or another seeks to model some specific aspects of an operator's, or the operating crew's cognitive processes.

In addition, the European Commission supported an extended network of experts in human performance, called the European Association on Reliability Techniques for Humans (EARTH), to identify a range of factors and issues that can cause failures in operator cognitive processes (Ref. 1.29). This catalog of issues has provided developers of the new methods with a common source of ideas for modeling.

In order to improve the efficiency of the development process, ATHEANA has tried to take advantage of ideas conceived and refined by the above developments through discussions with the methods' developers, reviews of related documentation, and general participation in the HRA developers' environment, such as participation in the Mosaic group (an informal network of HRA method developers). We wish to thank and acknowledge the discussions with those mentioned above and many others for their help, advice, and counsel while developing the ATHEANA method.

1.6 References

1.1 U.S. Nuclear Regulatory Commission, Final Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities. SECY-95-126, Washington, DC, May 16, 1995.

1.2 J. M. Taylor, "Summary of NRC uses of risk assessment for committee on risk analysis," Memo to Commissioner G. de Planque from the Executive Director of Operations, U.S. Nuclear Regulatory Commission, Washington, DC, June 6, 1994.

1.3 U.S. Atomic Energy Commission, *Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.* WASH-1400 (NUREG 75/014), Washington, DC, 1975.

1.4 H. W. Lewis et al, *Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission.* Ad Hoc Risk Assessment Review Group, NUREG/CR-0400, U.S. Nuclear Regulatory Commission, Washington, D.C., September 1978.

1.5 M. Rogovin and G. Frampton, *Three Mile Island - A Report to the Commissioners and to the Public*. Special Inquiry Group, Nuclear Regulatory Commission, Washington, DC, January 1980.

1.6 U.S. Nuclear Regulatory Commission, *Probabilistic Risk Assessment Reference Document*. NUREG-1050, Washington, DC, September 1984.

1.7 M. T. Barriere, W. J. Luckas, D. W. Whitehead, and A. M. Ramey-Smith, *An Analysis of Operational Experience During LP&S and Plan for Addressing Human Reliability Assessment Issues*. NUREG/CR-6093, Brookhaven National Laboratory: Upton, NY and Sandia National Laboratories, Albuquerque, NM, June 1994.

1.8 M. T. Barriere, W. J. Luckas, J. Wreathall, S. E. Cooper, D. C. Bley, and A. M. Ramey-Smith, *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis.* NUREG/CR-6265, Brookhaven National Laboratory, Upton, NY, August 1995.

1.9 S. E. Cooper, W. J. Luckas, and J. Wreathall, *Human/system Event Classification Scheme (HSECS) Database Description.* BNL Technical Report No. L2415/95-1, Brookhaven National Laboratory, Upton, NY, December 1995.

1.10 S. E. Cooper, A. Ramey-Smith, J. Wreathall, G. W. Parry, D. C. Bley, J. H. Taylor, W. J. Luckas, *A Technique for Human Error Analysis (ATHEANA).* NUREG/CR-6350, Brookhaven National Laboratory, Upton, NY, April 1996.

1.11 U.S. Nuclear Regulatory Commission, *Report on the Accident at the Chernobyl Nuclear Power Station.* NUREG-1250, Washington, DC, December 1987.

1.12 U.S. Nuclear Regulatory Commission, *Implications of the Accident at Chernobyl for Safety Regulation of Commercial Nuclear Power Plants in the United States*. NUREG-1251, Vols. 1 and 2, Final Report, Washington, DC, April 1989.

1.13 Office of Analysis and Evaluation of Operational Data (AEOD), U.S. Nuclear Regulatory Commission, *Engineering Evaluation - Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features*. AEOD/E95-01, Washington, DC, July 1995.

1.14 R. E. Hall, J. Fragola, and J. Wreathall, *Post Event Human decision Errors: Operator Action Tree/Time Reliability Correlation*. NUREG/CR-3010, Brookhaven National Laboratory, Upton, NY, November 1982.

1.15 B.A. Turner, and N.F. Pidgeon, *Man-made Disasters*. 2nd ed. 1997: Butterworth-Heinemann, Boston.

1.16. J.W. Senders and N.P. Moray, *Human Error: Cause, Prediction, and Reduction*. Hillsdale, N.J, Lawrence Erlbaum, 1991.

1.17 J. Rasmussen and W.B. Rouse eds. *Human Detection and Diagnosis of System Failures*. NATO Conference Series. Plenum Press, New York, 1981.

1.18 J. Reason, *Human Error*. Cambridge University Press, New York, 1990,

1.19 J.A. Julius, E.J. Jorgenson, G.W. Parry, A. M. Mosleh, "A procedure for the analysis of errors of commission in a Probabilistic Safety Assessment of a nuclear power plant at full power," *Reliability Engineering and System Safety* 50: 189-201, 1995.

1.20 J.A. Julius, E.J. Jorgenson, G.W. Parry, A.M. Mosleh, "A procedure for the analysis of errors of commission during non-power modes of nuclear power plant operation," *Reliability Engineering and System Safety* 53: 139-154, 1996.

1.21 A. Macwan and A. Mosleh, *Methodology for Analysis of Operator Errors of Commission During Nuclear Power Plant Accidents with Application to Probabilistic Risk Assessments*. MDNE-93-001. 1993, Department of Materials and Nuclear Engineering, University of Maryland, College Park, MD.

1.22 D.D.Woods, H.E. Pople, and E.M. Roth, *The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability*, NUREG/CR-5213. 1990, Westinghouse Electric Corp., Pittsburgh, PA.

1.23 C. Bieder, P. Le-Bot, E. Desmares, J-L Bonnet, F. Cara, "MERMOS: EDF's new advanced HRA method," in *Probabilistic Safety Assessment and Management (PSAM 4)*, A. Mosleh and R.A. Bari (eds), Springer-Verlag, New York, 1998.

1.24 O. Strater and H. Bubb, "Assessment of human reliability based on evaluation of plant experience: requirements and implementation," *Reliability Engineering and System Safety*, 63: 199-219, 1998.

1.25 P.C. Cacciabue, F. Decortis, B. Drozdowicz, M. Masson, J.P. Nordvik, "COSIMO: A cognitive simulation model of human decision making and behavior in accident management of complex plants," *IEEE Transactions on Systems, Man and Cybernetics*, **22**(5): 1058-1074, 1992.

1.26 P. C. Cacciabue, Cojazzi, and P. Parisi, "A dynamic HRA method based on a taxonomy and a cognitive simulation model, in Probabilistic Safety Assessment and Management," P.C. Cacciabue and I.A. Papazoglou (eds.): Springer-Verlag, London, 1996

1.27 D.I. Gertman, H.S. Blackman, L.N. Haney, K.S. Seidler, H.A.Hahn, *INTENT: A Method for Estimating Human Error Probabilities for Errors of Intention*, EGG-SRE-9178, Rev. 1. 1990, Idaho National Engineering Laboratory, Idaho Falls, ID

1.28 Hollnagel, E., *Cognitive Reliability and Error Analysis Method (CREAM)*. York: Elsevier Science, New York, 1988.

1.29 F. Monseron-Dupin, B. Reer, G. Heslinga, O. Strater, V. Gerdes, G. Saliou, W. Ullwer, "Human-centered modeling in human reliability analysis: some trends based on case studies," *Reliability Engineering and System Safety*, 58: 249-274, 1997.

2 GENERAL DESCRIPTION OF THE ATHEANA METHOD

The ATHEANA method is an incremental extension of previous HRA methods to provide the capability of analyzing (both retrospectively and prospectively) the kinds of human-performance problems discussed in Section 1. It is organized around a multidisciplinary framework that is directly applicable to the retrospective analysis of operational events and provides the foundation for a prospective analysis. This section explains the HRA framework and summarizes the principles underlying the prospective application process.

2.1 The Multidisciplinary HRA Framework

As discussed in detail in NUREG/CR-6265 (Ref. 2.1) and Appendix B of NUREG/CR-6350 (Ref. 2.2), a multidisciplinary HRA framework was established early in the project to guide the development of ATHEANA. This section provides a brief review of the framework, emphasizing those aspects particularly relevant to the application of ATHEANA for both retrospective and prospective applications. The framework has also been used extensively to provide a systematic structure for analyzing the human–system interactions in operational events, including the causes and consequences of errors of commission (EOCs) as discussed in NUREG/CR-6265 and the event summaries in Appendix A.

The fundamental concept of the multidisciplinary HRA framework is that many unsafe actions are the result of combinations of plant conditions and associated PSFs that trigger "error mechanisms" in plant personnel. The framework provides a means for using the knowledge and understanding from the disciplines that are relevant to analyzing risk-significant human performance in NPP accidents, including plant operations and engineering, PRAs, human factors, and the behavioral sciences. Existing HRA methods incorporate some but not all of these disciplines, which has limited the kinds of insights any one method provided into human-performance issues. The HRA framework uses the relationships among these disciplines. In order to facilitate the use of these cross-disciplinary relationships, a limited amount of new terminology has been adopted to reduce some ambiguities from the terms in one discipline being used differently in another discipline (see the discussion concerning the term "human error" in Section 2.1.2 for an example).

Figure 2.1 is the graphic description of the framework, which includes elements from plant operations and engineering PRA, human factors engineering, and behavioral sciences perspectives. All of these contribute to our understanding of human reliability and its associated influences, and have emerged from the review of significant operational events at NPPs by a multidisciplinary project team representing all of these disciplines. The following are the framework elements:

- error-forcing context (EFC)
- performance-shaping factors
- plant conditions
- human error
- error mechanisms
- unsafe actions (UAs)

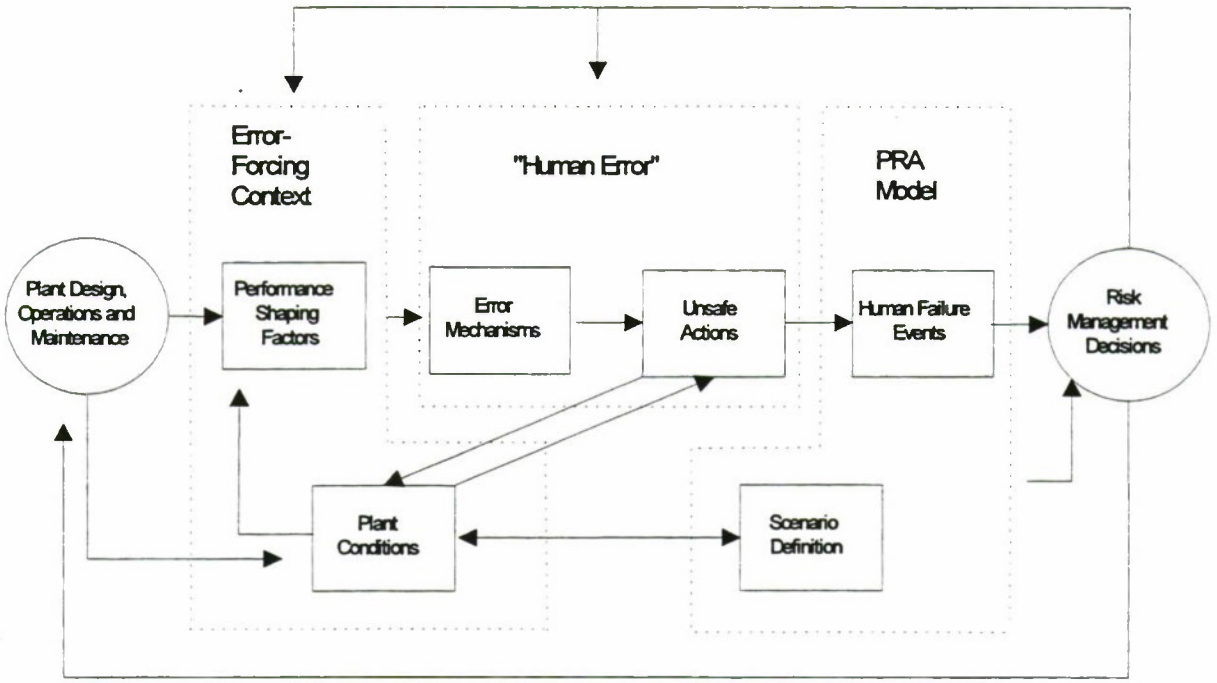


Figure 2.1 Multidisciplinary HRA Framework

- human failure events (HFEs)
- PRA model
- scenario definitions

These combined elements create the minimum set necessary to describe the causes and contributions of human errors in major NPP events. Figure 2.1 illustrates the interrelationships of these elements.

The human performance-related elements of the framework (i.e., those based principally on the human factors, behavioral sciences, and plant engineering disciplines) are reflected by the boxes on the left side of the figure; namely, performance-shaping factors, plant conditions, and error mechanisms. These elements represent the information needed to describe the underlying influences on unsafe actions and hence explain why a person may perform an unsafe action. The elements on the right side of the figure, namely, the HFEs and the scenario definition, represent the PRA model. The UA and HFE elements represent the point of integration between the HRA and PRA model. The PRA traditionally focuses on the consequences of the UA, which it describes as a human error that is represented by an HFE. The HFE is included in the PRA model associated with a particular plant state that defines the specific accident scenarios the model represents.

2.1.1 Error-Forcing Context

An *EFC* is the combined effect of PSFs and plant conditions that create a situation in which human error is likely. Analyses of NPP operating events reveal that the EFC typically involves an unanalyzed plant condition that is beyond normal operator training and procedure-related PSFs. The unanalyzed plant condition can activate a human error mechanism related to, for example, inappropriate situation assessment (i.e., a misunderstood regime). Consequently, when these plant

conditions and associated PSFs trigger internal psychological factors (i.e., error mechanisms), they can lead to the refusal to believe evidence that runs counter to the initial misdiagnosis, or the failure to recognize that evidence, resulting in subsequent mistakes (e.g., errors of commission) and ultimately a catastrophic accident.

PSFs represent the human-centered influences on human performance. Many of the PSFs used in this project are those identified in the human performance investigation process (HPIP) (NUREG/CR-5455, Ref. 2.3):

- procedures
- training
- communication
- supervision
- staffing
- human–system interface
- organizational factors
- stress
- environmental conditions

An example of a PSF is a procedure whose content is incorrect (e.g., wrong sequence of steps), incomplete (e.g., situation not covered), or misleading (e.g., ambiguous directions) and that contributes to a failure in situation assessment or response planning.

Plant conditions include plant configuration; systems component and instrumentation and control availability and reliability; process parameters (e.g., core reactivity, power level, and reactor coolant system temperature, pressure and inventory); and other factors (e.g., non-nominal or dynamic conditions) that result in unusual plant configurations and behavior. The following are some non-nominal plant conditions:

- history of false alarms and indications associated with a component or system involved in the response to an accident

- shutdown operations with instrumentation and alarms out of normal operating range and many automatic controls and safety functions disabled

- unusual or incorrect valve lineups or other unusual configurations

2.1.2 "Human Error"

A *"human error"* can be characterized as a divergence between an action performed and an action that should have been performed, which has an effect or consequence that is outside specific (safety) tolerances required by the particular system with which the human is interacting.

In the PRA community, the term "human error" has usually been used to refer to human-caused failures of a system or function. The focus is on the consequence of the error. In the behavioral sciences, the focus is on the underlying causes of the error. For the purpose of developing ATHEANA and to fully integrate it with the requirements of the PRA, the framework representation of human error encompasses both the underlying mechanisms of human error and the consequences of the error mechanism, which is the observable UA. For the remainder of this report, and in the application, we try to minimize the use of the term "human error" for two reasons. The first is its different connotation in the PRA and behavioral sciences fields, which limited some of the earlier dialogues between the groups.

Second, to some people, the term "error" has a connotation of placing blame on the people who took the action. We think that very few cases exist where operators took a UA and were, in any reasonable sense, to blame. Issues related to this, such as the meaning and significance of "a just culture" are beyond the considerations of ATHEANA. [Such issues are discussed at some length in, for example, Reason's Organizational Accidents" (Ref. 2.4)]. Therefore, we wish to avoid any debate on the significance of blameworthiness associated with the term "error" and we consider the kinds of unsafe actions analyzed in ATHEANA to be almost always the result of people being "set up."

Error mechanisms are used to describe the psychological mechanisms contributing to human errors that can be "triggered" by particular plant conditions and PSFs that lie within the PRA definitions of accident scenarios. These error mechanisms often are not inherently "bad" behaviors, but are mechanisms that generally allow humans to perform skilled and speedy operations. However, when applied in the wrong context, these mechanisms can lead to inappropriate actions with unsafe consequences. Different error mechanisms are influenced by different combinations of PSFs and plant conditions. Therefore, by considering specific error mechanisms, the analysis can be made more efficient because it can focus on specific PSFs and plant conditions relevant at the time.

Unsafe actions are those actions inappropriately taken by plant personnel, or not taken when needed, that result in a degraded plant safety condition. The term "unsafe action" does not imply that the human was the cause of the problem. Consequently, this distinction avoids any inference of blame and accommodates the assessment on the basis of the analysis of operational events that people are often "set up" by circumstances and conditions to take actions that were unsafe. In those circumstances, the person did not knowingly commit an error; they were performing the "correct" action as it seemed to them at the time.

While not all UAs identified in the analysis of operational events correspond to HFEs as defined in PRAs, in some cases there is a direct correspondence. For example, operators terminating the operation of needed engineered safety features would be performing a UA, and this action should be incorporated as an HFE in PRAs. More commonly though, UAs represent a "finer" level of detail than most HFEs defined in existing PRAs.

2.1.3 The PRA Model

The *PRA model* identified in the ATHEANA framework is no different from those used in existing PRA methodologies. However, in ATHEANA prospective analyses, the PRA model is an "end-user" of the HRA process. The PRA model is a means of assessing the risk associated with the NPP operation. It has as its basis logic models which consist of event trees and fault trees constructed to identify the scenarios that lead to unacceptable plant accident conditions, such as core damage. The PRA model is used to estimate the frequencies of the scenarios by converting the logic model into a probability model. To achieve this aim, estimates must be obtained for the probabilities of each event in the model, including human failure events. When human-performance issues are analyzed to support the PRA, it is in the context of HFEs applicable to a specific accident scenario defined by the plant state and represented by a PRA logic model.

HFEs are modeled in the PRA to represent the failure of a function, system, or component as a result of unsafe human actions that degrade the plant's safety condition. An HFE reflects the PRA systems analysis perspective and hence can be classified as either an EOC or an error of omission (EOO). An EOO typically represents the operator's failure to initiate a required safety function. An EOC represents either the inappropriate termination of a necessary safety function or an initiation of an inappropriate system. Examples of HFEs include the inappropriate termination of safety injection during a loss-of-coolant accident (an EOC) and the failure to initiate standby liquid coolant during an accident transient without scram (an EOO).

A basic event in the PRA model represents an uncorrected change in the status of the equipment affected within the context of the event definitions in the event tree model. To reflect the fact that the changes in a plant's state caused by human failures may not occur instantaneously, the HFEs are defined to represent not only the committing of an error but also the failure of the plant personnel to recognize that an error has been made, thereby inhibiting corrective action before the change in the plant state (within the definition of the event tree success criteria) has occurred. Depending on what the HFE is supposed to represent, HFEs may be associated with an event tree sequence or with specific minimal cut sets generated by the solution of a PRA model. The appropriate level of decomposition of the scenarios is that which is necessary to support the unique definition of an HFE with respect to the impact of the plant state on the probability of the HFE. Deciding on the appropriate level of definition is very much an iterative process.

PRA *scenario definitions* provide the minimum descriptions of a plant state required to develop the PRA model and define appropriate HFEs. The following examples illustrate typical elements of the PRA scenario definition:

- initiating event (e.g., transients, small-break loss-of-coolant accident, loss of offsite power)
- operating mode
- decay heat level (for shutdown PRAs)
- function/system/component status or configuration

The level of detail to which scenarios are defined can vary and include the following:

- functional level
- system level
- component state level (i.e., component successes or failure, or using the terminology of system analysts, cut sets)

2.2 The Approach for Analysis using ATHEANA

As discussed in Section 1, ATHEANA has been developed as a tool for resolving issues related to human performance. In NRC's move toward risk-informed regulation and inspection, this will often but not always involve the use of PRA models. ATHEANA has been developed to support PRA applications. However, it can be used as a qualitative assessment tool that involves relative rankings of alternatives, or even simply the identification of scenarios and EFCs, without requiring quantification of their contribution to measures of risk. For example, in earlier trials of ATHEANA, scenarios were identified that were potentially troublesome for operators. Based on that analysis, the plant participating in the trial has included the scenario in its operator training without requiring calculation of its contribution to core damage frequency. Therefore the ATHEANA application process recognizes the possibility of it being applied outside of the context of a PRA to identify and resolve issues.

Other sections of this document, particularly Sections 3 and 4, discuss important human-performance issues that must be addressed in the ATHEANA HRA method to achieve the improvements in HRA and PRA discussed in Section 1. As illustrated by past operational events, the issues that represent the largest departures from those addressed by current HRA methods all stem from the need to better predict and reflect the "real world" nature of failures in human–system interactions. Real operational events frequently include postaccident EOCs, which are minimally addressed in current HRA and PRAs and are strongly influenced by the specific context of the event (e.g., plant conditions and PSFs). In turn, the specific context of an event frequently departs from the nominal plant conditions assumed to prevail during at-power operations at NPPs.

Consequently, the HRA modeling approach adopted for ATHEANA differs significantly from current approaches. To be consistent with operational experience, the fundamental premise of ATHEANA is that significant postaccident HFEs, especially EOCs, represent situations in which the context of an event (e.g., plant conditions, PSFs) virtually forces operators to fail. ATHEANA's definition of HFEs and their quantification is on the basis of the EFC of the event, especially the unusual plant conditions. Many of the specific conditions of concern in ATHEANA are in the form of deviations from the plant behavior that the operators expect to see, or that form the basis of the plant procedures and training, creating mismatches between the expectations and the real plant behavior. This basis is a significant departure from that of traditional HRA methods in which HFEs are defined and quantified as being the result of random operator failures that occur under nominal accident-sequence conditions.

The ATHEANA modeling approach must involve a new quantification model. In particular, it must provide better and more comprehensive approaches to identifying and defining appropriate HFEs and placing them in the PRA model. As a result, new activities beyond those in traditional HRA methods are required when applying ATHEANA, which may identify HFEs not previously included in PRAs, together with the contributing UAs and associated EFCs. HRA analysts identify combinations of off-normal conditions and PSFs, that strongly increase the probability of UAs. Analysts are assisted by the understanding of the causes of human failures extracted from psychological literature and analyses of operational experience discussed in later sections. In addition, these identification activities require more interactions among HRA analysts, other PRA analysts, operations and training staff, and plant engineers. Finally, quantification of the probabilities of corresponding HFEs uses estimates of how likely or frequently the plant conditions and PSFs comprising the EFCs occur, rather than assumptions of randomly occurring human failures.

Beyond the elements outlined above, ATHEANA involves many of the same tasks that typically define a traditional HRA method. In terms of the functional elements of the PRA and HRA processes, the ATHEANA process requires the following tasks, which are listed generally in the sequence in which they are performed (with the understanding that the definition of the HFEs is usually an iterative process):

(1) Define and interpret the issue being analyzed.
(2) Define the resulting scope of the analysis.
(3) Describe base case scenarios.
(4) Define HFEs and UAs of concern.
(5) Identify potential vulnerabilities.
(6) Search for deviations from base case scenarios.
(7) Identify and evaluate complicating factors.
(8) Evaluate the potential for recovery.
(9) Interpret the results (including quantification if necessary).
(10) Incorporate into the PRA (if necessary).

When applying ATHEANA to a PRA, the representation of postaccident HFEs that are EOCs will be similar to the representation of EOOs already addressed by existing HRA methods (i.e., they will be identified and defined in terms of failed plant, system, or component functions). However, definitions of EOOs are based on failures of manual operator actions to initiate or change the state of plant equipment. Therefore, EOO definitions typically are phrased, for example, as "Operator fails to start pumps." EOCs must be defined differently since, generally, postaccident EOCs result from one of the following ways by which operators cause plant, system, or component functions to fail:

- by turning off running equipment
- by bypassing signals for automatically starting equipment

- by changing the plant configuration so it defeats interlocks that are designed to prevent damage to equipment

- by excessive depletion or diversion of plant resources (e.g., water sources)

For PRA models, the ATHEANA premise is to include only the HFEs for which a plausible and likely reason can be determined. An HFE may result from one of several UAs. Application of ATHEANA involves, for each HFE, identifying and defining UAs and associated EFCs. The identified EFCs (e.g., plant conditions and associated PSFs) and their underlying error mechanisms are the means of characterizing the causes of human failures. A UA could result from one of several different causes.

When applying ATHEANA, HFEs will be ranked on the basis of the probabilities of the contributing UAs, and these in turn on the basis of probabilities of the EFCs. Therefore, quantification of an HFE using ATHEANA is based on the answers to the following questions:

- What UA(s) can result in the HFE for which the probability is being quantified?
- What EFCs can result in committing each of the initial UAs?
- What EFC(s) can result in a failure to recover from each of the initial UAs?
- How likely are these EFCs to occur?

2.3 References

2.1 M. T. Barriere, W. J. Lucas, J. Wreathall, S. E. Cooper, D. C. Bley, and A. M. Ramey-Smith, *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis*, NUREG/CR-6265, Brookhaven National Laboratory, Upton, NY, August 1995.

2.2 Cooper, S. E., A. M. Ramey-Smith, J. Wreathall, G. W. Parry, D. C. Bley, W. J. Luckas, J. H. Taylor, and M. T. Barriere, A *Technique for Human Error Analysis (ATHEANA)*, NUREG/CR-6350, BNL-NUREG-52467, Brookhaven National Laboratory, May 1996.

2.3 M. Paradies, L. Unger, P. M. Haas, and M. Terranova, *Development of the NRCs Human Performance Investigation Process (HPIP)*, NUREG/CR-5455, System Improvements, Inc., Aiken, SC, October 1993.

2.4 J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate Press, Brookfield, VT, 1997.

3 THE IMPORTANCE OF PLANT CONDITIONS AND CONTEXT IN HUMAN PERFORMANCE

The reviews of accidents and serious incidents performed in this project, such as those described in Appendix A, have led to the identification, development, and ultimately to the confirmation of the principles underlying ATHEANA. One of the key aspects of ATHEANA is the recognition that plant conditions are a key influence on operator performance, and that these conditions can be much more varied than current combinations of HRA and PRA tools typically represent. This chapter discusses the reasons why ATHEANA has been developed to significantly expand the incorporation of particularly challenging plant conditions and the associated contexts faced by operators. It presents the general principles that underlie the way ATHEANA does this.

3.1 Current HRA and PRA Perspective

Most HRA analyses performed in current PRAs provide a limited recognition of the influences of plant behavior on human reliability. This comes about as a consequence of two inter-related features. First, in most applications of PRA models, analyses are performed for classes of initiating events (such as small loss-of-coolant accidents and transient reactor trips) and equipment faults, with only limited consideration given to variations of the initiating event and equipment failures. For example, only complete equipment failures are usually considered. This is partly a result of the use of fundamentally binary success or failure models that lie at the center of almost all PRA modeling methods and that tend to lead to the need for simplifications in the complexity of real plant conditions. In the PRA analysis, the "most challenging" version of the initiating event is often assumed; here "most challenging" is usually used with respect to the demands made on equipment, such as the largest number of pumps and the shortest time scale for them to start to prevent core damage. This approach is often considered to be conservative, and it may well be with respect to demands on equipment performance and physical resources. However, as discussed below and in Section 4, these conditions may well not be the most challenging in terms of the demands on the operator in responding to the event.

Second, most HRA methods currently used are very limited in terms of their ability to take into account different plant conditions. Some methods can take into account differences in the time scales available for operator response. Most other methods can take into account the performance-shaping factors (PSFs) such as the layout of procedures, the location and number of displays, and the experience level of the operators. However, very few of these factors provide the most important variations in the conditions under which people perform and which are found to be very challenging. In summary, both the PRA approach of analyzing wide ranges of conditions using "conservative" all-embracing models and assumptions, and the lack of sensitivity of HRA methods to changes in plant conditions, have led to the lack of explicit consideration of ranges of plant conditions in most PRAs. (It is recognized that attempts to consider some ranges of plant conditions have been made in a few PRAs, such as where some accident sequences that have significantly different time scales for actions are addressed separately. However, the insensitivity of the available HRA tools has limited the analyst's ability to take into account anything other than simple time-scale differences.)

3.2 The Significance of Context

Recent work in the behavioral sciences (such as that in Ref. 3.1 and Ref. 3.2) has contributed to the understanding of the interactive nature of human errors and plant behavior that characterize accidents in high-technology industries. This understanding suggests that it is essential to analyze both the human–centered factors (e.g., PSFs such as human–machine interface design, content and format of plant procedures and training) and the conditions of the plant that call for actions and create the operational causes for human–system interactions (e.g., misleading indicators, equipment unavailabilities, and other unusual configurations or operational circumstances).

The human-centered factors and the influence of plant conditions are not independent of each other. In many major accidents, particularly unusual plant conditions create the need for operator actions and, under those unusual plant conditions, deficiencies in the human-centered factors lead people to make errors in responding to the incident.

Therefore the typical evaluations performed in HRA assessments of PSFs, such as procedures and human–machine interfaces and training (as discussed above) may not identify critical human-performance problems unless consideration is also given to the range of plant conditions under which the controls or indicators may be required. To identify the most likely conditions leading to failure, the analysis of PSFs must recognize that plant conditions can vary significantly within the event-tree or fault-tree definition of a single PRA scenario. Moreover, some plant conditions can be much more demanding of operators than others. Both the conditions themselves and the limitations in PSFs, such as procedures and training, can affect an operator's performance during an accident.

For example, a particular layout of indicators and controls may be perfectly adequate for the nominal conditions assumed for a PRA scenario. However, deviations from the conditions implicitly or explicitly assumed for the PRA scenario possibly may occur so that specific features of the layout would influence the occurrence of operator errors in an accident response. An example of such a deviation was the location of the breach in the Three Mile Island-2 (TMI-2) accident. The typical conditions assumed for a small loss-of-coolant accident (the type of PRA scenario representing the TMI-2 accident) included a falling pressurizer level, but not the position indications of the pressurizer power-operated relief valves (PORVs). However, the deviation created by a leak in the pressurizer PORVs made these indications much more important.

Simply stated, operator failures associated with a PRA scenario are perhaps more likely to result from particular deviations from typical plant conditions that create significant challenges to the operators than they are from "random" human errors that might occur under the single set of conditions generally assumed by PRA analysts. Analyses of power plant accidents and near-misses support this perspective, indicating that the influence of unusual plant conditions is much more significant than random human errors [NUREG/CR-1275, Vol. 8 (Ref. 3.3), NUREG/CR-6093 (Ref. 3.4), NUREG/CR-6265 (Ref. 3.5), and NUREG/CR-6350 (Ref. 3.6)]. The need for consideration

of context has been a recurrent theme in discussions about improved HRA methods, including those by Hall et al. (Ref. 3.7), Dougherty (Ref. 3.8), Woods (Ref. 3.9), and Hollnagel (Ref. 3.10).

The significance of unusual contexts derived from incident analyses is consistent with experience described by training personnel. They have observed that operators can be "made to fail" in simulator exercises by creating particular combinations of plant conditions and operator mindset. Examples of difficulties in operator performance in challenging simulator training situations are given in NUREG/CR-6208 (Ref. 3.11).

Our review of operating events, particularly those that seem to have the potential for serious degradations of safety, has shown that these events involve various types of deviations that cause significant challenges to the operators. There are several types of such deviations from the typical conditions assumed in the PRA scenarios. Examples include:

- Physical deviations, in which the plant behaves differently than is typically expected in the related PRA scenario and which affect the way the plant behaves compared with the operator's training and expectations. These may cause the indications of the plant condition to be significantly different from the operators' expectations and may not match those used in development of procedures and operator training.

- Temporal deviations, in which the time scales of the plant conditions are different from those typically assumed in the related PRA scenario and may affect the time scales in which operators must act. These may cause symptoms to occur significantly more slowly or be out of sequence with those assumed in procedures and in training, thus causing doubt about the relevance or effectiveness of the expected responses. Alternatively, the conditions may occur much faster than expected, thereby inducing high levels of stress in the operators or leading to failure while the operators are systematically stepping through their procedures.

- Deviations in the causes of initiating events, in which partial equipment failures or failures in support systems occur, thus creating complex sets of unexpected symptoms that may lead operators to act inappropriately or to delay taking action. When support-system failures are explicitly incorporated in PRA models, they are often focused on complete or single-train losses and are concerned with the impact on plant hardware, not on the operators being confused or misled by the failures.

- Deviations associated with failures in instrumentation systems can make it difficult for operators to understand and plan suitable responses. While some PRAs may incorporate some kinds of instrumentation failures that lead, for example, to automatic equipment not being started when needed or interlocks that prevent correct operator actions, there has been very little consideration of how instrument faults will affect the ability of the operators to understand the conditions within the plant and act appropriately. In addition, failures of the instrumentation and control systems can bring about the kinds of deviations discussed above.

In many cases, these types of deviations can lead operators to fail because of some kind of "mismatch." For example, when a plant behaves in a way that is significantly different from the operators' expectations (a mismatch between plant behavior and training), and the operators respond in accordance with their expectations, the resultant actions can lead to loss of important equipment operation and functions for the conditions actually taking place. The operators' belief that the reactor system was "going solid" at TMI-2 led them to reduce and stop high-pressure injection, which led to the loss of core cooling and damage. More recent examples from operating experience discussed below indicate that despite the changes in training, development of procedures, and the like, mismatches are still a concern in operations.

The idea of a "mismatch" has proved a useful concept for describing several kinds of problems underlying events, and provides one basis for searching for problem scenarios. In the discussion of operating experiences summarized in Appendix A, for example, the types of mismatch that contributed to the performance problems are described.

To provide an effective tool for measuring and controlling risk, a PRA must be able to realistically incorporate those human failures that are caused by off-normal plant conditions, as well as those that occur randomly during nominal accident conditions. In the ATHEANA application process, the concept of mismatches is used to provide a basis for the searches for challenging conditions. Particularly important types of mismatches are used to identify specific contexts that may cause failures. Four specific types of searches are used in Step 6 of the prospective application process:

(1) searches that use keywords to prompt the analysts to consider types of physical deviations from the standard, or base case, accident conditions (for example; larger, smaller, faster, slower)

(2) searches that examine the key decision points in related procedures to see if deviations from the base case scenario could lead to inappropriate actions (this is similar in concept to the approach developed by Julius et al. described in Section 1.5, for full-power applications, though their focus was to identify instrumentation errors that could induce the same kinds of failures)

(3) searches for possible dependencies between equipment faults and support system failures. Such dependencies can create cognitively challenging situations because:

- their effects can be very plant specific and therefore operators are unlikely to have learned relevant lessons about them from other plants' experiences

- the consequences of the dependencies will often appear as seemingly independent multiple failures in both balance-of-plant and safety equipment

- partial failures in support systems can create abnormal conditions in the equipment they support that are difficult to identify and understand

(4) searches that try to identify other causes of deviations beyond those listed above. This is an attempt at accomplishing relative "completeness." ATHEANA provides tables and structures to help the analyst think of causes of EFCs beyond those listed here.

The identification of important mismatches and associated EFCs is largely based on an understanding of the kinds of psychological mechanisms causing human errors that can be "set up" by particular plant conditions lying within the PRA definitions of accident scenarios. Section 4 discusses these mechanisms, the background in the behavioral sciences on which these mechanisms are based, and the basis for identifying their likely effect on operator behavior.

3.3 Examples of the Effects of Plant Conditions and Context on Operations

Many events, including some non-nuclear power plant events, were reviewed in developing ATHEANA. These analyses used the multidisciplinary HRA framework as a guide to the important factors influencing human performance. In some cases the events were analyzed in detail, using event reports recorded in the Human-System Event Classification Scheme (HSECS) database (Ref. 3.12) and are summarized next. In other cases, relevant information was extracted from analyses by others and used to support the development work; these are described later in this section.

3.3.1 ATHEANA Reviews of Events

Reviews of four events are used to illustrate the insights gleaned from event analyses. All four involve important postaccident human errors, which are the focus of ATHEANA:

(1) *TMI-2 (Refs. 3.13 and 3.14)*: On March 3, 1979, a loss of feedwater transient (as a result of personnel errors outside the control room) and a reactor trip occurred. The emergency feedwater (EFW) pumps started automatically, but misaligned valves prevented flow to the steam generators. A maintenance tag obscured the operators' view of an indicator showing that these valves were closed. A relief valve opened automatically in response to increasing pressure and temperature, and stuck open. However, the control room indicator showed that the relief valve was closed. Operators failed to recognize that the relief valve was open for more than 2 hours, resulting in water loss from the reactor vessel. In addition, operators reduced high-pressure injection flow to the reactor vessel for 3 ½ hours because of concerns about flooding the core and "solid" reactor coolant system conditions, resulting in significant core undercooling. Serious core damage resulted from the open relief valve and reduced coolant flow. The event was terminated after a shift change of personnel, who discovered the open relief valve.

(2) *Crystal River 3 (Ref. 3.15)*: On December 8, 1991, a reactor coolant system (RCS) pressure transient occurred during startup following a reactor power increase. A pressurizer spray valve opened automatically and stuck open. However, the control room indicator showed that the spray valve was closed. Operators failed to recognize that the spray valve was open. Believing the drop in pressure was a result of an unexplained cooldown, the operators pulled

rods to increase power. They expected that increasing RCS temperature would create an in-surge into the pressurizer, which in turn would restore pressure. However, RCS pressure continued to decrease, resulting in a reactor trip. After the reactor trip, RCS pressure continued to decrease, reaching setpoints for arming the engineered safety features (ESF) system. Circumventing procedural guidance, the operators bypassed ESF for 6 minutes in anticipation of terminating the transient. The control room supervisors directed operators to take ESF out of bypass and the high-pressure injection system automatically started. RCS pressure was controlled with high-pressure injection. The pressure transient was terminated after the pressurizer spray line isolation valve was closed at the suggestion from a supervisor that it might be helpful.

(3) *Salem 1 (Ref. 3.16)*: On April 7, 1994, a loss of circulating water, a condenser vacuum transient, and an eventual reactor trip occurred as a result of a severe intrusion of grass into the circulating water intake structure. A partial (i.e., only train A) erroneous safety injection (SI) signal was generated because of preexisting hardware problems after the reactor trip, requiring operators to manually position many valves that normally actuate automatically. Operators failed to control the high-pressure injection (HPI) flow to the reactor vessel. After more than 30 minutes passed, the pressurizer filled solid and the pressurizer relief valves actuated repeatedly. The operators then terminated the HPI. As a result of operator inattention and preexisting hardware failures, the steam generator pressure increased concurrently with the pressurizer level, causing the steam generator's safety relief valves to open. Following this, a rapid depressurization occurred, followed by a second SI actuation and more pressurizer relief valve openings.

(4) *Oconee 3 (Ref. 3.17 and Ref. 3.18)*: On March 8, 1991, decay heat removal was lost for about 18 minutes during shutdown because of a loss of RCS inventory. The RCS inventory was diverted to the emergency sump via a drain path created by the combination of a blind flange installed on the wrong sump isolation line and testing of a sump isolation valve stroke. Operators aligned residual heat removal pumps to the refueling water storage tank (RWST) in an attempt to restore reactor vessel level. When the vessel level did not rise, operators isolated the RWST and sent an auxiliary operator to close the sump isolation valve. Approximately 14,000 gallons of coolant were drained to the sump and spilled onto the containment floor (i.e., 9,700 gallons of RCS inventory and about 4,300 gallons of RWST inventory).

Elements of each of these events illustrate the importance of the concepts underlying ATHEANA. For example, three of these events involved postaccident errors of commission (EOC). In TMI-2, the throttling of high- pressure injection was an EOC that resulted in serious core damage. In Crystal River 3, the bypass of ESF was an EOC that prevented automatic injection of coolant into the reactor core. However, this operator action was recovered without core damage occurring. In Oconee 3, the alignment with the RWST before the drain path to the sump was isolated resulted in additional coolant being lost. Consequently, this action was an EOC that also was recovered before the event was terminated. In addition, three of these events (Crystal River 3, Salem 1, and Oconee 3) involved EOCs that either occurred just before the reactor trip or caused the reactor trip.

Context played an important role in all of these events. In TMI-2, plant conditions that contributed to the event included the preexisting misalignment of EFW valves and the stuck-open relief valve. These combined with negative performance-shaping factors, including the maintenance tag obstructing the position indicator for the EFW valve, a misleading relief valve position indicator, and lack of procedural guidance for the event-specific conditions. Other indications of the open relief valve were either misinterpreted or discounted by operators. In addition, operator training emphasized the dangers of "solid" plant conditions, causing operators to focus on the wrong problem. The Crystal River 3 incident involved similar factors, especially the open spray valve and the associated misleading position indicator. There was no procedural guidance to support the diagnosis and correction of a loss of RCS pressure control. In the Oconee 3 event, operators did not have a position indicator because the isolation valve (which ultimately created the drain path) was racked out for stroke testing. Also, the erroneously installed blind flange was a temporary obstruction that remained undiscovered despite several independent checks. On the one hand, various instrumentation (e.g., reactor vessel-level indicators and alarms) indicated a falling vessel level of the reactor in the Oconee 3 event, which operators discounted until field reports from technicians in the containment confirmed that the level was falling and radiation levels were increasing. On the other hand, the Salem 1 event involved different contextual factors, principally the partial, erroneous SI signal, which was generated by preexisting hardware problems and which required the operators to manually align several valves. Also, there was no procedural guidance regarding appropriate actions in response to a disagreement with the SI train logic.

Applying the information processing model concepts to these events reveals that situation assessment was critical in all of them. In TMI-2, operators did not recognize that the relief valve was open and that the reactor core was overheating. In Crystal River 3, operators did not recognize that the pressurizer spray valve was open and causing the pressure transient. In the Salem 1 event, operators failed to recognize and anticipate the pressurizer overfill, steam generator pressure increases, and the rapid depressurization following the opening of steam generator safety valves. Finally, in Oconee 3, operators did not recognize that a drain path to the sump existed until eyewitness reports were provided. These situation assessment problems involved either the sources of information (e.g., instrumentation) or their interpretation. In TMI-2, operators misread the temperature indicator for relief valve drain pipe twice thus attributing the high in-core and RCS loop temperatures to faulty instrumentation. They also were misled by the control room indicator's position for the status of the relief valve. Also, some key indicators were located on back panels and the computer printout of plant parameters ran more than 2 hours behind the event. In Crystal River 3, operators initially conjectured that the pressure transient was caused by RCS shrinkage. Unconnected plant indicators, as well as the misleading indication of spray valve position and (unsuccessful) cycling of the spray valve control, were taken as supporting this hypothesis. In Oconee 3, operators suspected that the indication of a decreasing reactor vessel level was a result of faulty operation. Two sump high-level alarms were attributed to possible washdown operations. As noted above, field reports eventually convinced operators to believe that their instrumentation was functioning correctly.

3.3.2 Other Analyses of Operational Events

Several independent studies of accidents, including those cited above, support the principles underlying ATHEANA. In addition, discussions with those who have analyzed transportation and aviation accidents (Ref. 3.1) and reviews of accidents at chemical plants (Ref. 3.20) indicate that an error-forcing context is most often present in serious accidents involving human operational control in these industries. Reason (Ref. 3.1) identified important contextual factors in several major accidents, including the accident at TMI-2 and the Challenger shuttle explosion in January 1986. Analyses of NPP incidents in Volume 8 of NUREG-1275 (Ref. 3.3) identified non-nominal plant conditions, and associated procedural deficiencies for these conditions, as strongly influencing 8 of 11 events that were significantly affected by human actions. Of the 11 events, 6 involved EOCs. The NRC AEOD report, *Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features* (AEOD/E95-01, Ref. 3.21), identified 14 events over the past 41 months in which ESF was inappropriately bypassed, all of which are EOCs. NUREG/CR-6208 (Ref. 3.7) identified situation assessment and response planning as important factors in simulator experiments involving cognitively demanding situations (i.e., situations not fully covered by procedures or training because the plant conditions for the specific, simulated event were different from the nominal). Also, in the Electric Power Research Institute (EPRI)-sponsored Operator Reliability Experiment (ORE) program, 70% of the operating crew errors or near-misses observed in the simulator experiments, regardless of plant type, were categorized as information processing or diagnosis and decision-making" errors (Ref. 3.22).

3.4 References

3.1 J. Reason, *Human Error*, Cambridge University Press, New York, 1990.

3.2 E. Hollnagel, *Reliability of Cognition: Foundations of Human Reliability Analysis*, Plenum Press, New York, 1993.

3.3 U.S. Nuclear Regulatory Commission, *Operating Experience Feedback Report - Human Performance in Operating Events*, NUREG-1275, Vol. 8, Washington, DC, December 1992.

3.4 M. T. Barriere, W. J. Luckas, D. W. Whitehead, and A. M. Ramey-Smith, *An Analysis of Operational Experience During LP&S and A Plan for Addressing Human Reliability Assessment Issues*, Brookhaven National Laboratory, and Sandia National Laboratories, NUREG/CR-6093, Albuquerque, NM, Upton, NY, June 1994.

3.5 M. T. Barriere, W. J. Luckas, J. Wreathall, S. E. Cooper, D. C. Bley, and A.M. Ramey-Smith, *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis*, NUREG/CR-6265, Brookhaven National Laboratory, Upton, NY, August 1995.

3.6 S. E. Cooper, A. Ramey-Smith, J. Wreathall, G. W. Parry, D. C. Bley, J. H. Taylor, W. J. Luckas, *A Technique for Human Error Analysis (ATHEANA),* NUREG/CR-6350, Brookhaven National Laboratory, Upton, NY, April 1996.

3.7 R. E. Hall, J. Fragola, and J. Wreathall, *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, NUREG/CR-3010, Brookhaven National Laboratory, Upton, NY, November 1982.

3.8 E. M. Dougherty, "Guest editorial: Human reliability analysis–Where shouldst thou turn?" *Reliability Engineering and System Safety*," **29**: 283-299, 1990.

3.9 D. D. Woods, "Risk and human performance: Measuring the potential for disaster," *Reliability Engineering and System Safety*, **29**: p. 387-405, 1990.

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

3.11 E. M. Roth, R. J. Mumaw, and P. M. Lewis, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, Westinghouse Science and Technology Center, Pittsburgh, PA, NUREG/CR-6208, July 1994.

3.12 S. E. Cooper, W. J. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report No. L2415/95-1, Brookhaven National Laboratory, Upton, NY, December 1995.

3.13 J. Kemeny, *The Need for Change: Report of the President's Commission on the Accident at Three Mile Island*, Pergamon Press, New York, 1979.

3.14 M. Rogovin, and G. Frampton, Special Inquiry Group, Nuclear Regulatory Commission *Three Mile Island - A Report to the Commissioners and to the Public*, Washington, DC, January 1980.

3.15 U.S. Nuclear Regulatory Commission, AEOD (Human Factors Team) Report, Crystal River, Unit 3 - December 8, 1991, *On-Site Analysis of the Human Factors of an Event (Pressurizer Spray Valve Failure)*, Washington, DC, January 1992.

3.16 U.S. NRC, Augmented Inspection Team Report, Salem Unit 1, April 7, 1994, *Loss of Condenser Vacuum (and Loss of Pressure Control - RCS Filled Solid)*, Report No. 50-272/94-80 and 50-311/94-80, Washington, DC, 1994.

3.17 U.S. Nuclear Regulatory Commission, Augmented Inspection Team Report, No. 50-287/91-008, Oconee, Unit 3, *Loss of RHR (March 9, 1991)*, Augmented Inspection Team Report, Washington, DC, April 10, 1991.

3.18 U.S. Nuclear Regulatory Commission, AEOD (Human Factors Team) Report, Oconee, Unit 3 - March 9, 1991, *On-Site Analysis of the Human Factors of an Event (Loss of Shutdown Cooling)*, May 1991.

3.19 National Transportation Safety Board, *National Transportation Safety Board Safety Study: A Review of Flight Crew-Involved in Major Accidents of U.S. Air Carriers*, 1978-1990, NTSB/SS-94/01, Washington, DC, 1994.

3.20 T. A. Kletz, *What Went Wrong? Case Histories of Process Plant Disasters*, Gulf Publishing, Houston, TX, 1985.

3.21 U.S. Nuclear Regulatory Commission, *Engineering Evaluation - Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features*, Office of Analysis and Evaluation of Operational Data (AEOD), AEOD/E95-01, Washington, DC, July 1995.

3.22 A. N. Beare, A. N., C. D. Gaddy, G. W. Parry, and A. J. Singh, "An Approach for Assessment of the Reliability of Cognitive Response for Nuclear Power Plant Operating Crews," in G. Apostolakis (ed.) *Probabilistic Safety Assessment & Management (PSAM)*, Elsevier Science, New York, 1991.

4 BEHAVIORAL SCIENCE PERSPECTIVE

As discussed in Sections 2 and 3 of this report, one part of the framework underlying the ATHEANA method is the relationship between unsafe actions, error mechanisms, and error-forcing contexts. The information required to describe this relationship is provided by two parallel and complementary sources, including (1) an understanding of human failures derived from models of human behavior created within the behavioral sciences discipline and (2) an analysis of operational events.

There have been many attempts over the past 30 years to better understand the causes of human error. The main conclusion from these works is that few human errors represent random events; instead, most can be explained on the basis of the ways in which people process information in complex and demanding situations. Thus, it is important to understand the basic cognitive processes associated with plant monitoring, decision-making, and control, and how these can lead to human error. A number of good discussions of the cognitive factors associated with human performance and error in complex dynamic tasks are available in the literature (listed in the bibliography in Section 4.6). The main purpose of this section is to describe the relevant models in the behavioral sciences, the mechanisms leading to failures, and the contributing elements of error-forcing contexts in power plant operations. The discussion is largely based on the work of Woods, Roth, Mumaw, and Reason (Refs. 4.1-4.5).

The basic model underlying the work described in this section is the information processing model that describes the range of human activities required to respond to abnormal or emergency conditions. The model, in the form used in this application, considers actions in response to abnormalities as involving basically four cognitive steps:

(1) situation assessment
(2) monitoring/detection
(3) response planning
(4) response implementation

4.1 Analysis of Operator Cognitive Performance

Figure 4.1 illustrates the major cognitive activities that underlie operator performance, and the remainder of this subsection discusses them.

4.1.1 Situation Assessment

When confronted with indications of an abnormal occurrence, people actively try to construct a coherent, logical explanation to account for their observations. This process is referred to as *situation assessment*. Situation assessment involves developing and updating a mental representation of the factors known, or hypothesized, to be affecting plant state at a given point in time. The mental representation resulting from situation assessment is referred to as a *situation model*. The situation model is the person's understanding of the specific current situation, and the model is constantly updated as new information is received.

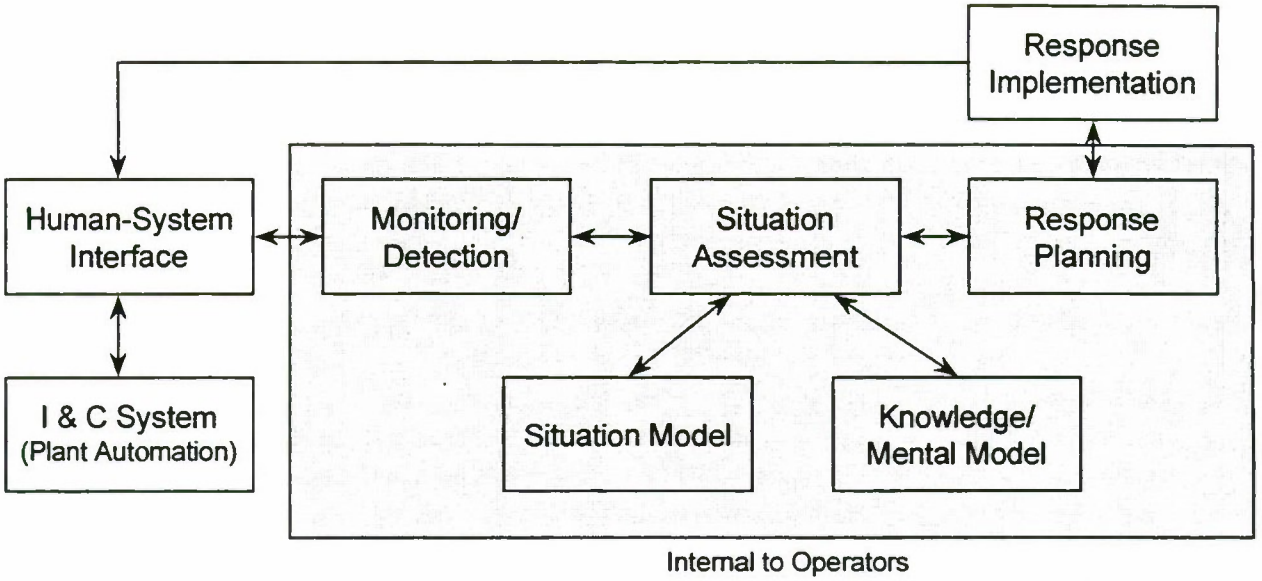


Figure 4.1 Major Cognitive Activities Underlying NPP Operator Performance

Situation assessment is similar in meaning to "diagnosis," but is broader in scope. Diagnosis typically refers to searching for the cause(s) of abnormal symptoms. Situation assessment encompasses explanations that are generated to account for normal as well as abnormal conditions.

Operators use their general knowledge and understanding about a plant and how it operates to perform situation assessment and generate a situation model. Operator knowledge takes the form of relatively permanent memory representations that are built upon through training and experience. Operator knowledge can range from detailed knowledge of specific events to relatively abstract, generalizable principles that are applicable to a broad class of situations. Types of knowledge that are significant to performance include the following:

- Episodic knowledge refers to detailed memories of specific past events, including events the individual has experienced personally as well as events he or she has heard about.

- Stereotypic knowledge refers to knowledge about "typical" or "textbook" cases, as opposed to knowledge of specific past cases. Stereotypic knowledge can be developed by forming an abstract representation on the basis of the general aspects of specific similar past events that are representative of a class of situations. This type of knowledge is also gained from training and exercises in simulators. Using this type of knowledge, for example, operators may diagnose a LOCA event though the specific situation they are confronted with is not exactly the same as one experienced during training.

- Mental models refer to mental representations that capture a person's understanding of how a system works. A key feature of a mental model is that it is "runable." A mental model

enables a person to mentally simulate system performance to predict system behavior. Nuclear power plant examples include using knowledge of the physical interconnections among plant systems to predict flow paths (e.g., considering piping and valve interconnections to figure out how water from one system could get into another), and using knowledge of mass and energy changes in one system to predict the effect on a second system (e.g., predicting the effect of cooldown in the primary system on the behavior of secondary side steam generator level).

- Procedural knowledge addresses strategies for dealing with events. This includes knowledge of procedures and how and when to use them, knowledge of formal processes and practices for responding to situations, as well as knowledge of informal practices for responding to situations. This type of knowledge can also exist in nearly episodic form (i.e., knowledge of limited generalizability that addresses a specific step-by-step sequence that can be used so long as nothing deviates from the episodic representation of the situation). Procedural knowledge can also be quite abstract so that it can be applied broadly and can be used to adapt or generate new response plans should the specific conditions deviate from the ideal.

Long-term knowledge is drawn upon when generating and updating a situation model. It is important to note that operator knowledge may not be fully accurate or complete. For example, mental models often include oversimplifications or inaccuracies. Limitations in knowledge will result in incomplete or inaccurate situation models or response plans.

Situation models are constantly updated as new information is received and as a person's understanding of a situation changes. In power-plant applications, maintaining and updating a situation model entails tracking the changing factors that influence plant processes, including faults, operator actions, and automatic system responses.

Situation models are used to form *expectations*, which include the events that should be happening at the same time, how events should evolve over time, and effects that may occur in the future. People use expectations in several ways. Expectations are used to search for evidence to confirm the current situation model. People also use expectations they have generated to explain observed symptoms. If a new symptom is observed that is consistent with their expectations, they have a ready explanation for the finding, giving them greater confidence in their situation model.

When a new symptom is inconsistent with their expectation, it may be discounted or misinterpreted in a way to make it consistent with the expectations derived from the current situation model. For example, there are numerous examples where operators have failed to detect key signals, or detected them but misinterpreted or discounted them, because of an inappropriate understanding of the situation and the expectations derived from that understanding.

However, if the new symptom is recognized as an *unexpected plant behavior*, the need to revise the situation model will become apparent. In that case, the symptom may trigger a situation assessment activity to search for a better explanation of the current observations. In turn, situation assessment

may involve developing a hypothesis for what is occurring and then searching for confirmatory evidence in the environment.

Thus, a situation assessment can result in the detection of abnormal plant behavior that might not otherwise have been observed, the detection of plant symptoms and alarms that may have otherwise been missed, and the identification of problems such as sensor failures or plant malfunctions.

The importance of situation models, and the expectations that are a result of them, cannot be overemphasized. Situation models not only govern situation assessment, but also play an important role in guiding monitoring, in formulating response plans, and in implementing responses. For example, people use expectations generated from situation models to anticipate potential problems and to generate and evaluate response plans.

4.1.2 Monitoring and Detection

Monitoring and detection refer to the activities involved in extracting information from the environment. They are influenced by two fundamental factors: the characteristics of the environment and a person's knowledge and expectations.

Monitoring that is driven by characteristics of the environment is often referred to as *data-driven* monitoring. Data-driven monitoring is affected by the form of the information, its physical salience (e.g., size, color, loudness, etc.). For example, alarm systems are basically automated monitors that are designed to influence data-driven monitoring by using aspects of physical salience to direct attention. Characteristics such as an auditory alert, flashing, and color coding enable operators to quickly identify an important new alarm. Data-driven monitoring is also influenced by the behavior of the information being monitored, such as the bandwidth and rate of change of the information signal. For example, observers monitor a signal that is rapidly changing more frequently.

Monitoring can also be initiated by the operator on the basis of his or her knowledge and expectations about the most valuable sources of information. This type of monitoring is typically referred to as *knowledge-driven monitoring*. Knowledge-driven monitoring can be viewed as "active" monitoring in that the operator is not merely responding to characteristics of the environment that "shout out" like an alarm system does, but is deliberately directing attention to areas of the environment that are expected to provide specific information.

Knowledge-driven monitoring typically has two sources. First, purposeful monitoring is often guided by specific procedures or standard practice (e.g., control panel walk-downs that accompany shift turnovers). Second, knowledge-driven monitoring can be triggered by situation assessment or response planning activities and is therefore strongly influenced by a person's current situation model. The situation model allows the operator to direct attention and focus monitoring effectively. However, knowledge-driven monitoring can also lead operators to miss important information. For example, an incorrect situation model may lead an operator to focus his attention in the wrong place, fail to observe a critical finding, or misinterpret or discount an indication.

Typically, in power plants an operator is faced with an information environment containing more variables than can realistically be monitored. Observations of operators under normal operating conditions, as well as emergency conditions, make it clear that the real monitoring challenge comes from the fact that there are a large number of potentially relevant things to attend to at any point in time and that the operator must determine what information is worth pursuing within a constantly changing environment. In this situation, monitoring requires the operator to decide what to monitor and when to shift attention elsewhere. These decisions are strongly guided by an operator's current situation model. The operator's ability to develop and effectively use knowledge to guide monitoring relies on the ability to understand the current state of the process.

Under normal conditions, situation assessment is accomplished by mapping the information obtained in monitoring to elements in the situation model. For experienced operators, this comparison is relatively effortless and requires little attention. During unfamiliar conditions, however, the process is considerably more complex. The first step in realizing that the current plant conditions are not consistent with the situation model is to detect a discrepancy between the information pattern representing the current situation and that detected from monitoring activities. This process is facilitated by the alarm system which helps to direct the attention of a plant operator to an off-normal situation.

When determining whether a signal is significant and worth pursuing, operators examine the signal in the context of their current situation model. They form judgments with respect to whether the anomaly signals a real abnormality or an instrumentation failure. They will then assess the likely cause of the abnormality and evaluate the importance of the signal in determining their next course of action, if action is needed.

4.1.3 Response Planning

Response planning refers to the process of making a decision as to what actions to take. In general, response planning involves the operators' using their situation model of the current plant state to identify goals, generate alternative response plans, evaluate response plans, and select the most appropriate response plan to the current situation model. While this is in the basic sequence of cognitive activities associated with response planning, one or more of these steps may be skipped or modified in a particular situation. For example, in many cases in NPPs, when written procedures are available and judged appropriate to the current situation, the need to generate a response plan in real-time may be largely eliminated. However, even when written procedures are available, some aspects of response planning will still be performed. For example, operators still need to perform the following four steps:

(1) Identify appropriate goals on the basis of their own situation assessment.
(2) Select the appropriate procedure.
(3) Evaluate whether the procedure defined actions are sufficient to achieve those goals.
(4) Adapt the procedure to the situation if necessary.

It is important for operators to monitor the effectiveness of the response plan, even when it is described by established procedures. Monitoring includes evaluating the consequences of particular procedural actions and evaluating the appropriateness of the procedure path for achieving identified goals. This enables operators to detect when procedures are not achieving the desired goals, when they may contain errors, or when errors were made in carrying out procedure steps.

Another cognitive activity included under response planning is response plan adaptation. This includes filling in gaps in a procedure, adapting a procedure to the specific situation, and redirecting the procedure path.

4.1.4 Response Implementation

Response implementation refers to taking the specific control actions required to perform a task. It may involve discrete actions (e.g., flipping a switch) or continuous control activity (e.g., controlling steam generator level). It may be performed by a single person or it may require communication and coordination among multiple individuals.

The results of actions are monitored through feedback loops. Two aspects of NPPs can make response implementation difficult: time response and indirect observation. The plant processes cannot be directly observed, instead they are inferred through indications and thus errors can occur in the inference process. Nuclear power plant systems are also relatively slow to respond compared with other types of systems, such as aircraft. Since time and feedback delays are disruptive to executing a response (because they make it difficult to determine that control actions are having their intended effect), the operator's ability to predict future states using mental models can be more important in controlling responses than feedback.

In addition, response implementation is related to the cognitive task demands. When the response demands are incompatible with response requirements, operator performance can be impaired. For example, if the task requires continuous control over a plant component, then performance may be impaired when a discrete control device is provided. Such mismatches can increase the chance of errors being made. Another factor is the operator's familiarity with the activity. If a task is routine, it can be executed automatically, thus requiring little attention.

4.2 Cognitive Factors Affecting Operator Performance

Three classes of cognitive factors affect the quality of output of the major cognitive activities thereby affecting operator performance. They are knowledge, processing resource, and strategic factors. Errors arise when there is a mismatch between the state of these cognitive factors (i.e., the cognitive resources available to the operator) and the demands imposed by the situation. This section addresses how these cognitive factors affect the operator's cognitive performance.

4.2.1 Knowledge Factors

In considering the influence of knowledge factors on performance, two types of problems need to be considered: content and access. Information content was discussed above with respect to an operator's knowledge. As noted, the operator's knowledge is not necessarily accurate or complete and at times it can be oversimplified. However, even when knowledge is available, it must be accessed by operators and be used to assess a situation and plan a response.

This is known as the memory retrieval process and it is highly context-dependent. That is, contextual cues facilitate the retrieval of information from memory. The more retrieval cues available, the greater the probability that information can be retrieved. Retrieval cues, for example, can be a pattern of information that the operator recognizes as a particular event or situation.

There are other knowledge factors that influence the information retrieval process, making some information more likely to be recalled than other information:

- *Recency* - operators are biased to recall or bring to mind events that have occurred recently or are the subject of recent operational experience, training, or discussions

- *Frequency* - operators are biased to recall or bring to mind events that are frequently encountered in operations in situations that appear (even superficially) to be similar to the scenario being analyzed

- *Similarity* - operators are biased to recall or bring to mind events that have characteristics (event superficial) similar to the scenario, particularly if the event brought to mind is a "classic" event used in training or discussed extensively by the operators.

These factors may lead to the recall of information that is not entirely appropriate to the situation. For example, if a situation includes features that are similar to an event that recently occurred, an operator might recall that recent event and interpret the current situation to be the same.

In addition, relevant information that the operator may possess may not be recalled. For example, if a situation that rarely occurs has features in common with an event that is more familiar, operators may fail to recognize the rare event when it occurs because they interpret the information as indicative of the familiar event.

4.2.2 Processing Resource Factors

Tasks that operators perform use cognitive processing resources. However, people do not have an infinite amount of cognitive resources, such as attention and memory. Instead, there is a limited amount that must be distributed among the tasks that operators are performing. Tasks differ in terms of their demands for processing resources. If one task requires a great deal of attention and memory resources, then there is little available to perform other tasks. If a set of tasks uses up most of the available processing resources, then new tasks will have to be delayed until resources become

available. If a task requires more resources than are available, then its performance may suffer and may be slow, inaccurate, or error prone.

In general, tasks that operators are familiar with and well trained in require fewer resources than those that are unfamiliar and novel. Operators may perform routine procedure-based tasks almost effortlessly, using little of the processing resources available. However, when operators are confronted with a cognitively demanding situation in which the information provided by indications is confusing or contradictory (and where it may be unclear how well the available procedures are addressing the situation), a great deal of processing resources will be expended to analyze the situation and plan appropriate responses. In such situations, the resource limitations can considerably limit the operator's capabilities to monitor, reason, and solve problems.

It is also important to note that when operators are performing familiar, well-trained tasks, their information processing capabilities appear almost automatic and large amounts of information are processed in parallel. In contrast, when confronted with unfamiliar situations, the effects of limited information processing resources become more apparent. Operators no longer respond in an automatic mode and instead become slow, deliberate, serial processors of information. Information processing comes under much more conscious control. This type of analytic processing rapidly drains resources. To cope with such demanding cognitive situations, operators tend to use cognitive shortcuts that bypass careful, complete analysis of information. These shortcuts, called "heuristics," are methods that reduce the expenditure of cognitive effort and resources, and reduce the uncertainty of unfamiliar situations. An example is to do only enough analysis to form an initial hypothesis about the cause of the current situation. Once the partial analysis leads to a diagnosis, the information analysis is terminated. The potential problem with this type of heuristic is that a more detailed analysis of information may have revealed the situation to be a similar but less familiar one. In this example, the incomplete situation analysis may lead to an inaccurate situation model and inappropriate response plans.

In summary, when confronted with situations that are highly demanding, the following problems can occur:

- slow information processing becomes serial and effortful, leading to the use of processing shortcuts in the face of limited resources
- failure to perceive or process critical information about the situation in a timely manner and failure to properly integrate the information, which results in poor situation awareness and an inadequate situation model
- failure to revise incorrect situation assessments or courses of action, even when opportunities to do so arise
- failure to integrate multiple interacting symptoms and, instead, treating the symptoms independently.

4.2.3 Strategic Factors

Strategic factors influence choices under uncertain, potentially risky conditions. This can include situations where there are multiple conflicting goals, time pressure, and limited resources.

People often are placed in situations where they have to make choices and tradeoffs under conditions of uncertainty and risk. Situations often involve multiple interacting or conflicting goals that require considering the values or costs placed on different possible outcomes. An example relates to the decision of when to terminate a safety injection. Safety injection is required to mitigate certain types of accidents. On the other hand, if safety injection is left operating too long, it can lead to overfilling of the pressurizer. This creates a conflict situation where multiple safety-related goals must be weighed in determining an appropriate action.

One factor affecting these tradeoffs is the actual perception of risk. Using their knowledge and experience, operators estimate the risk that is associated with various situations. However, there is a common tendency to underestimate risk in low-probability, risk-significant situations in which operators have experience and when they perceive themselves to be in control.

Since their perception of risk is optimistic, plant operators do not expect significant abnormal situations to occur. Thus, they rely on redundant and supplemental information to confirm the unusual condition. Upon verification of several confirmatory indicators, the operator can accept the information as indicating an actual off-normal condition (compared with a spurious condition). However, this process still creates a conflict between the cost to productivity for falsely taking an action that shuts down the reactor versus the cost for failing to take a warranted action.

The above example illustrates another factor that operators often must consider (i.e., the consequences of different types of errors). For example, under conditions of uncertainty, an operator may have to weigh the consequences of failure to take an action that turns out to have been needed against the consequences of taking an action that turns out to be inappropriate.

There are also tradeoffs on when to make the commitment to a particular course of action. Within the constraints of limited processing resources and available time, operators have to decide whether to take corrective action early in a situation on the basis of limited information, or to delay a response until more information is available and a more thorough analysis can be conducted. On the one hand, in dynamic, potentially high-consequence (to risk or productivity) situations, the costs of waiting can be high. On the other hand, the costs of incorrectly making a decision can be high as well.

In summary, operators in abnormal events can be confronted with having to make decisions while facing uncertainty, risk, and the pressure of limited resources (e.g., time pressure, multiple demands for the same resources). The factors that influence operators' choices in such situations include goal tradeoffs, perceived costs and benefits of different options, and perceived risk. When considering the decisions that operators are likely to make, it is necessary to explicitly consider the strategic

factors that are likely to affect performance, including the presence of multiple interacting goals, the tradeoffs being made, and the pressures present that shift the decision criteria for these tradeoffs.

4.3 Failures in Operator Cognitive Activity

In this section, we consider how each of the major cognitive activities (monitoring or detection, situation assessment, response planning, and response implementation) can lead to cognitive failures. In cognitively demanding situations, a typical problem-solving sequence may assume the following four steps:

(1) Initial scanning is started by signals from the alarm system or other indicator, and the operator's attention is divided among a variety of data-gathering activities.

(2) The operator focuses on a specific group of indicators and makes an initial situation assessment.

(3) The operator now structures attentional resources to seek data confirming the hypothesis.

(4) The operator may become fixated on the hypothesis and fail to notice changes in the plant's state or new developments.

The operator eventually may become aware of subsequent changes, but the process is hampered by attention being directed toward the current hypothesis and the overall processing limitations. Cognitive errors stem from limitations in knowledge, access to knowledge, processing resources, and strategic factors.

4.3.1 Failures in Monitoring or Detection

The primary error during monitoring and detection is the failure to detect or observe a plant state indication (e.g., parameter value and valve position). In general, the probability of detecting or observing a given indication will be a function of the following:

- the salience of the indication (i.e., how much it alerts the operator resulting in data-driven detection)
- whether monitoring that parameter is "standard practice," called out in a procedure, etc.
- the perceived relevance (e.g., priority, value) of the indication (i.e., whether the operator has some "knowledge-driven" reasons to look at that indication)
- the relative perceived priority of monitoring that parameter as opposed to performing other activities competing for available attentional resources (an example of strategic factors influencing monitoring choices)

- the availability of attentional resources, which has two components:

  - arousal and alertness level (which brings in issues of boredom, vigilance, etc.)
  - overall workload

As discussed above, monitoring is often knowledge driven. Where operators choose to look is determined by their current situation model, and the information perceived to be relevant to support the current situation assessment, response planning, and response implementation activities.

One bias that enters into decisions as to where to look for evidence is referred to as the *confirmation bias*. This refers to the tendency to look for evidence to confirm the hypothesis currently being considered (i.e., plant indications that should be observed if the hypothesis is correct) rather than evidence that negates the hypothesis. As a consequence, if a plant indication is not perceived to be relevant for confirming a hypothesis that is currently being considered, it is less likely that the operator will decide to look at it. As a result, unless the indication is very salient, operators may fail to observe it.

4.3.2 Failures in Situation Assessment

The primary error during situation assessment is the failure to correctly interpret an observation. When a plant indication is observed, three "checks" are likely to be made to determine whether the indication needs to be pursued further:

- Is this observation consistent with my current understanding of the plant state (i.e., the current situation model)? Is it expected? Is it readily explained by the situation model? If the answer to any of these is yes, the operator is likely to be satisfied that he/she can account for the observation, and will not search further for an explanation.

- Is this observation likely to be spurious (i.e., invalid)? If the answer is yes, the operator is not likely to search further for an explanation of the finding.

- Is this observation "normal" given the current plant mode or does it signal a plant abnormality that needs to be responded to? If the operator determines that the observation is "normal" then it will not be pursued further.

If the operator determines that an observation is valid and unexpected, then situation assessment is initiated to come up with an explanation for the observation. In emergency situations where there are procedures available to guide performance, the situation assessment activity will be subordinate to a procedure-guided response, but it is likely to be engaged in as a "background" activity performed as resources permit (i.e., mental workload and availability of additional personnel).

There are four types of interpretation failures:

(1) failure to recognize that the indication is "abnormal"

(2) discounting or explaining away an indication by deciding it is "invalid" or spurious

(3) discounting or explaining away an indication by deciding that it can be accounted for on the basis of the operator's "current understanding" of the plant state (i.e., their situation model)

(4) engaging in situation assessment to try and come up with an explanation for the indication, but coming up with the "wrong" situation assessment (i.e., wrong situation model)

An individual may incorrectly conclude that an observation is "normal" for the following reasons:

- poor displays that do not indicate targets, limits, and set points, requiring operators to retrieve and integrate values to determine whether something is normal (These memory retrieval and information integration requirements are subject to memory retrieval, working memory limits, and computational processing limitations.)
- lack of knowledge or incomplete knowledge
- impact of processing limitation factors, exacerbated in situations where the workload is high or alertness level is low

An individual may incorrectly conclude that an observation is "expected" as a result of the following factors:

- lack of knowledge or incomplete knowledge (In complex accident situations, such as severe accidents, the phenomena may be less understood, and operators may not be familiar with what plant dynamics to expect.)
- limitations on working memory and computational processing that make it difficult for operators to keep in mind all relevant parameters and accurately "compute" what plant behavior should be expected (In complex situations, it may be difficult for them to perform the mental computations required to detect that observed plant behavior deviates either quantitatively or qualitatively from what would be expected.)
- impact of processing limitation factors, which are exacerbated in situations where the workload is high or alertness level is low

An individual may incorrectly conclude that an observation is "spurious" as a result of the following factors:

- history of "spurious" indications
- mental model that could explain how a spurious signal could be generated
- indication inconsistent with the operator's current situation model

An individual may engage in situation assessment activity, but decide on an incorrect explanation for the observation:

- The operator may generate the wrong explanation for the observation. Explanations that are more likely to be used are a result of the following:
  - representativeness (events for which this observation is a "classic" symptom)
  - frequency (events that happen frequently, or are familiar, e.g., due to training)
  - recency (events that have occurred recently)
- The operator may reject a correct explanation as implausible. An explanation's perceived plausibility is a function of the following:
  - the perceived likelihood of occurrence
  - the number of indications it can account for
- There will be a tendency to search for evidence that is consistent with the hypothesis that is first called to mind.
- There is a tendency to try to explain future observations in terms of that hypothesis and discount evidence inconsistent with that hypothesis.
- The above tendencies will be more likely when demands on processing resources are high:
  - high workload (e.g., other demands competing for attentional resources)
  - high computational demands (e.g., when the correct explanation requires integrating evidence across space and time)

Several factors can influence how a person interprets a given observation. One set has to do with memory retrieval processes. Some explanations for a given finding are likely to come to mind more readily than others. As discussed above, the principles of "recency," "frequency," and "similarity," affect those explanations that are more likely to be called to mind.

Failures in memory retrieval processes are particularly likely when processing resources are limited. In these situations operators tend to overutilize cognitive processes that simplify complex information tasks by applying previously established heuristics. Heuristics used by operators to retrieve information from memory exert a strong influence on human performance. These heuristics are based on the use of these memory-retrieval processes (recency, similarity, and frequency) in place of more thorough cognitive analysis. Under high demand situations, operators attempt to match a perceived information pattern (such as a pattern of indicators) with an already existing known pattern in the memory. The operator cognitively tries to establish a link because once this is done, previously identified successful or trained response sequences are identified. This saves the operator the effort of knowledge-based reasoning that is resource intensive. When the perceived

information is only partially linked to well-known patterns, the discrepancy may be resolved by identifying the situation as the one most frequently used in the past.

The following generally account for many human errors:

- the undue influence of salient features of the current situation (resulting in premature identification of the situation) or the intention or expectation of the operator (resulting in a bias to see only confirmatory data)
- the fact that in ill-defined situations the action most similar to frequently performed actions will often be selected
- limitations in the processing of memory and attention that cause important information to be lost, especially in high-stress conditions
- operators will generally favor heuristics (i.e., mental short cuts) over knowledge-based processing because they minimize cognitive effort and strain
- incomplete or incorrect knowledge

A second set of factors has to do with situation assessment processes. People are prone to search for an explanation for an observation that is consistent with their current situation model. This is related to the principle of confirmation bias. Once a hypothesis is generated to explain a set of findings, new findings are likely to be explained in terms of that initial hypothesis or to be discounted. A failure to revise situation assessment as new evidence is introduced is called a *fixation error*.

4.3.3 Failures in Response Planning

The primary error during response planning is the failure to follow the correct response plan. Response planning involves establishing goals, developing a response plan, which in turn may involve identifying and following a predefined procedure, and determining whether the actions taken are achieving the goals that have been established. Response planning also includes response plan adaptation which involves modifying procedures in cases where it is determined that the procedures are not achieving the desired goals.

Failures in response planning arise from any of the four elements involved. Specifically, operators may commit the following actions:

(1) Establish the wrong goal or incorrectly prioritize goals for any of the following reasons:

- an incomplete or inaccurate situation model
- incomplete or inaccurate knowledge
- inaccurate perceptions of risk

(2) Select an inappropriate procedure to follow or fail to recognize that the procedure is not applicable to the situation as result of the following problems:

- an incomplete or inaccurate situation model (missed elements of a situation that make the procedure not fully applicable)
- lack of knowledge, incomplete or inaccurate knowledge in relation to the plant or the procedure being followed (e.g., the goals, assumptions, and bounds of application of the procedure)
- computational processing limitations that result in a failure to anticipate violated preconditions, side effects of actions, or the existence of multiple goals that need to be satisfied

(3) Attempt to develop a response plan that turns out to be inadequate in cases where procedures are unavailable or are evaluated as inappropriate to the situation, which can be caused by the following problems:

- an incomplete or inaccurate situation model
- a failure to recognize that preconditions are not met
- a failure to anticipate side effects

(4) Incorrectly decide to deviate from procedures in any of the following ways:

- taking an action that is not explicitly specified in the procedures
- not taking an action that is specified in the procedures
- changing the order of actions from that specified in the procedures
- delaying an action that is specified in the procedures as a result of the following problems:
  - an incomplete or inaccurate situation model
  - lack of knowledge, incomplete or inaccurate knowledge in relation to the plant or the procedure being followed (i.e., the goals, assumptions, and bounds of application of the procedure)
  - computational processing limitations that result in a failure to anticipate potential negative consequences
  - the existence of multiple conflicting goals
  - inaccurate perceptions of risks

Situations where multiple conflicting goals must be weighed may lead operators to significantly delay or totally avoid taking an action specified in a procedure, as illustrated by the following examples:

- taking action may violate standard operating practice (e.g., take the operator out of the usual operating band)
- taking action may lead to reduced availability of safety systems, equipment, or instruments
- taking action may have a potential negative effect on some other safety function (e.g., lead to overfill of the pressurizer)
- significant uncertainty or unknown risk is associated with taking the action (e.g., PORV after being opened may stick open)
- taking the action will adversely affect areas within the plant and further burden recovery (e.g., actions may contaminate an auxiliary building)
- taking the action will have severe consequences associated with cost (e.g., the plant will be shut down for major cleanup after bleed and feed)
- taking the action will release radiation to the environment

The tendency to delay an action, or not take the action, will be more likely if the potential for negative consequences is perceived to be small, as in the following possible examples:

- The action is not relevant or constitutes "overkill" under the particular circumstances.
- The undesirable action can be delayed without negative consequences (i.e., with negligible probability of negative consequences).
- The criterion for taking action is overly conservative.
- The process can be monitored and action taken if the situation degrades.
- Delaying the action would buy time needed to rectify the situation by alternative means.
- The action is violated routinely without negative safety consequences (resulting in the perception that the probability of negative safety consequences from failure to take action is extremely small).
- The criterion for taking action is ambiguous or difficult to determine and/or requires a judgment call.

4.3.4 Failures in Response Implementation

Response implementation refers to taking the specific control actions required to perform a task. The primary error during response implementation is the failure to execute actions as required. In considering errors of implementation, it is assumed that the individual intends to take the correct action, but because of a memory lapse or unintended action, fails to take the action (i.e., an error of omission); unintentionally takes a different "wrong" action (i.e., an error of omission); or executes the action incorrectly (e.g., timing problem, overshooting or undershooting a value).

Several factors that can contribute to implementation errors:

- An operator may forget to take an action because of a memory lapse. This may occur in the following cases:
  - Other actions of greater importance or greater urgency that are taken earlier.
  - The procedure is written to allow significant flexibility for sequencing of actions (e.g., words such as "as time permits...").
  - The action cannot be executed immediately because there is a need for another criterion to be satisfied first (e.g., wait till a parameter reaches value *x*).
- An operator may inadvertently take the wrong action because of a "slip." This may occur in the following cases:
  - The required action deviates from a typical response.
  - The required action is similar to, but differs in critical respects from, an action sequence that the operator routinely performs.
- An operator may inadvertently take the wrong action, or execute an action incorrectly as a result of sensory-motor errors (e.g., lose his or her place in the procedure; hand literally slips).
- An operator may inadvertently take the wrong action because of communication errors.

4.4 Contributing Elements of Error-Forcing Contexts in Power Plant Operations

Sections 4.1 through 4.3 have described characteristics of human information processing that can result in unsafe actions and human failure events. It is important to remember that not all of the described processing characteristics will necessarily lead to unsafe actions and human failure events. In fact, many of the processes, heuristics, and strategies represent normally efficient and effective means for individuals to evaluate incoming information and to develop and implement appropriate

responses. For example, attempting to match a perceived information pattern (such as a pattern of indicators) with an already existing known pattern in memory can facilitate performance in high-demand situations. Alternatively, the use of such a heuristic can also lead to an unsafe action if, for example, an individual's criteria for accepting a match are set too low (possibly due to time constraints) or the indications are actually unreliable. While individuals (and crews) will develop their own set of more or less "naturalistic" processing strategies (e.g., Ref. 4.6) over time, it is also the context in which individuals are placed (i.e., the plant conditions and the performance-shaping factors), that determines which processing characteristics are activated or implemented in certain situations and whether or not they are appropriate. As discussed in Section 2, when processing mechanisms lead to inappropriate actions with unsafe consequences because of the context in which they are used, they are referred to as error mechanisms.

An important set of context-related factors likely to contribute to the potential for particular error mechanisms becoming operative in accident scenarios is the behavior of the parameters that reflect critical aspects of the plant conditions, e.g., steam generator level and pressure. The "behavior of the parameters" includes the behavior of individual parameters as perceived by the operators, the behavior of the parameters relative to one another, and the more global or "Gestalt" behavior of the parameters as perceived or interpreted by the operators. It is proposed that the behavior of critical parameters over time and relative to one another can, in conjunction with relevant PSFs such as operator training and experience, plant procedures, and the nature of the human-machine interface, have a significant impact on the manifestations of human error mechanisms. The basic assumption is that accident scenario characteristics, as represented by the behavior of critical parameters, can elicit or interact with certain human responses (e.g., complacency, anxiety) that facilitate the occurrence of an unsafe action or create situations that make certain processing mechanisms, strategies, or biases (e.g., recency effects, confirmation bias) inappropriate or ineffective. It is further assumed that the behavior of critical parameters can have different impacts, depending on the stage of information processing in which an individual is engaged, i.e., detection, situation assessment, response planning, or response implementation. Moreover, the PSFs that will contribute to the likelihood of an unsafe action occurring will be tied to the specific behavior of the plant and its impact on the operators.

4.4.1 Characteristics of Parameters and Scenarios

A number of aspects regarding the behavior of parameters in an accident scenario have been identified as potentially influencing the likelihood of certain error mechanisms becoming operative and thereby contributing to an unsafe action. The first set is based on an extension of the "guide words" and concepts used in HAZOP (Ref. 4.7) analyses. A second set is based on a set of characteristics catalogued by Woods, Roth, Mumaw, and their colleagues (Refs. 4.3, 4.4, 4.8, 4.9)[1] that attempts to describe why problem scenarios are difficult. The basic notion is that scenarios (which by definition evolve over time) contain features that create the opportunity for normal human information processing and action to be inappropriate or ineffective, essentially by creating unusual cognitive demands.

[1] Also D.D.Woods & E.S. Patterson, How Unexpected Events Produce An Escalation Of Cognitive And Coordinative Demands. P.A. Hancock and P.A. Desmond (Eds.), *Stress Workload and Fatigue*. Lawrence Erlbaum, Hillsdale NJ, (in press).

4.4.1.1 Parametric Influences

A set of descriptors can be used to describe the behavior of parameters that reflect the plant dynamics resulting from a given initiating event and any contributing system failures. It is assumed that the parameters vary (or do not vary) according to the existing plant conditions, and the current focus is on how particular variations in the parameters could interact with characteristics of human information processing to lead to unsafe actions. Relevant aspects of the way the parameters behave include (but are not limited to):

- the lack of a critical indication (instrumentation failure) or the lack of a compelling indication for an important parameter
- a small or large change in a relevant parameter
- a lower or higher than expected value of a parameter
- a low or higher rate of change in a parameter
- changes in two or more parameters in a short time
- delays in changes in two or more parameters
- one or more false indications
- direction of change in parameter(s) over time is not what is expected
- direction of change in parameters over time relative to each other is not what is expected.
- relative rate of change in two or more parameters is not what is expected
- apparently relevant parameters are actually irrelevant and misleading

Whether such behavior in critical parameters will affect human information processing depends on such things as the operators' physiological responses to the situation, their current situation model, their expectations regarding what is occurring, the availability of other sources of information, and other PSFs that could be relevant to the scenario. Nevertheless, the way the parameters behave (as represented by plant indicators) has the potential to elicit certain error mechanisms that lead to unsafe actions. For example, a slow rate of change in a parameter may not be detected in a timely manner and even if it is, it may induce complacency during the early stages of an accident. Furthermore, if operators have already formed an expectation about what is occurring in a scenario, a small change in a parameter might be dismissed due to a fixation error, confirmation bias, or other error mechanism. The potential influences of such variations in parameters in the context of the different information processing stages, likely error mechanisms, and contributing PSFs are used in steps 6 and 7 of the proactive search process presented in Section 9.

4.4.1.2 Scenario Influences

Woods, Roth, Mumaw, and their colleagues (Ref. 4.3, 4.4, 4.8, 4.9)[2] described a class of scenario-related conditions that can contribute to operators taking unsafe actions. The basic thesis is that the characteristics of the evolution of a scenario (including the behavior of critical parameters) can complicate operator performance during the different stages of information processing. For example, a scenario that starts out appearing to be a simple problem (based on strong but incorrect or incomplete evidence) can lead operators to take apparently appropriate actions, but then make them resistant to change or insensitive to correct information that appears later. Such a scenario is referred to as a "garden path problem," since the operators get set up to form a strong but incorrect hypothesis that prevents them from appropriately considering later information. Once again, underlying error mechanisms such as simplifying, fixation, recency effects, and confirmation bias can contribute to operators taking unsafe actions. Other types of complicating scenarios catalogued by Woods and others include those that:

- contain missing or misleading information
- require unexpected late changes
- create dilemmas, impasses, or double-binds
- require choices that have tradeoffs
- induce plant-related side effects
- contain "red herrings"
- contain activities by other agents or automatic systems that mask key evidence
- induce multiple (all seemingly valid) lines of reasoning
- require multiple tasks to be performed at a high tempo
- contain events that seem to be escalating the problem
- contain events in which the operators' responses lead to new problematic events
- contain events that interact to create complex symptoms

As with the parametric influences discussed in the preceding section, whether scenarios with such characteristics will affect human information processing and lead to unsafe actions depends on a number of factors, but certainly, reasonably possible accident scenarios should be examined to see if they contain these or similar characteristics. More detailed descriptions of these types of scenarios and guidance on how to consider other potential influences are provided in steps 6 and 7 of the proactive search process presented in Section 9.

4.5 Conclusions

This section has described the characteristics of human behavior that can result in unsafe actions and human failure events. There exists a body of knowledge developed in the behavioral sciences that allows the analyst to understand what kinds of influences can lead operators to misunderstand the conditions in a plant or fail to prepare an adequate response, resulting in plant damage. Such failures are not random but are shaped by the contexts in which the operators are placed (i.e., the plant conditions and the performance-shaping factors).

[2] See Footnote 1, page 4-18.

4.6 References

4.1 J.T. Reason, *Human Error*, Cambridge University Press, New York, 1990.

4.2 D.D. Woods, H.E. Pople, and E.M. Roth, Westinghouse Electric Corp., *The Cognitive Environment Simulation (CES) as a Tool for Modeling Human Performance and Reliability*, NUREG/CR-5213, Pittsburgh, PA, 1990.

4.3 D.D. Woods, L.J. Johannesen, R.I. Cook, and N.B. Sarter, *Behind Human Error: Cognitive Systems, Computers, and Hindsight*, Crew System Ergonomics Information Analysis Center (CSERIAC), Ohio State University, Wright-Patterson Air Force Base, Columbus, OH, December 1994.

4.4 E.M. Roth, R.J. Mumaw, and P.M. Lewis, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, NUREG/CR-6208, Westinghouse Science and Technology Center, July 1994.

4.5 J. Wreathall and J. Reason, *Human Errors and Disasters*, in Proceedings of the 1992 IEEE Fifth Conference on Human Factors and Power Plants, IEEE, New York, 1992.

4.6 G. A. Klein, J. Orasanu, R. Calderwood, and C. E. Zsambok, *Decision-making in Action: Models and Methods, Abley, Norwood, NJ, 1993.*

4.7 R. Ellis Knowlton, *An Introduction to Hazard and Operability Studies: The Guide Word Approach,* Chemetics International Co. Ltd., October 1992.

4.8 R. J. Mumaw & E. M. Roth, How to be more devious with a training simulator: Redefining scenarios to emphasize cognitively difficult situations. *1992 Simulation MultiConference: Nuclear Power Plant Simulation and Simulators*, Orlando, FL, April 6-9, 1992

4.9 J. W. Perotti and D.D. Woods. *A Cognitive Analysis of Anomaly Response in Space Shuttle Mission Control. Cognitive Systems Engineering Laboratory (CSEL)*, CSEL 97-TR-02, The Ohio State University, Columbus OH, March1997. Prepared for NASA Johnson Space Center

4.7 Bibliography of Cognitive Psychology Literature Relevant to ATHEANA

General Treatment of the Cognitive Basis for Human Error

Hollnagel, E. (1993). *Human Reliability Analysis Context and Control.* Academic Press, London, 1993.

R.J. Mumaw, D. Swatzler, E. M. Roth, and W.A. Thomas (1994). *Cognitive Skill Training for Decision Making.* NUREG/CR-6126, U.S. Nuclear Regulatory Commission, Washington, D.C.

D. Norman (1988). *The Psychology of Everyday Things.* Basic Books, NY.

J. Rasmussen (1986). *Information Processing and Human-Machine Interaction.* NY, North Holland.

J. Reason (1990). *Human Error.* Cambridge University Press, NY.

D.D. Woods, L.J. Johannesen, R.I. Cook, and N.B. Sarter (1994). *Behind Human Error: Cognitive Systems, Computers and Hindsight,* CSERIAC State-of-the-Art Report.

D.D. Woods and E.M. Roth (1986). *Models of Cognitive Behavior in Nuclear Power Plant Personnel*, NUREG/CR-4532, U.S. Nuclear Regulatory Commission, Washington, D.C.

Related Works on the Concepts Discussed in this Section

M.J. Adams, Y.J. Tenney, and R.W. Pew (1991). *State-of-the-Art Report: Strategic Workload and the Cognitive Management of Advanced Multi-Task Systems* (CSERIAC 91-6).

J.D. Bransford (1979). *Human Cognition: Learning, Understanding and Remembering.* Wadsworth, Belmont, CA.

V. DeKeyser and D.D. Woods (1990). "Fixation errors: Failures to revise situation assessment in dynamic and risky systems," in A.G. Colombo and A. Saiz de Bustamente (eds.), *System Reliability Assessment* (pp. 231-251). Kluwer Academic, Dondrecht, The Netherlands:.

D. Dorner (1983). "Heuristics and cognition in complex systems," in R. Groner, M. Groner, and W.F. Bischof (eds.), *Methods of Heuristics.* Lawrence Erlbaum, Hillsdale, NJ.

M.R. Endsley (1995). Towards a theory of situation awareness in dynamic systems. *Human Factors* 37: 65-84.

K. Hukki and L. Norros (1993). Diagnostic orientation in control of disturbance situation. *Ergonomics* 36: 1317-1328.

E. Hutchins (1990). "The technology of team navigation," in J. Galegher, R. Kraut, and C. Egido (eds.), *Intellectual Teamwork: Social and Technical Bases of Collaborative Work.* Lawrence Erlbaum, Hillsdale, NJ.

D. Kahneman, P. Slovic and A. Tversky (1982). *Judgment Under Uncertainty: Heuristics and Biases.* Cambridge University Press, London.

J.V. Kauffman, G.F. Lanik, E.A. Trager and R.A. Spence (1992). *Operating Experience Feedback Report - Human Performance in Operating Events.* NUREG-1275, Office for Analysis and Evaluation of Operational Data. Washington, D.C: U.S. Nuclear Regulatory Commission.

G.A. Klein and R. Calderwood (1991). "Decision models: Some lessons from the field," *IEEE Transactions on Systems, Man, and Cybernetics*, 21: 1018-1026.

P.H. Lindsay and D.A. Norman (1977). *Human Information Processing.* Academic Press, New York.

J.C. Montgomery, C.D. Gaddy, R.C. Lewis-Clapper, S.T. Hunt, C.W. Holmes, A.J. Spurgin, J.L. Toquam, and A. Bramwell (1992). "Team Skills Evaluation Criteria for Nuclear Power Plant Control Room Crews (Draft)." Washington, D.C.: U.S. Nuclear Regulatory Commission.

N. Moray (1986). "Monitoring behavior and supervisory control," in K. Boff, L. Kaufman, and J. Thomas (eds.), *Handbook of Human Perception and Performance.* Wiley, New York.

R.L. Mumaw, E.M. Roth, K.J. Vicente and C.M. Burns (1995). Cognitive Contributions to Operator Monitoring During Normal Operations. AECB Project No. 2.376.1, Atomic Energy Control Board, Ottawa, Canada.

J. O'Hara. (1994). *Advanced Human-System Interface Design Review Guideline:* Volume 1: *General Evaluation Model, Technical Development, and Guideline Description.* (NUREG/CR-5908). Washington, D.C.: U.S. Nuclear Regulatory Commission.

J. Orasanu (1993). "Decision-making in the cockpit," in E.L. Weiner, B.G. Kanki and R.L. Helmreich (eds.) *Cockpit Resource Management.* Academic Press, San Diego.

C. Perrow (1984). *Normal Accidents. Living with High-Risk Technologies.* Basic Books, New York..

J. Rasmussen (1969). *Man-Machine Communication in the Light of Accident Records* (S-1-69). Roskilde, Denmark: Electronics Dept., Danish Atomic Energy Commission.

J. Rasmussen (1976). "Outlines of a hybrid model of the process operator," in T.B. Sheridan and G. Johannsen (eds.), *Monitoring Behavior and Supervisory Control* (pp. 371-383). Plenum Press, New York.

J. Rasmussen (1986). *Information processing and Human-Machine Interaction: An Approach to Cognitive Engineering.* North-Holland, New York.

E.M. Roth, R.J. Mumaw and P.M. Lewis (1994). *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies.* NUREG/CR-6208, U. S. Nuclear Regulatory Commission, Washington, D.C.

N. Sarter and D.D. Woods (1994). "Pilot interaction with cockpit automation II: an experimental study of pilots' model and awareness of the flight management system," *International Journal of Aviation Psychology* 4 (1): 1-28.

N.B. Sarter and D.D. Woods (1991). "Situation awareness: A critical but ill-defined phenomenon," *International Journal of Aviation Psychology*, 1(1): 43-55.

H. Simon (1957). *Models of Man (Social and Rational).* Wiley, New York.

W. Wagenaar and J. Groeneweg (1987). Accidents at sea: Multiple causes and impossible consequences," *International Journal of Man-Machine Studies* 27: 587-598.

C. Wickens (1984). *Engineering Psychology and Human Performance.* Merrill, Columbus, OH.

C.D. Wickens and J.M. Flach (1988). "Information processing," in E.L. Weiner and D.C. Nagel (eds.), *Human factors in Aviation.* Academic Press, New York.

D.D. Woods (1992a). *The Alarm Problem and Directed Attention* (Technical Report TR-01). Cognitive Systems Engineering, Ohio State University, Columbus, OH.

D.D. Woods (1992b). *Cognitive Activities and Aiding Strategies in Dynamic Fault Management* (Technical Report CSEL 92-TR-05). Cognitive Systems Engineering Laboratory, Ohio State University, Columbus, OH.

D.D. Woods, H.E. Pople, and E.M. Roth (1990). *The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability.* NUREG/CR-5213, U.S. Nuclear Regulatory Commission, Washington, D.C.

D.D. Woods, E.M. Roth, and H.E. Pople (1987). *Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment.* NUREG/CR-4862, U.S. Nuclear Regulatory Commission, Washington D.C.

5 OPERATIONAL EXPERIENCE ILLUSTRATING ATHEANA PRINCIPLES

Reviews and analyses of operational events have been used throughout the development and demonstration of ATHEANA. As discussed in Section 2, operational experience was used iteratively in the development of the ATHEANA framework. Reviews of operational events assisted in the formulation of the ATHEANA perspective, beginning with the early work documented in NUREG/CR-6093 (Ref. 5.1), NUREG/CR-6265 (Ref. 5.2), and NUREG/CR-6350 (Ref. 5.3). The behavioral sciences principles and concepts described in Section 4 were confirmed using examples from operational experience. The retrospective ATHEANA analysis approach described in Section 8 is based upon this experience in performing event analyses. Also, a brief tutorial on how to analyze events from the ATHEANA perspective and hands-on experience in operational event analysis was included in the ATHEANA training of third-party users for an earlier demonstration. The prospective (or human reliability analysis) ATHEANA approach described in Section 9 incorporates insights from operational event analyses (i.e., those documented in Appendix A), both those performed in the development of ATHEANA and its application aids, and those that might be performed by future, potential users of ATHEANA. Finally, the success of ATHEANA applications to date (e.g., those examples given in Appendices B through E, prior third-party demonstrations) is due in part to the ability of the analysts to relate examples of past operational experience to potential future failure paths.

Event analyses using the ATHEANA perspective have been documented in several places. Early reviews of NPP events are documented in NUREG/CR-6093, NUREG/CR-6265, and NUREG/CR-6350. Reviews of events from other industries have been performed to illustrate the broader usefulness of basic ATHEANA principles. A more mature analysis method and database structure for NPP events was eventually developed and documented as the Human-System Event Classification Scheme (HSECS) (Ref. 5.4). Recently, refinements to the HSECS structure and additional event analyses have been made. Appendix A documents the analyses of six events that use these most recent refinements. Eventually an expanded structure and method that can accommodate both nuclear and non-nuclear events will be developed and implemented.

This section provides excerpts of selected event analyses to illustrate:

- how operational experience confirms the ATHEANA perspective on serious accidents
- the importance and usefulness of the behavioral science concepts discussed in Section 4
- what unsafe actions (UAs) are (through use of examples), including errors of commission
- how UAs occur and the role of error-forcing contexts (EFCs) in their occurrence
- UAs and EFC elements from actual events

Consequently, the event excerpts provided in this section are intended to be used by ATHEANA users not only in learning ATHEANA's basic principles and concepts but also in applying ATHEANA. However, the examples given in this section are simply illustrative models of the types of information that could be useful in trying to apply ATHEANA. Section 7, which describes the preparatory activities for applying ATHEANA for retrospective or prospective analyses, directs

ATHEANA users to identify other event analyses (e.g., the HSECS database), and plant-specific events that would be relevant to review.

In particular, the most difficult task in applying the ATHEANA HRA approach is the identification of UAs and associated EFCs for defined human failure events (HFEs). The excerpts from operational event analyses provided in this section attempt to establish a connection between UAs and EFCs and the observable influences on human performance. These observable influences are the error-forcing context elements [i.e., the plant conditions and associated performance-shaping factors (PFSs)]. Consequently, the event analysis categorization terminology used in this section may differ from the breakdown of the different information processing stages described in Section 4 since they are based strictly upon plant conditions, known PSFs, and the actions of the operators. Because they are based upon contextual factors from past operational experience, these categorizations can be used as the auditable factors in the HRA information-gathering processes that are necessary if predictions about likely human errors are to be made.

Section 5.1 discusses how analyses of operational events can provide future users of ATHEANA with basic information on the contributions of humans and error-forcing contexts in past operational experience. Section 5.2 gives some insights from operational event analyses about operator performance and associated potential EFCs. Section 5.2 also provides some illustrative examples of UAs and EFCs taken from operational event analyses. Section 5.3 uses an operational event example to illustrate how the dependent effects of performance-shaping factors and plant conditions can cause an incorrect initial situation assessment (or mindset) to persist.

5.1 Contributions of Humans and Error-Forcing Contexts in Past Operational Experience

The four event analyses (TMI-2, Crystal River 3, Salem 1, and Oconee 3) summarized in Section 3.3.1 demonstrated that EFCs have played significant roles in serious accidents in the nuclear power as well as other industries. This section briefly discusses the plant conditions and negative PSFs that created EFCs in these four events. Then a brief discussion is provided on how these EFCs can be related to failures in one or more of the four information-processing stages described in Section 4.

5.1.1 Plant Conditions and PSFs

In TMI, the two plant conditions that contributed to the event were the preexisting misalignment of EFW valves and the stuck-open relief valve. They combined with the negative PSFs, including the maintenance tag that obstructed the position indicator for the EFW valve, a misleading relief valve position indication, and lack of procedural guidance for the event-specific conditions. Operator training emphasized the dangers of solid plant conditions, causing operators to focus on the wrong problem. Overall, there was a mismatch between the actual plant conditions and the operator job aids (e.g., training, experience) for this event.

In the Crystal River 3 (CR3) event, the open spray valve and the associated misleading position indicator created an EFC. There was no procedural guidance to support the diagnosis and correction of a loss of reactor coolant system (RCS) pressure control. Consequently, like the TMI-2 event, there was a mismatch between the actual plant conditions in this event and job aids such as procedures and valve position indicator.

In the Oconee 3 event, operators did not have a position indication because the isolation valve (which ultimately created the drain path) was racked out for stroke testing. Also, the erroneously installed blind flange was a temporary obstruction that remained undiscovered despite several independent checks. The plant conditions in this event (including the fact that the event took place during shutdown) activated various deficiencies in job aids, such as inadequate procedures and lack of a "real" valve position indication. In addition, poor communication between the technician performing the valve stroke testing and the control room operators played a role in the event. Another negative PSF was the use of an informal (and incorrect) label to identify the sump line for blind flange installation.

The Salem 1 event involved different contextual factors, principally the partial, erroneous SI signal that was generated by preexisting hardware problems and required the operators to manually align several valves. Also, there was no procedural guidance regarding appropriate actions in response to the SI train logic disagreement (i.e., a mismatch between actual plant conditions and procedures). Like the other event examples, the actual plant conditions in this event (including the SI signal failure that increased operator workload) activated several negative PSFs.

5.1.2 Failures in Information Processing Stages

Analysis of these events reveals that the situation assessment and situation model update were critical. The analysis indicates that operators were quite good in discounting information that did not fit expectations. The discounting can result in incorrect situation assessment and prevent timely updating of the situation model.

In TMI-2, operators did not recognize that the relief valve was open and that the reactor core was overheating, and the situation model was not updated. In Crystal River 3, operators did not recognize that the pressurizer spray valve was open and causing the pressure transient. The information contrary to this was discounted. In the Salem 1 event, operators failed to recognize and anticipate the pressurizer overfill, steam generator pressure increases, and the rapid depressurization following opening of the steam generator safety valve. Finally, in Oconee 3, operators did not recognize that a drain path to the sump existed until eyewitness reports were provided.

These situation assessment and situation model updating problems involved either the sources of information (e.g., instrumentation) or their interpretation. In TMI-2, operators misread the temperature indicator for the relief valve drain pipe twice, thus attributing the high in-core and RCS loop temperatures to faulty instrumentation; they also were misled by the control room position for the relief valve. Also, some key indicators were located on back panels, and the computer printout of plant parameters ran more than 2 hours behind the event. In Crystal River 3, operators initially

conjectured that the pressure transient was caused by RCS shrinkage. Unconnected plant indicators, as well as the misleading spray valve position indicator and (unsuccessful) cycling of the spray valve control, were taken as supporting this hypothesis. In Oconee 3, operators suspected that the indication of decreasing reactor vessel level was a result of faulty operation. Two sump high-level alarms were attributed to possible washdown operations. As noted above, field reports eventually convinced operators to believe their instrumentation.

5.2 Analysis of Error-Forcing Context

While the HFE definition specifies what consequences are experienced at the plant, system, and component level, the definition of UA correlates with specific failure modes of systems and components, including the timing of failures (e.g., early termination of emergency safety features (ESF) without recovery versus termination of ESF when needed). As described in Section 9, definitions of both HFE and UAs can be developed in a straightforward manner from the understanding of plant, system, and component success criteria (including timing), failure modes, plant behavior and dynamics, and accident sequence descriptions.

In contrast, relationships between a UA and a specific error-forcing context are very difficult to define and require the synthesis of psychological and hardware causes. (Recall that, as described in Section 3, several different EFCs can result in the same UA, and different UAs can result in the same HFE.) In order to establish relationships between a UA and EFCs, various EFCs and EFC elements should be analyzed to determine their impact on execution of UAs. It should be noted that although only two types of EFC elements, namely plant conditions and PSFs, are identified, these elements themselves can be very complicated.

The analyses of the events listed below provide examples of specific UAs and EFCs and the links between them. Section 5.2.1 discusses important EFC elements that should be addressed by an HRA/PRA. Section 5.2.2 lists PSFs that were important in events analyzed in ATHEANA. Analyses of three at-power events and two shutdown events provided the basis for these sections. The two shutdown events, Prairie Island 2 (2/20/92) and Oconee 3 (3/8/91), were selected because they had been previously analyzed in earlier phases of the project and were known to contain many examples of factors that adversely affect human performance. The three at-power events, Crystal River 3 (12/8/91), Dresden 2 (8/2/90), and Ft. Calhoun (7/3/92), were selected primarily as a result of their similarity to the small-break loss-of-coolant accident (SLOCA) scenario, which was chosen for the trial application discussed in NUREG/CR-6350 (Ref. 5.3). In particular, both the Dresden 2 and Ft. Calhoun events were LOCAs and the key features of the Crystal River 3 event (e.g., decreasing reactor coolant system pressure, increasing RCS temperature, the need for high-pressure injection) were similar to a SLOCA scenario. The event analyses provided in Appendix B provide further illustrations of ATHEANA principles and concepts.

5.2.1 Error-Forcing Context and Unsafe Actions

The five events identified above provided insights on UAs and EFC elements. This section focuses on how EFC elements (PSFs and plant conditions) affected the four stages of information processing described in Section 4. The EFC elements were identified for each of the stages (i.e., detection, situation assessment, response planning, and response implementation). As stated in the introduction to Section 5, these categorizations differ from those given in Section 4 because they are generally based upon observable factors, while the psychological error mechanisms in Section 4 most often are not observable. In addition, some elements (especially PSFs) were identified as being important, but appeared to generally affect human performance, probably influencing multiple stages in information processing.

For each information processing stage (except detection), categories of UAs are described in Tables 5.1 through 5.5. The descriptions are based on the analyses of operational events. While a complete categorization scheme was not created (because it was dependent upon the events selected as examples), the categories shown in Tables 5.1 through 5.5 give some additional means for discriminating among the different ways in which humans have failed in particular information-processing stages. To illustrate how such failures could occur, specific EFC elements from actual events that created the context, or some part thereof, for each category of failure have been identified. The results show examples of these EFC elements, which include problems with unusual plant conditions (e.g., high decay heat, N_2 overpressure, instrumentation problems) and problems with PSFs [e.g., deficient procedures, training, communication, human–system interfaces (HSI), supervision, and organizational factors and time constraints]. In many cases, the importance of plant conditions was usually implied by the specific problems (e.g., instrumentation failed because of plant conditions, or procedural guidance not applicable to specific plant conditions).

Since there was more than one UA in most of the events analyzed, the different specific EFC elements used to illustrate one category of failure for one event may actually be associated with different unsafe actions. For example, in Table 5.2, the first two EFC elements identified from the Dresden 2 event that cause operators to develop a wrong situation model of the plant are associated with one UA, while the third and fourth EFC elements are associated with another UA.

5.2.1.1 Error-Forcing Context in Detection

Failures in detection identified in the five illustrative events include the following:

- operators unaware of actual plant state
- operators unaware of the severity of plant conditions
- operators unaware of continued degradation in plant conditions

Based upon the example events, instrument failures are expected to be the predominant cause of detection failures. For example, reactor vessel (RV) level instrumentation that fails high off-scale, and redundant RV level instrumentation readings requiring correction through hand calculations can cause operators to fail to detect abnormal RV levels.

Table 5.1 Examples of Detection Failures

Detection failure	Contextual Influences	Event
Operators unaware of actual plant state, its severity, and continued degradation in conditions.	(1) Reactor vessel (RV) level instrumentation failed high off-scale as a result of unusual plant conditions (i.e., high N_2 overpressure). (2) Redundant RV level instrumentation readings required correction through hand calculations (and were performed incorrectly). (3) Procedures did not specifically address the high N_2 overpressure that existed at the time of the event; did not contain stop points in the draindown to allow static readings; did not specify the frequency of level readings; did not require a log of time, Tygon tube, and calculated level readings to be maintained (to establish level trends, etc.); did not specify the required accuracy of calculations for correcting level readings for overpressure; did not adequately specify what instrumentation was required to be operable before the draindown; and did not describe how to control N_2 overpressure or what the overpressure should be at various points during the draindown (some decreasing trend in overpressure was implied).	Prairie Island 2 (2/20/92), loss of reactor coolant system (RCS) inventory and shut-down cooling during shutdown.

In general, problems in the detection of an accident or accident conditions are expected to be rare. As shown in Table 5.1, only one (the Prairie Island 2 event) of the five events analyzed included detection problems. Because of the number of alarms and other indications typically available during at-power operations, the likelihood of operators not being aware of the fact that something is wrong and that some actions are needed is low.

For the Prairie Island 2 event, minimal indications were available since this event took place during shutdown operations during a draindown to mid-loop. As indicated by the contextual factors noted in Table 5.1, instrumentation problems (both failures and unreliability) and procedural deficiencies conspired to make it difficult for draindown operators to detect that they were actually overdraining the vessel. In addition, unusual plant conditions (especially the high N_2 overpressure) exacerbated the instrumentation and procedural problems. Overall, there was a mismatch between the plant conditions in this event and operator job aids (e.g., procedures, training, experience, human–system interface).

5.2.1.2 Error-Forcing Context in Situation Assessment

A situation assessment failure can cause operators to develop wrong situation models of the plant state and plant behavior. As indicated in Table 5.2, instrumentation or interpretation problems are the predominant influences in situation assessment problems. Other factors can also contribute to situation assessment failures. For instance, human interventions with the plant and its equipment

Table 5.2 Examples of Situation Assessment Failures

Situation Assessment Failure	Contextual Influences	Event
Operators develop wrong situation model (or cannot explain) plant state and behavior.	(1) Pressurizer (PRZR) spray valve position indication inconsistent with actual valve position (because of preexisting hardware failure and design). (2) No direct indication of PRZR spray flow provided.	Crystal River 3 (12/8/91), RCS pressure transient during startup.
	(1) Position indicating lights for the safety relief valve show the valve closed (although it has failed open). (2) Operators generally unaware of generic industry problems involving Target Rock safety relief valves (e.g., spurious opening and tendency to stick open after actuation) until after the event occurred. (3) Operators had no understanding of the effect of auxiliary steam loads on the reactor pressure vessel cooldown rate and of the effect of the combination of the open safety relief valve, auxiliary steam loads, and opening turbine bypass valves. (4) Operators surprised by the rate of increase in torus temperature.	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
	(1) Computer displays normally used for containment temperature and RCS subcooling parameters were malfunctioning and operators had difficulty obtaining required information.	Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).
	(1) Blind flange installed on wrong residual heat removal (RHR) sump suction line despite two independent checks and one test. (2) As a result of miscommunication, technician racked out then stroked RHR sump suction isolation valve (creating a drain path from the RCS to the sump through the mistakenly open sump suction line) without telling control room operators.	Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown.
Operators unable to distinguish between results of their own actions and accident progression.	(1) Evolution in progress to increase reactor power (basis for the erroneous conjecture that RCS over-cooling occurred). (2) Field operators report plant behavior associated with the evolutions in progress (erroneously taken as confirmation of RCS over-cooling hypothesis).	Crystal River 3 (12/8/91), RCS pressure transient during startup.

Table 5.2 Examples of Situation Assessment Failures (Cont.'d.)

Situation Assessment Failure	Contextual Influences	Event
Operators unable to distinguish between results of their own actions and accident progression.	(1) Operators were reducing power from 87% (723 MWe) at a rate of 100 MWe per hour, a frequent night shift evolution because of decreasing network load demand during the late night and early morning hours.[a]	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
Operators misinterpret information or are misled by wrong information, confirming their wrong situation model.	(1) Erroneous report from technicians that one bank of PRZR heaters are at 0% power. (2) Cycling of switch for PRZR spray valve did not terminate the transient (because valve was broken).	Crystal River 3 (12/8/91), RCS pressure transient during startup.
	(1) Reactor pressure vessel pressure was less than the safety relief valve (SRV) setpoint (coupled with position indicating lights showing the SRV to be closed).[b]	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
	(1) High-level alarm from reactor building normal sump (interpreted as being the result of washdown operations).	Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown.
Operators reject evidence that contradicts their wrong situation model.	(1) Strip chart recorders showed PRZR level increasing (which is inconsistent with RCS overcooling and associated inventory shrinkage), but were not monitored. (2) Recollection of information passed during shift turnover concerning a problem with PRZR spray valve indication discounted because of unsuccessful valve cycling.	Crystal River 3 (12/8/91), RCS pressure transient during startup.
Operators reject evidence that contradicts their wrong situation model.	(1) Indication of increased SRV tailpipe temperature (310°F).[b] (2) Back panel acoustic monitor showed red open light.[b]	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
Operators reject evidence that contradicts their wrong situation model.	(1) Reactor vessel level reading at 20 inches and decreasing. (Erroneous operation of the RV wide-range level transmitter suspected.) (2) Health physics technician in reactor building verified reduction in RV level and increasing radiation.(3) Operating low-pressure injection (LPI) pump A current fluctuating downward. (Pump was stopped and isolation valves to borated water storage tank suction line were opened to provide injection to RCS.) (3) Operating low-pressure injection (LPI) pump A current fluctuating downward. (Pump was stopped and isolation valves to borated water storage tank suction line were opened to provide injection to RCS.)	Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown.

Table 5.2 Examples of Situation Assessment Failures (Cont.)

Situation Assessment Failure	Contextual Influences	Event
Operators reject evidence that contradicts their wrong situation model.	(4) Evidence that RCS was not being filled and health physics technician notifies control room that there is 6-12 inches of water on the floor near the emergency sump in the reactor building.[c]	Oconee 3 (3/8/91), loss of RCS and shut-down cooling during shutdown.

[a] In the Dresden event, the evolution in progress did not appear to play an important role in the operator's ability to perform, although it probably did trigger the spurious safety relief valve opening that started the event.

[b] In the Dresden event, the wrong situation assessment regarding the SRV was temporary– within about 1 minute after actuation of the back panel annunciator, the shift control room engineer decided that the SRV must be open and continued on a course of action associated with that correct situation assessment.

[c] This information, probably combined with previous evidence, ultimately caused operators to change their situation assessment to the correct one.

(either immediately before or during the event and with or without the knowledge of control room operators) can mask accident symptoms or cause them to be misinterpreted.

Table 5.2 illustrates possible causes for situation assessment problems, especially during the initial development of wrong situation models. In the Oconee 3 shutdown event, an undiscovered pre-accident human failure led to the draining of the RCS to the sump, which occurred when the sump isolation valve was stroke-tested. The failure of a technician to communicate to the control room when he was starting to stroke the valve further distorted the operators' situation models of the plant's configuration. As shown by the third and fourth factors for the Dresden 2 event, the operators' lack of training and experience are the likely causes for their inability to predict how the plant behaved in response to their inappropriate corrective actions.

Wrong situation models can be strengthened by irrelevant information or the effects of (unknown) hardware failures. As shown by EFCs for the Crystal River 3, Dresden 2, and Ft. Calhoun events, wrong situation models are frequently developed as a result of instrumentation problems, especially undiscovered hardware failures. Instrumentation also plays an important role in confirming wrong situation models and rejecting information that is contrary to wrong situation models. Wrong situation models can persist in the face of contrary (and true) evidence. Once operators develop a situation model, they typically seek confirmatory evidence (Ref. 5.5). As shown in Table 5.2, when this model is wrong, several issues regarding confirmatory information arise and can further degrade human performance:

- information can be erroneous or misleading (e.g., field reports in the Crystal River 3 event)
- plant indicators can be misinterpreted (e.g., sump alarms in the Oconee 3 event)

- plant or equipment behavior can be misunderstood (e.g., switch cycling in the Crystal River 3 event and SRV set point in the Dresden 2 event)

Furthermore, operators often develop rational but wrong explanations for discounting evidence that is contrary to their wrong situation model. Table 5.2 provides some examples of such rational explanations for discounting or failing to recognize information that could lead to a more appropriate situation model of the plant state and behavior. Those rational explanations can result from indicators that are not monitored (e.g., Crystal River 3), undiscovered hardware failures (e.g., Crystal River 3), and erroneous hypotheses that indicators are not operating correctly (e.g., Oconee 3). Operators also tend to misinterpret indications of actual plant behavior consistently with their wrong situation model, for example, confusing the effects of concurrent activities or the delayed effects of previous actions with actual plant behavior (e.g., Crystal River 3 and Dresden 2).

5.2.1.3 Error-Forcing Context in Response Planning

Failures in response planning result when operators fail to select or develop the correct actions required by the accident scenario. Major contributors in response planning failures, in addition to a wrong situation model, are deficiencies in procedures and poor training. Past experience has shown that five categories of response planning problems could occur; these are shown in Table 5.3:

(1) operators select nonapplicable plans
(2) operators follow prepared plans that are wrong or incomplete
(3) operators do not follow prepared plans
(4) prepared plans do not exist, so operators rely upon knowledge-based behavior
(5) operators inappropriately give priority to one plant function over another

The first category is illustrated by the unusual plant conditions (e.g., high N_2 overpressure) in the Prairie Island 2 event. The Ft. Calhoun event illustrates the procedural deficiencies represented by the second category. Three different deficiencies were revealed in this event; possibly all are the result of a recent revision to plant procedures. The Crystal River 3 event illustrates the third category, in which the operators' search for the cause of the RCS pressure transient was directed by their erroneous situation assessment, thereby excluding procedural guidance that could have terminated the event sooner. Operators also inappropriately used procedural steps (intended for shutdown) for bypassing the emergency safeguards features actuation system (ESFAS) and automatic actuation of high pressure injection (HPI). The justification for this bypass was that it was reversible and the setpoint was set conservatively (i.e., operators had a little more time to reverse the decreasing RCS pressure). The fourth category of response planning problems is illustrated in the Dresden 2 event in which both procedural and training deficiencies caused operators to have difficulty responding to a simpler event (i.e., transient with successful reactor trip and stuck-open relief valve) than the event addressed by procedures and training (i.e., anticipated transient without scram (ATWS) with a stuck-open relief valve). The last category of response planning problems, as shown in Table 5.3, is illustrated by two events: Crystal River 3 and Dresden 2. In the Crystal River 3 event, operators terminated HPI (without procedural guidance) too early because of concerns that the pressurizer would be filled solid. In the Dresden 2 event, operators caused an excessive cooldown rate as a result of their misplaced concerns about rising torus temperature, their lack of experience and training, and lack of procedural guidance.

Table 5.3 Examples of Response Planning Failures

Response Planning Failure	Contextual Influences	Event
Operators follow prepared plans (e.g., procedures), but these plans direct operators to take actions that are inappropriate for specific situation.	(1) Draindown procedure assumed a lower N_2 overpressure; therefore RV level conversion calculations, time for draindown, etc., were different than assumed in procedure.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.
Operators follow prepared plans (e.g., procedures), but these plans are wrong and/or incomplete (resulting in inappropriate actions).	(1) Procedure deficiency, resulting from recent procedure revisions regarding the restart of reactor coolant pumps (RCPs) without offsite power. (Wrong actions not taken because of operator's prior knowledge and experience.) (2) Procedure did not contain sufficient detail regarding the tripping of condensate pumps–results in complete loss of condensate flow. (3) Early in event, procedures directed operators to close pilot-operated relief valve (PORV) block valves in series, making the PORVs unavailable as relief protection. (Later, during plant cooldown, operators recognized situation and reopened block valves.)	Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).
Operators do not explicitly use prepared plans (e.g., procedures) and take actions that are inappropriate.	(1) Search for cause of pressure transient was on the basis of a wrong situation assessment and open PRZR spray valve was not discovered. (2) Operators increased reactor power (more than once) without understanding the cause of RCS pressure transient. (3) Operators bypassed ESFAS and HPI for 6 minutes without understanding cause of RCS pressure transient and without prior approval (i.e., acknowledgment) from supervisors.	Crystal River 3 (12/8/91), RCS pressure transient during startup.
Operators forced into knowledge-based (wrong) actions because prepared plans (e.g., procedures) are incomplete or do not exist.	(1) Abnormal operating procedure for relief valve failure did not contain some of the symptoms for this type of event (e.g., decrease in MWe, steam flow/feed flow mismatch, decrease in steam flow, difficulties in maintaining the 1 psi differential pressure between drywell and the torus). (2) Emergency operating procedures for primary containment control and reactor control did not provide guidance for pressure control with one stuck- open relief valve. (3) Classroom and simulator training typically used stuck-open relief valve as the initiating event for an ATWS. Operators had not been trained for the simpler event that occurred (i.e., stuck-open safety relief valve followed by successful scram).	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).

Table 5.3 Examples of Response Planning Failures (Cont.)

Response Planning Failure	Contextual Influences	Event
Operators give priority to one accident response goal (or safety function) at the expense of another or disregard the importance of the safety function.	(1) Operators terminated HPI (without procedural guidance) because of concerns regarding filling the PRZR and lifting safety valves, but RCS pressure at termination and the continued decreasing pressure trend was not adequate for maintaining sub-cooling margin (and HPI had to be turned on again).	Crystal River 3 (12/8/91), RCS pressure transient during startup.
	(1) Because of inexperience, and lack of training and procedural guidance, the shift engineer overreacted to rising torus temperature and opened turbine bypass valves to reduce heat load, resulting in an unnecessary challenge to the reactor pressure vessel pressure control safety function (i.e., excessive cooldown rate). (2) Operators were generally unconcerned with the RPV cooldown rate because they assumed the technical specification cooldown rate limit would have been exceeded anyway.	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).

5.2.1.4 Error-Forcing Context in Response Implementation

The major contributors to the response implementation failures identified in the five example events are PSFs, although plant conditions also can affect an operator's general performance. Table 5.4 shows three categories of response implementation problems identified in the events analyzed:

(1) important procedure steps are missed
(2) miscommunication
(3) equipment failures hinder operators' ability to respond

The Crystal River 3, Dresden 2, and Ft. Calhoun events illustrate each of these problems, respectively. In the Crystal River 3 event, operators moved from one procedure to another before completing the section that would have directed them to take actions that would have terminated the event. However, operators are trained to know that it is good practice to check all remaining sections of a procedure for relevant steps before transferring to another. In the Dresden 2 event, supervisors gave vague directions to board operators who, in turn, took actions that were not appropriate. Finally, operators in the Ft. Calhoun event were hindered by hardware failures and design features that made it difficult to perform the appropriate response actions.

5.2.2 Performance-Shaping Factors

From the analyses of events carried out, it is evident that plant conditions played significant roles in all events. In addition, negative PSFs contributed to deteriorated human performance. As discussed in Section 5.1, poor environmental factors and ergonomics, unfamiliar plant conditions and/or situations, and inexperience, affected operator performance. The list below represents PSFs that negatively influenced operator performance in the five example events listed. Table 5.5 elaborates on this list of PSFs and provides the more traditional PSF terms.

Table 5.4 Examples of Response Implementation Failures

Response Implementation Failure	Contextual Influences	Event
Operators do not check all applicable sections of procedure before exiting - results in omission of important actions.	(1) Operators exited abnormal response procedure because SI termination criteria were met, so they missed the procedural directions for closing the isolation valve for the (failed) open PRZR spray valve.	Crystal River 3 (12/8/91), RCS pressure transient during startup.
Miscommunication results in inappropriate or less than optimal actions.	(1) Suppression pool cooling was not initially maximized, as required by procedure. (2) Operator was not given specific instructions as to the number of turbine bypass valves to be opened, the desired pressure at which the valves should be closed, or the desired rate of depressurization.	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
Equipment problems hinder operators' ability to respond to event.	(1) Failure of the safety valve created LOCA from the PRZR that could not be isolated. (2) Control of HPI during event was hindered by the fact that the relevant valve controls were located on a panel 8-10 feet away from the panel with the HPI flow and pressure indicators. Hence, two operators were required, one at each panel, in order to perform appropriate HPI control actions. (3) HPI valves were not designed as throttle valves, making it difficult to control flow and creating the need for monitoring HPI flow and pressure.	Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck open relief valve).

- human performance capabilities at a low point
- time constraints
- excessive workload
- unfamiliar plant conditions and/or situation
- inexperience
- nonoptimal use of human resources
- environmental factors and ergonomics

In some of the events analyzed, PSFs had an important impact on human performance, particularly in relation to the plant conditions at the time of the events (e.g., excessive workload and poor use of human resources in Dresden 2, inexperience and new conditions in Prairie Island 2). In other events, it is not clear that the factors shown in Table 5.5 strongly influenced the outcome of the events. Though the likelihood of PSFs triggering human errors by themselves is very low, this table illustrates that such factors (especially mismatches between plant conditions and PSFs) can distract operators from critical tasks or drastically hinder or inhibit their ability to perform. Also, in some

cases, the PSFs were activated by the specific plant conditions in the event context (i.e., operators lacked training or experience for the actual event conditions). In other cases, the PSFs seem to be generic or insensitive to the specifics of the event (e.g., environmental conditions).

5.2.3 Important Lessons from Analyses of Events

From analyses of events such as those documented in Appendix A and the excerpts given in Tables 5.1 through 5.5, some overall insights from operational experience were developed and are documented in Tables 5.6 and 5.7.

Table 5.6 is a list of characteristics that were commonly found in the serious accidents and event precursors reviewed using the ATHEANA perspective–both nuclear and non-nuclear. This list can be used as a kind of template in the ATHEANA search for unsafe actions and associated error-forcing contexts.

Table 5.7 is a list of important aspects of real operational events that are typically overlooked or dismissed in current PRAs. This list, in addition to being "blind spots" in PRAs, also can be used to identify operational situations that are potentially troublesome to operators.

Together, the two tables provide lessons learned that can be used to give a broader perspective in the ATHEANA search for unsafe actions and associated error-forcing contexts. The lessons learned provided by these two tables were important in developing the guidance given in the next section.

Most important, however, is their usefulness in overcoming the mindset pervading current HRAs. Even among the ATHEANA development team, these lessons, representing the evidence from past operational events, were an effective counter to the (apparently well-trained) tendency to argue that can't happen!

Both tables also highlight the importance of correct instrument display and interpretation in operator performance. Two of the characteristics listed in Table 5.6 are directly related to instrumentation problems. The first six factors shown in Table 5.7 are all related to instrumentation problems and show how such problems can affect operators and their situation assessment. This observation conforms with the theoretical consideration that situation assessment and situation model updating are critical phases of information processing. Table 5.7 also includes factors important to response planning and implementation. Other factors in Table 5.7 are related to the creation of unusual plant conditions that can cause equipment to fail, creating additional tasks for operators and otherwise hindering the operators' ability to respond to an accident.

Table 5.5 Examples of PSFs on Cognitive and Physical Abilities

PSF[a]	Contextual Influences	Event
Human performance capabilities at a low point (environmental conditions).	(1) Significant actions during the event took place between 3:00 a.m. and 4:00 a.m. (Effect of duty rhythm is expected to affect cognitive capabilities more than skill- or rule-based activities.)	Crystal River 3 (12/8/91), RCS pressure transient during startup.
	(1) Event occurred at 1:05 a.m.	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
	(1) Event occurred at 11:35 p.m. (2) Event occurred at the beginning of the shift, when awareness is typically high.[b]	Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).
	(1) Event occurred at 11:10 p.m.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.
Human performance negatively affected by time constraints (stress).	(1) Plant dynamics provided limited time (i.e., 18 minutes between detection of RCS pressure decrease and reactor trip) for investigation, analysis, and decision-making.	Crystal River 3 (12/8/91), RCS pressure transient during startup.
Aspect of the plant or its operation is new and unfamiliar to operators (training).	(1) First time electronic reactor vessel level instrumentation was used– its operation and design are not understood. (2) First time draindown was performed with such a high N_2 overpressure. (3) First time draindown was performed without experienced SE to support draindown operators. (4) Decay heat high (~6 MW) because only 2 days after shutdown.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.
Operators inexperienced (training, procedures).	(1) Operators relatively inexperienced in responding to unplanned transients (and may need closer supervision of their interpretation of transients, increasing reactor power, use of bypass controls, and use of procedures).	Crystal River 3 (12/8/91), RCS pressure transient during startup.
	(1) Operators and assisting system engineer performing draindown were inexperienced.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.

Table 5.5 Examples of PSFs on Cognitive and Physical Abilities (Cont.)

PSF	Contextual Influences	Event
Excessive workload interferes with operators ability to perform (organizational factors).	(1) The shift control room engineer (SCRE) was completely occupied with filling out event notification forms and making the required notifications to state and local officials and the NRC. Consequently, the SCRE was not able to perform his shift technical advisor (STA) function of oversight, advice, and assistance to the shift engineer (SE); potentially, this resulted in some loss of continuity in control room supervision's familiarity with the event circumstances. (2) The ability of the SE to function as emergency director in response to the event was impaired because he was diverted by the need to direct plant operators. (If the plant foremen had remained in the control room, they could have performed these activities.)	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
	(1) In addition to problems directly related to the initiator and stuck-open relief valve, operators experienced problems in plant support systems (e.g., fire (false) alarms in two areas of the plants, running air compressor shut down, toxic gas alarms shifted control room ventilation, turbine plant cooling water flow gauge ruptured and caused minor local flooding, PRZR heaters developed grounds as a result of the LOCA in the containment, temporary total loss of condensate flow when pumps tripped on SI signal, component cooling water to RCPs temporarily isolated when CCW pumps were sequenced) during the early stages of the event.[c]	Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).
	(1) System engineer assigned to assist in draindown also had the responsibility of functionally testing the new electronic level instrumentation (probably why he left control room during draindown to investigate potential problems with this instrumentation), leaving inexperienced operators without support.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.

Table 5.5 Examples of PSFs on Cognitive and Physical Abilities (Cont.)

PSF	Contextual Influences	Event
Nonoptimal use of human resources (organizational factors).	(1) When the SE arrived in the control room, he relieved the SCRE, who was in the control room when the SRV opened and who diagnosed the open SRV, so that the SCRE could fulfill the STA role. After this change of duties, the SCRE was completely occupied with other activities (see workload above) so he was not able to perform his STA function of oversight, advice, and assistance to the SE; potentially, this resulted in some loss of continuity in the control room supervision's familiarity with the event circumstances. (2) Both shift foremen for Units 1 and 2 were sent into the plant to perform local valve manipulations and other activities and therefore were not available to review, assess, and evaluate response to the event. Both foremen were in the control room when the SRV opened. (Shift clerks or equipment operators could have performed the activities assigned to the shift foremen.)	Dresden 2 (8/2/90), LOCA (stuck-open relief valve).
	(1) Normal control room operating crew and supervisors were busy with duties related to outage so (inexperienced) draindown operators received only occasional supervision, which also was not increased to compensate for the absence of the system engineer.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.
Environmental factors interfere with operators' ability to perform (human–system interface).	(1) Poor lighting in the area of the Tygon tube made taking readings difficult. (2) Because of view obstructions, it was difficult to take Tygon tube readings from the local observation position level.	Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.

[a] The term in parentheses is the more traditional PSF.

[b] Positive rather than negative factor in event and in operators' response.

[c] Although each of the support system problems required additional operator attention and time, operators appeared to be able to overcome or compensate for these distractions in this event.

Table 5.6 Characteristics of Serious Accidents and Event Precursors

Characteristic		Example
(1)	Extreme and/or unusual conditions	Seasonal grass intrusions in Salem 1 event, earthquakes, unusual plant configurations, high nitrogen pressure during shutdown at Prairie Island 2.
(2)	Preexisting conditions that complicate response, diagnosis, etc.	Failed auxiliary feedwater (AFW) system in TMI-2, instruments miscalibrated, etc.
(3)	Misleading or wrong information	PORV position indication in TMI-2, Tygon tubes with high nitrogen pressure in Prairie Island 2 shutdown event, temporary and wrong labels in Oconee 3 event.
(4)	Information rejected or ignored	Core exit thermocouples in TMI-2, sump level alarms in Oconee 3 shutdown event, multiple evolutions whose effects cannot be separated).
(5)	Multiple hardware failures	Davis Besse loss of feedwater event, TMI-2.
(6)	Transitions in progress	Prairie Island 2 shutdown event– draining down; Crystal River 3–startup).
(7)	Symptoms similar to frequent and/or salient events	Symptoms of going "solid" in TMI-2.

Table 5.7 Factors Not Normally Considered in PRAs

Factors	Examples
(1) Instrumentation fails (or is caused to be failed) and fails in many ways	• indication is high, low, lagging, stuck, or miscalibrated • preaccident failures (human and hardware-caused) • unavailable because of maintenance, testing, etc. • does not exist
(2) Instrumentation problems that cause operators to not use the instruments	• recent or persistent history of reliability and availability problems • inconsistent with other indications and/or initial operator diagnosis of plant status and behavior • lack of redundant instrumentation to confirm information • not conveniently located • redundant, backup indicator that is not typically used
(3) The instrumentation used by operators is not necessarily all that is available to them or what designers expect them to use.	• multiple, alternative (although perhaps not equivalent) front panel indications (but one indicator may be preferred or more typically used by operators) [Crystal River 3 (12/8/91)– strip chart recorders ignored] • redundant or alternative indicators available on back panels (but their use is perceived as inconvenient or unnecessary)[(Dresden 2 (8/2/90) back panel acoustic monitor] • indicators used outside their operating ranges (e.g., reactor vessel level indicators during midloop operations at shutdown [Prairie Island 2 (2/20/92)]
(4) Operators typically will believe valve position indicators in spite of contradictory indications.	• PORV fails open (as indicated by tailpipe temperature indications), while valve position indicator shows valve as shut [Crystal River 3 (12/8/91); Dresden 2 (8/2/90)] • RCS drain path through an open RHR valve (which was being locally stroke-tested) during shutdown [Oconee 3, (3/8/91)]
(5) Operators can misunderstand how instrumentation & control (I&C) systems work, resulting in erroneous explanations for their operation and indications.	• misunderstand the location of a sensor or what is sensed (e.g., valve stem position versus controller position) • misunderstand how what is sensed is translated into an instrument reading (e.g., RVLIS system, PRZR pressure is not "real," really an algorithm)

Table 5.7 Factors Not Normally Considered in PRAs (Cont.)

Factors	Examples
(6) A history of false or spurious or automatic actions will result in operator conditioning to expect these events (especially when reinforced by management directives) thereby overriding the formal diagnosis required for a real event.	• previous spurious reactor water cleanup (RCWU) system isolations in LaSalle 2 (4/20/92) and a management directive regarding such isolations lead to an erroneous bypass of automatic RCWU isolation • spurious main feedwater pump trips in Davis Besse loss of feedwater resulted in MFW being in manual control at the time of reactor trip
(7) One plausible explanation can create a group mindset for an operating crew.	• belief that RCS overcooling was the cause of the pressure transient in Crystal River 3 (which involved a 6-minute bypass of automatic HPI start) when a stuck-open PRZ spray valve was the actual cause
(8) Operators will persist in the recovery of failed systems.	• the alternatives have negative consequences • recovery is imminent (in the operators' opinion) • they were the cause of the system failure (i.e., recoverable failure)
(9) The recovery of slips may be complicated.	• Encounter unexpected I&C resetting difficulties (problems starting AFW in the Davis-Besse loss of feedwater event)
(10) Management decisions regarding plant configurations can result in defeated plant defenses and additional burdens on operators .	• scheduling of maintenance and testing activities • on-line corrective maintenance and entering limiting condition for operation (LCO) statements in technical specifications • special configurations or exceptions from technical specifications to address persistent hardware problems
(11) Multitrain (or "all-train") maintenance has been performed.	
(12) Systems do not always fail at T=0 in accident sequence (i.e., simultaneous with initiating event).	
(13) Systems and components are not truly binary state.	• can experience a range of degraded conditions between optimal performance and catastrophic failure

Table 5.7 Factors Not Normally Considered in PRAs (Cont.)

Factors	Examples
(14) Preexisting, plant-specific operational quirks can be important in specific accident sequences.	• history of spurious high steam flow signals due to design problem (causing spurious SI signals)– Salem 1 (4/7/94) • recent history of spurious main feedwater pump trips so feedwater was controlled manually at time of trip [Davis Besse (6/9/85)]
(15) "Sneak circuits" can exist.	
(16) Selective tripping failures are possible.	
(17) Dependencies can occur across systems (as well as within systems).	
(18) Plant power at the time of trip may be < 100%.	
(19) Technical specification requirements	• may not be met at the time of plant trip
(20) The specific, detailed causes of initiating events (especially those caused by humans) can be important to accident response.	

5.3 An Operational Event Example Illustrating Dependency Effects

The impact of complicating plant conditions and performance-shaping factors on operator situation assessment and hence performance can best be appreciated by example. An event sequence that occurred at Oconee 3 during a shutdown period in 1991 (Ref. 5.6) has been selected because it is fairly simple to describe and understand and because the diagnosis log for this event provides striking illustration that a powerful amount of contrary evidence is required to break through a strong mindset because of a mistaken situation model. Figure 5.1 shows the decay heat removal system at Oconee 3. In preparation for testing low-pressure injection sump suction valve 3LP-19, a maintenance technician set out to install a blind flange on line LP-19. By mistake, the blind was installed on line LP-20. Some two weeks later, an operator was sent to perform an independent check that the blind flange was properly installed. He reported that it was. At that time, a reactor operator and an I&C technician were authorized to perform the test. Because the flange was installed on the wrong line, stroking the valve initiated a loss of coolant. A significant amount of time was required to identify the source of leakage. Many alternatives were investigated before it was recognized that stroking the valve 3LP-19 opened a path to the sump.

Figure 5.2 (a,b,c) provides an analysis of this event using the HSECS format and coding scheme (see Ref. 5.4). Figure 5.2a summarizes plant conditions before and during the event. Figure 5.2b analyzes the three UAs and the recovery act in terms of the performance-shaping factors affecting

each act. Finally, Figure 5.2c describes the dependencies among the four acts. These dependencies explain why the diagnosis log (Figure 5.2c) can show that apparently six different cues could be ignored before the seventh cue finally forced the operators to investigate the test as the source of the problem. When an HRA analyst considers the separate cues independently, the analyst cannot help but conclude that failure is nearly impossible. However, recognizing the dependence among elements of evidence, failure remains a distinct possibility.

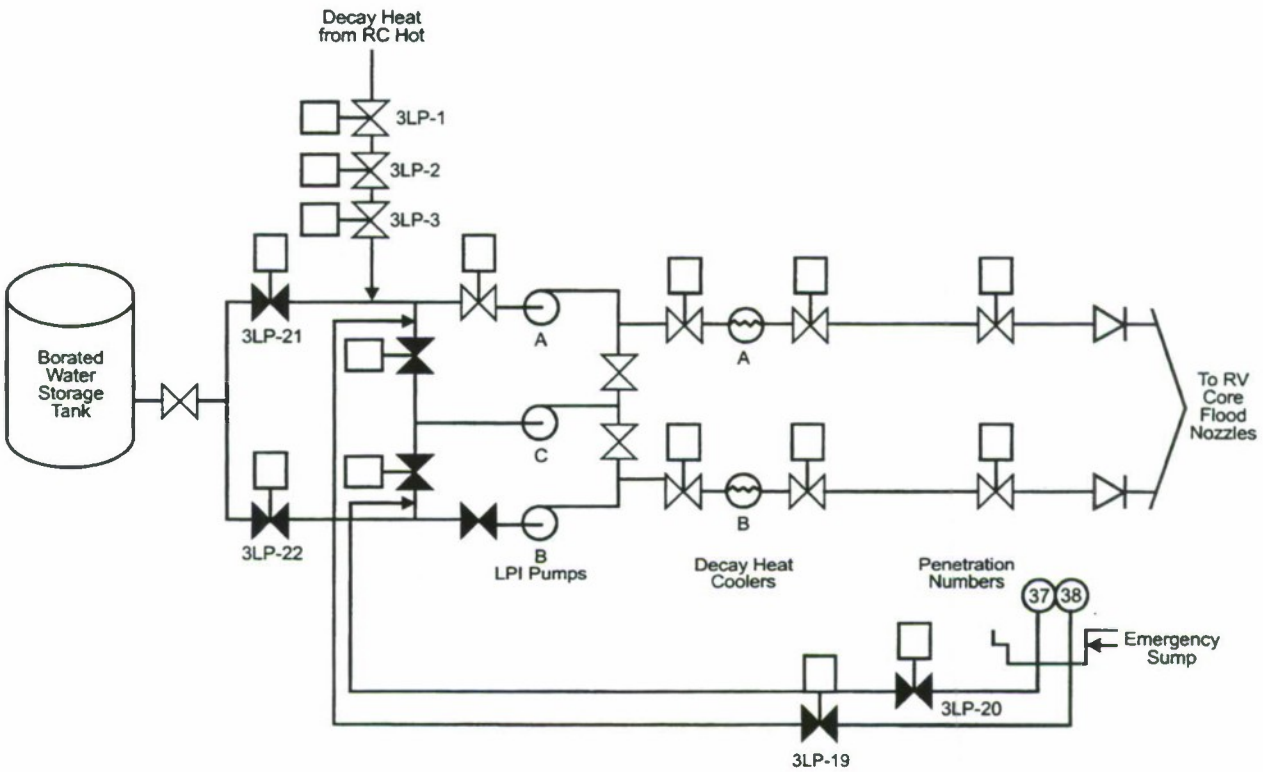


Figure 5.1 Oconee 3 Loss of Cooling

Plant Name: *Oconee 3*
Event Type: *Loss of RCS Inventory*
Secondary Event: *Loss of SDC*

Event Date: *3/8/91*
Event Time: *08:48*
Plant Type: *PWR/*

Description: *Loss of decay heat removal for ~ 18 min. because of a loss of RCS inventory via drain path to emergency sump created by combination of blind flange installed on wrong line and isolation valve stroke testing.*

INITIAL CONDITIONS

Other Unit Status:
RCS Conditions:
- **Power:** *Cold S/D*
- **Temperature (°F):** *94*
- **Pressure:** *(head off)*
- **RV Level:** *12 ft. above core (76 in. on wide RV wide-range level transmitter)*
- **Other:**

Plant Conditions:
* *24th day of refueling outage*
* *Refueling complete*

Plant Configuration:
Available:
* *LPI pump A & HX B operating*
* *LPI pump C*
* *RCS temperature indication via LPI*
* *RV level indication via dp instrument w/ CR indication*
* *Equipment & personnel hatches closed*

Unavailable:
* *LPI pump B (racked out)*
* *Incore instrumentation (e.g., RCS temperature)*
* *RB radiation monitors*
* *Containment open*

ACCIDENT CONDITIONS

Other Unit Status:
RCS Conditions:
- **Power:** *Cold S/D*
- **Temperature (°F):** *117*
- **Pressure:** *(head off)*
- **RV Level:** *4 ft. above core*
- **Other:**
  * *Loss of 9,700 gal. of RCS*

Plant Conditions:
* *14,000 gal. spilled via drain path to sump (RCS & BWST)*
* *Loss of SDC*
* *Maximum radiation dose rate - 8 rem/hr*
* *Local evacuation of areas in RB*

Automatic Equipment Response:
* *Various alarms (sumps & RV level)*

Hardware Failures:

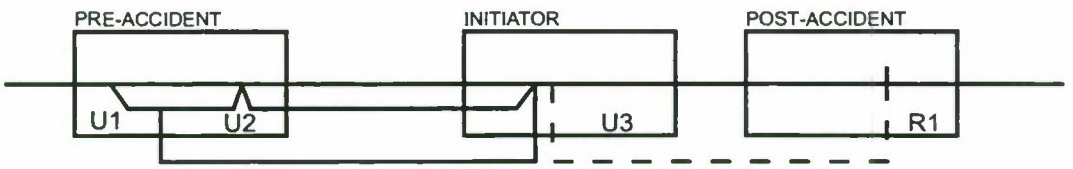
FINAL STATUS SUMMARY

Unique? (S/F/L/N): *L*
Significance:
Corrective Actions:
(5) Operator aids improved; stenciled labels added to sump suction lines
(8) Maintenance procedure modified: added requirements for proper identification and labeling of flanged connections

Comments: *AEOD report and LER used as sources of information*

Figure 5.2a Event Information

Event Timeline:



Unsafe Actions (U):

U1. Blind flange for LPI sump suction installed on wrong line
U2. Subsequent checking failed to detect incorrect flange installation
U3. RCS drained through unblanked sump line

Act No.	Error Effect	Error Mode	Error Type	S/R/K	Location	Personnel Type	Activity	PSFs (+/-)
U1	Latent	EOC	Mistake	R	ex-CR	Maintenance	Maintenance	-1 MMI (labels LTA): poor visibility & access -2 Procedures (incomplete): did not require penetration ID # -3 Training (LTA): incorrect use of drawing -4 Training (LTA): use of informal label -5 Org factors (lack of control): existence of informal labels -6 Org factors: incomplete procedures
U2	Latent	EOO	Mistake	R	ex-CR	NLO	Operations	-1,- 4, -5
U3	Initiator	EOC	Mistake	K	ex-CR in-CR	I&C, RO	Testing	-6 -7 Procedure (incomplete): did not specify coordination or testing activities -8 Communication (no repeat back): misunderstanding between I&C and RO

Other Events (Nonhuman Error) (E, H, or R):

R1. Operators isolate drain path, restore RCS level, and restore SDC (including pump venting)

Event No.	Effect	S/R/K	Recovery Time	Recovery Location	Personnel Type	PSFs & Defenses (+/-)
R1	Recovery	R & K	23 minutes	in-CR, ex-CR	RO	-7, -8 +9 Procedure: Loss of DHR was useful in response +10 Training: +11 Communication: HP in RB on RCS level drop • Sump alarms • In-CR RV level indicator

Figure 5.2b Summary of Human Actions

HARDWARE DEPENDENCIES

System(s) Involved:
LPI

Interfacing Systems:
RCS

Component(s) Involved:
LPI sump line isolation valve (3LP-19)
BWST suction line isolation valves (3LP-21 & -22)
BWST

Spatial Dependencies:

HUMAN DEPENDENCIES

Actions	Dependence Mechanism	Description
U1, U2	*Common PSFs*	*MMI (labeling), training (use of informal label)*
U1, U2	*Common organizational factors*	*Existence of informal label*
U1, U3	*Common organizational factors*	*Incomplete procedures*
(U1&U2), U3	*Cascading effect (i.e., setup)*	*Planned defense defeated*
(U1, U2, U3), R1	*Suboptional response due to CR perception/ reality mismatch created by previous actions*	*Positive PSFs and defenses provided justification for the break with mindset required for response*

ACCIDENT DIAGNOSIS LOG

Accident Symptoms	Response
RB emergency sump high-level alarm	* *None*
RV level reading at 20 inches and decreasing	* *Erroneous operation of RV wide-range level transmitter suspected*
RB normal sump high-level alarm	* *Washdown operations suspected*
RV ultrasonic-level alarm (i.e., no water in HL pipe nozzle)	* *Investigation of cause begun* * *Entered AP/3/A/1700/07, loss of LPI in DHR mode*
HP in RB verifies reduction in RV level and increasing radiation	* *None*
LPI pump A current fluctuating downward	* *Stopped pump* * *Opened BWST suction isolation valves*
Evidence that RCS was not being filled	* *Reclosed BWST isolation valves* * *NLO sent to close 3LP-19 or -20*
HP notifies CR that 6-12 gallons of water are on RB floor near emergency sump	

Figure 5.2c Event Dependencies

5.4 Summary

In summary, the above discussion demonstrates that analyses of operational events can be used in two ways when applying ATHEANA:

(1) They can provide illustrative examples of UAs, EFCs, and other human performance factors (i.e., anecdotes).

(2) They can assist in the development of generalized categories of UAs that can be used to search for UAs and associated EFCs to model in a PRA.

In both cases, such examples derived from event analyses are used to guide HRA analysts in applying ATHEANA.

The understanding of operator performance developed through analyses of events also laid the foundations for the development of ATHEANA application and procedures. It is evident from the events analyses discussed that UAs are likely to be caused at least in part by actual instrumentation problems or misinterpretation of existing indications. The associated EFCs, therefore, are more likely to exist when instrumentation failures or interpretation errors are combined with deficient procedures (probably triggered or revealed by specific plant conditions). This knowledge supported the development of the search aids for EFC and UAs.

5.5 References

5.1 M. Barriere, W. Luckas, D. Whitehead, A. Ramey-Smith, D. Bley, M. Donovan, W. Brown, J. Forester, S. Cooper, P. Haas, J. Wreathall, and G. Parry, *An Analysis of Operational Experience during Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues*, NUREG/CR-6093, Washington, D.C., June 1994.

5.2 M. Barriere, J. Wreathall, S. Cooper, D. Bley, W. Luckas, and A. Ramey-Smith, *Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies*, NUREG/CR-6265, Washington, D.C., August 1995.

5.3 S. Cooper, W. Luckas, J. Wreathall, G. Parry, D. Bley, W. Luckas, J. Taylor, and M. Barriere, *A Technique for Human Error Analysis (ATHEANA)*, NUREG/CR-6350, Washington, D.C., May 1996.

5.4 S. Cooper, A. Ramey-Smith, W. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report L-2415/95-1, Brookhaven National Laboratory, December, 21, 1995.

5.5 J. Reason, *Human Error*, New York, Cambridge University Press, 1990.

5.6 U.S. Nuclear Regulatory Commission, Augmented Inspection Team Report, *Oconee, Unit 3, Loss of RHR* (March 9, 1991), No. 50-287/91-008, Washington, D.C., April 10, 1991.

6 OVERVIEW OF THE ATHEANA PROCESS

While Part 1 discussed the principles and concepts underlying ATHEANA, Part 2 provides the more practical, "how- to" steps for applying the methodology. However, as stated earlier, the material in Part 1 underlies the application guidance given in Part 2. For example, Sections 1, 2, and 3 provide the general basis and perspective that guide applications of ATHEANA at a high level. The understanding and concepts from behavior science described in Section 4 are used directly in the prospective ATHEANA process to identify the elements of error-forcing contexts. Finally, the understanding gained from reviews of operational experience, such as that summarized in Section 5, not only helped form the basis of the ATHEANA perspective but also can assist analysts in applying the ATHEANA process.

This section provides:

(1) a road map to the remainder of Part 2, Sections 7–11

(2) a summary of the two ATHEANA application processes
- retrospective analyses of past operational events,
- prospective analyses [or human reliability analyses (HRA)] to support probabilistic risk assessment (PRA) or other risk studies

(3) a perspective on the place of ATHEANA among the many HRA methods

6.1 Road Map to Part 2

Section 7 describes the preparatory activities that should be performed before applying ATHEANA. These include:

- selection of analysis activity (retrospective analysis, prospective analysis, or both)
- selection and training of the multidisciplinary team that will apply ATHEANA
- collection of background information
- planning for use of simulator exercises in applying ATHEANA

Section 8 describes the approach for performing retrospective analyses based upon the ATHEANA perspective. This is illustrated by the examples of event analyses given in Appendix A.

Sections 9 and 10 present the prospective ATHEANA analysis. They provide guidance on how to perform a human reliability analysis using ATHEANA. While the focus of this guidance is on the performance of an HRA to support a PRA, both qualitative and quantitative analyses are addressed. Section 9 provides guidance on:

- selecting an issue for analysis
- setting the scope of the analysis

- identifying and defining human failure events and unsafe actions
- defining the error-forcing context for a human failure event (HFE) or an unsafe action (UA).

Section 10 principally addresses the quantification of HFEs and their incorporation in PRAs. However, qualitative analyses for issue resolution can be obtained by performing the same types of assessments that are used for quantitative analyses. Section 11 summarizes the purpose and capabilities of ATHEANA.

Examples of retrospective analyses are presented in Appendix A, while examples of prospective analyses are presented in Appendices B–E.

6.2 Summary of Retrospective ATHEANA Analysis

The retrospective analysis initially was developed to support the development of the prospective ATHEANA analysis. However, as the retrospective analysis matured, it became evident that this approach was useful beyond the mere development of the ATHEANA prospective approach. For example, as shown in Sections 3 and 5, the results of retrospective analyses are powerful tools in illustrating and explaining ATHEANA principles and concepts. Also, the ATHEANA approach for retrospective analysis was used to train third-party users of ATHEANA in an earlier demonstration of the method. In this training, not only example event analyses, but actual experience in performing such analyses helped new users develop the perspective required to apply the prospective ATHEANA process. Finally, the results of event analyses using the ATHEANA approach are useful in themselves.

The retrospective approach can be applied broadly, using the ATHEANA framework described in Section 2. Both nuclear and non-nuclear events can be easily analyzed using this framework and its underlying concepts. A more detailed approach has been developed for nuclear power plant events, although it can be generalized for other technologies. This more detailed approach is more closely tied to the ATHEANA prospective analysis than general use of the framework. Section 8 provides examples of event analyses using the framework approach and guidance for performing the more detailed analyses. Appendix A provides examples of more detailed analyses for six nuclear power plant events.

In performing retrospective analysis, the basic objective is to gain an understanding of the causes of human failures in risk-significant operational events. To do so, the analysts must answer such question as:

- What happened?
- What were the consequences?
- Why did it happen (i.e., what were the causes)?

Important features of the detailed retrospective analysis approach include:

- a summary of what happened in the event
- identification of the important functional failures
- an event time line
- a summary of important human actions and their apparent causes
- a summary of the important contextual factors (i.e., plant conditions and performance-shaping factors) before, during, and after the event
- an event diagnosis log showing plant conditions and operator responses to them as a function of time

Potential users of the ATHEANA retrospective analysis should be cautioned that this approach has been developed to take advantage of the amount of information typically provided in detailed accounts of events. Experience has shown that there are limited benefits in applying this approach to event reports containing incomplete information. In these cases, the analysts must be willing to do the research necessary to obtain the information needed. (See Appendix C in Refs. 6.1 and 6.2 for a discussion of this issue.)

6.3 Summary of Prospective ATHEANA Analysis

The prospective ATHEANA process is illustrated in Figure 6.1, which identifies and summarizes ten major steps in the process (following preparatory tasks, such as assembling and training the analysis team, which are described in Section 7). Section 9 provides detailed guidance on how to perform Steps 1 through 8. Steps 9 and 10 are described in Section 10. Illustrative examples of how to apply all ten of the process steps are given in Appendices B through E.

The ten steps in the prospective ATHEANA process are:

Step 1: Define and interpret the issue

The purpose of this first step is to define the objectives of the analysis being undertaken, i.e., why it is being performed. ATHEANA can support a wide range of HRA applications, from complete PRAs to special studies focused on specific issues. In the nuclear power industry, because most plants have already performed a PRA, the issues for which the PRA will be extended using ATHEANA will usually focus on the significance of human contributions to risk and safety that are particular areas of concern to the NRC or plant management. In such applications, the issue to be addressed usually defines a relatively narrow scope of

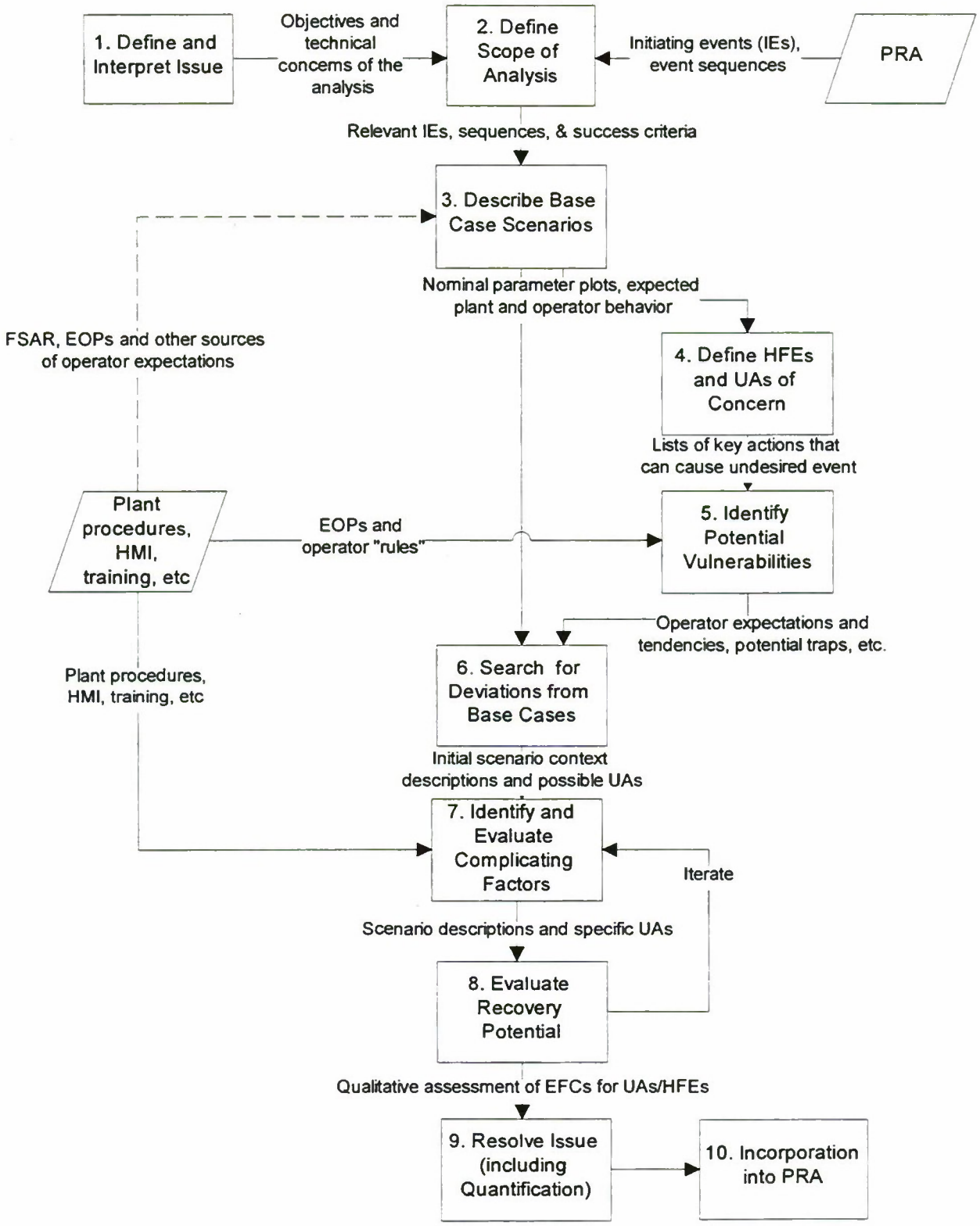


Figure 6.1 ATHEANA Prospective Search Process

analysis. In this step, the issue is defined to provide the basis for bounding the scope of the analysis (Step 2) and for other analysis steps.

Step 2: Define the scope of the analysis

This step limits the scope of the analysis by applying the issue defined in Step 1 and, if necessary for practical reasons, further limits the scope by setting priorities on the characteristics of event sequences. Although ATHEANA can be used for both PRA and non-PRA applications, the process for setting priorities is based upon plant-specific PRA models and general concepts of risk significance. The first limitation is to select the initiating event classes and associated, relevant initiators to be analyzed. Later scope restrictions are then considered for each selected initiator, balancing analysis resources against specific project needs.

Step 3: Describe the base case scenario

In this step, the base case scenario is defined and characterized for a chosen initiator(s). The base case scenario:

- represents the most realistic description of expected plant and operator behavior for the selected issue and initiator

- provides a basis from which to identify and define deviations from such expectations (which will be performed in Step 6)

In the ideal situation, the base case scenario:

- has a consensus operator model (COM)
- is well defined operationally
- has well-defined physics
- is well documented in public or proprietary references
- is realistic

Operators and operator trainers provide the information to describe the consensus operator model. This model exists if a scenario is well defined and consistently understood among all operators. Procedures and operator training help to describe the scenario operationally. Documented reference analyses [e.g., plant-specific final safety analysis reports (FSARs) or other detailed engineering analyses of the neutronics and thermal hydraulics of a scenario] can assist in defining the scenario operationally and the scenario physics. The most relevant reference analyses are those that closely match the consensus operator model. The reference analyses may need to be modified to match the consensus model or to be more realistic.

The consensus operator model and reference analyses together form the basis for defining the base case scenario. In the ideal case, the description of the base case scenario should include:

- a list of assumed causes of the initiating event
- a brief, general description of the expected sequence of events, starting before reactor trip (considering key functional parameters such as reactor power, electric power, reactor coolant system level and pressure, and core heat removal)
- a description of the assumed initial conditions of the plant
- a detailed description of the expected sequence and timing of plant behavior (as evidenced by key functional parameters) and plant system and equipment response
- the expected trajectories of key parameters, plotted over time, that are indications of plant status for the operators
- any assumptions with respect to the expected plant behavior and system or equipment and operator response (e.g., equipment assumed to be unavailable, single failures of systems assumed to have occurred)
- key operator actions expected during the scenario progression

The description of the base case scenario is the basis for defining deviation scenarios in Step 6. However, in practice, the available information for defining a base case scenario is usually less than ideal.

Step 4: Define HFE(s) and/or UAs

Possible human failure events and/or unsafe actions can be identified and defined in this step. However, Step 1 may have already defined an HFE or UA as being of interest. Alternatively, the deviation analysis, recovery analysis, or quantification performed in later steps may identify the need to define an HFE or UA. Also, recovery analysis or quantification may require development and definition of operator actions at a different level (e.g., UA versus HFE). Consequently, the ATHEANA analysis may require iteration back to this step. To the extent possible, the information that would be needed in any of these cases is provided in this step.

HFE definitions are based upon the critical functions required to mitigate the accident scenario, expected operator actions, operator actions that could degrade critical functions, and features of the plant-specific PRA model. Unsafe actions are the specific operator actions inappropriately taken or not taken when needed that result in a degraded plant state.

Several tables and associated guidance are provided to assist in the definition of HFEs and UAs.

Step 5: Identify potential vulnerabilities in the operators' knowledge base

This is a preliminary step to the searches for the deviations from the base case scenario that are identified in Steps 6 and 7. In particular, analysts are guided to find potential vulnerabilities in the operators' knowledge base for the initiating event or scenario(s) of interest that may result in the HFEs or UAs identified in Step 4. For example, they identify the implications of operator expectations and the associated potential pitfalls (i.e., traps) inherent in the initiating event or scenario(s) that may represent vulnerabilities in operator response.

The information that is obtained in this step should be put on a mental or literal blackboard for use in later steps, especially Step 6. In this way, analysts will be reminded of and guided to the more fruitful areas for deviation searches, based upon the inherent vulnerabilities in the operators' knowledge base for the initiator or scenario of interest.

Potential traps inherent in the ways operators may respond to the initiating event or base case scenario are identified through the following:

- investigation of potential vulnerabilities in operator expectations for the scenario
- understanding of a base case scenario time line and any inherent difficulties associated with the required response
- identification of operator action tendencies and informal rules
- evaluation of formal rules and emergency operating procedures expected to be used in response to the scenario

Step 6: Search for deviations from the base case scenario

The record has shown that no serious accidents have occurred for a base case (or expected) scenario. On the contrary, past experience indicates that only significant deviations from the base case scenario are troublesome for operators. Thus, in Step 6, the analysts are guided in the identification of deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). In serious accidents, these deviations are usually combinations of various types of unexpected plant behavior or conditions.

The search schemes in this step guide the analysts in finding physical or "physics" deviations, which are real deviations in plant behavior and conditions. Analysts may identify

performance-shaping factors and explanations for human behavior (e.g., error mechanisms), along with these plant conditions.

Four somewhat overlapping search schemes are used to identify characteristics that should be contained in a deviation scenario. However, each search scheme has a slightly different perspective regarding significant plant or human concerns. These four search schemes are:

(1) identify physical deviations from the base case scenario (e.g., how can the initiator be different?)

(2) evaluate rules with respect to possible deviations

(3) use system dependency matrices to search for possible additional causes of the initiator or the scenario development

(4) identify what operator tendencies and error types match the HFEs and UAs of interest.

After each of the search schemes has been exercised, the analysts should review and summarize the characteristics of a deviation scenario (or potentially important deviations) that were identified in the searches. In ATHEANA, the combination of plant conditions (including the deviations), along with resident or triggered human factors concerns, defines the error-forcing context for a human failure event that is composed of one or more unsafe actions. With these combined results, the analysts then develop descriptions of deviation scenarios and associated HFEs or UAs. These deviations also become the initial error-forcing context for the HFEs or UAs. Step 7, builds upon or refines this initial error-forcing context (EFC) definition by identifying other possible complicating factors (including possible hardware failures) and resident or triggered human factors concerns (e.g., mismatches between deviant plant behavior or conditions and procedures or other job aids).

Step 7: Identify and evaluate complicating factors and links to performance shaping factors (PSFs)

This step expands and further refines the EFC definition begun in Step 6 by considering:

- performance-shaping factors
- additional physical conditions, such as:
  - hardware failures, configuration problems, or unavailabilities
  - indicator failures
  - plant conditions that can confuse operators
  - factors not normally considered in PRAs

Like Step 6, this step may need to be performed iteratively with quantification (Step 9). In particular, the judgments that analysts will need to make regarding how many complicating factors to add to the EFC are best based upon the quantification considerations.

Step 8: Evaluate the potential for recovery

In this step, the definitions of HFEs and the associated EFCs are completed by considering the opportunities for recovering from the initial error(s) (or more precisely not recovering from initial errors). Performance of this step, perhaps even more so than previous search steps, is linked to issues considered in quantification. Consequently, some iteration between this step and the quantification step is possible. Also, since the consideration of the opportunities for recovery will involve extending the context defined in previous deviation search steps, recovery analysis also is iterative with Steps 6 and 7. The analysts are provided with guidance to identify the additional contextual factors (e.g., new cues for action or new plant symptoms) that might aid operators in recovering from their initial inappropriate actions. If an HFE can be ensured to be recovered, the analysis stops and proceeds to issue resolution. If recovery cannot be ensured, then the analysis proceeds according Step 9.

Step 9: Quantify the HFE probability

In this step, the probabilities of the human failure events (and associated unsafe actions) that have been identified and defined in the previous steps are quantified. ATHEANA requires a somewhat different approach for quantification from those used in earlier HRA methods. Where most existing methods have assessed the chance of human error occurring under nominal accident conditions (or under the plant conditions specified in the PRA's event trees and fault trees), quantification in ATHEANA becomes principally a question of evaluating the probabilities of specific classes of error-forcing contexts within the wide range of alternative conditions that could exist in the scenario, and then evaluating the conditional likelihood of the unsafe action occurring, given the occurrence of the EFC. The overall probability of the HFE also takes into account the potential for recovery and its associated contextual factors and potential mismatches.

Human failure events are quantified by considering three separate but interconnected stages:

(1) the probability of the EFC in a particular accident scenario

(2) the conditional likelihood of the UAs that can cause the human failure event

(3) the conditional likelihood that the UA is not recovered prior to the catastrophic failure of concern (typically the onset of core damage as modeled in the PRA)

Step 10: Incorporate the HFE into the PRA

After human failure events are identified, defined, and quantified, they must be incorporated into a PRA. When using ATHEANA, this process is generally identical to that already performed in state-of-the-art HRAs. Guidance for certain ATHEANA-specific incorporation issues is provided.

6.4 The ATHEANA Prospective Process: An Evolutionary Extension of Existing HRA Methods

PRA and HRA practitioners may ask: when is it necessary or proper to apply ATHEANA to an HRA problem? Such a question fails to recognize that, at some level ATHEANA is always used. In a real sense, ATHEANA is evolutionary, not revolutionary. Practitioners will recognize that, at the most general level, the ATHEANA prospective process steps introduced in the previous section have the same titles as the tasks required to support and perform HRA in existing PRAs. In some HRA methods, these steps are integral to the method itself;[1] in others, they must be performed before the method can be applied. The ATHEANA prospective process description, to be presented in Section 9 of this report, provides instructions for applying each HRA step. At this detailed level, ATHEANA makes activities explicit that are implicit or assumed as input information in many other methods. The detailed ATHEANA steps also extend current methods to consider new concepts in a number of areas. Consequently, the question for practitioners becomes, whether or not to apply the full detail of ATHEANA. This is really a project management decision that depends on the intended use of the HRA/PRA and the potential impact on risk of an abbreviated approach. Simplifications may be reasonable, but the consequences of the loss of information caused by such simplifications, on the evaluation of risk and on risk management capabilities, should be consciously recognized.

For reasons described below, the full detail of Steps 1 through 4 should always be performed. Anything less will prove costly. The additional effort involved in following the ATHEANA guidance the first time will pay for itself in saved effort later. Parts of the remaining steps are also always needed, if the analysis is to have a clear basis and be well documented. In these cases, ATHEANA bolsters existing methods by providing clear guidance and providing control of the PRA/HRA project. It is more rigorous and systematic, as well as more explicit, than that for previous HRA processes and methods. For example, the definition of the base case in Step 3 forces careful consideration and documentation of plant thermal-hydraulic performance, the search for HFEs and UAs in Step 4 is systematic and based on plant functional requirements, the search for potential vulnerabilities in Step 5 organizes relevant information in a useful form and requires a

[1] SHARP (Ref. 6.3) and SHARP1 (Ref. 6.4) were the only early HRA documents to lay out a systematic and complete HRA process, rather than simply providing methods to quantify the probability of HFEs. ATHEANA builds on these ideas, adding more detail to the search for HFEs, anchoring the method more tightly to knowledge from the behavioral sciences, developing a search process for error-forcing context, and extending the PRA concept of plant state to a more general concept of plant conditions.

detailed review of procedures for potential ambiguities, and the evaluation of recovery in Step 8 concentrates on dependencies that can defeat the efficacy of multiple cues. Where ATHEANA really breaks from the past is in the search for error-forcing context. The searches in Steps 6 and 7 go well beyond simple PSF identification of previous methods. They root out unexpected plant conditions that, coupled with relevant PSFs, can have significant impact on human information processing, enabling a wide range of error mechanisms and error types. The search for scenario deviations is deeply tied to the ATHEANA perspective of serious accidents that is discussed in Part 1. The result of this change is that quantification becomes more an issue of calculating the likelihood of specific plant conditions, for which UAs are much more likely than would be true under anticipated conditions. The benefits of all these improvements are:

- explicit guidance for performing each step
- consistency among analyses
- increased efficiency, in the long run
- added traceability
- added realism and credibility
- improved completeness
- more rigorous analysis

The following discussion provides more details, for each ATHEANA process step, regarding the enhancements provided by ATHEANA over previous HRA processes.

Steps 1 and 2: Define and Interpret the Issue and Define Scope of Analysis

Even if not explicitly defined as part of the method, these steps are always be done, either explicitly or implicitly. The ATHEANA process recommends explicit definitions of the issue and scope to better focus the analysis and make it more efficient. Past PRA experience has shown that significant effort can be wasted or inappropriate analyses may be performed, when these steps are not carefully specified early on.

Step 3: Describe Base Case Scenarios

All analyses must include a realistic characterization of the scenarios in which the HFEs occur, if the analysis is to have any hope of viable quantification and later consideration of recovery. While this step is usually not described in other HRA methods, some more thorough analyses have included some description of plant behavior and a time line of significant events in the scenario progression. The ATHEANA process explicitly addresses this step and adds rigor to its performance by recommending the development of a complete description of the scenario to be analyzed, including a realistic thermal-hydraulic analysis that defines the time sequencing of the scenario progression and the behavior of key plant parameters. It also requires an evaluation of the operators familiarity with the scenario. ATHEANA uses the base case scenario as a well-defined basis for finding deviation scenarios in Step 6.

Step 4: Define HFEs and UAs of Concern

Very few HRA methods provide search tools to identify the human failure events (HFEs) to be included in the PRA or the specific unsafe acts that can cause them. Typically they provide algorithms and tables to quantify HFEs identified elsewhere. Nevertheless, these events must always be specified before the HRA can continue. Traditionally, identification of HFEs have been based upon HFEs included in previous PRA models and operator actions required in procedures (both EOPs and surveillance procedures). This basis restricts the range of possible HFEs to those events called "errors of omission" in PRA jargon. Consequently, by failing to use a structured search process to identify potential HFEs, is very likely that important events, for example, those "errors of commission" discussed in Part 1, will be missed. The ATHEANA HFE search has two bases: 1) the required system functions for the scenarios under consideration and 2) the failure modes for the associated equipment.

Step 5: Identify Potential Vulnerabilities

This step provides a bridge between the preparatory work in the first four steps and the analysis to follow. It involves organizing available information for easy access in the analysis:

- *Investigation of potential vulnerabilities in operator expectations for the scenario.* Most methods provide for consideration of familiarity and training. ATHEANA pushes further, asking analysts to identify if those factors could cause problems if the scenario deviates from the most common case.

- *Understanding of a base case scenario time line and any inherent difficulties associated with the required response.* This is a summary review of the scenario information from Step 3, organized to identify time regimes of interest and associated influences on operators. While not specified in other methods or documented in existing analyses, thorough analysts using other methods identify and consider such characteristics.

- *Identification of operator action tendencies and informal rules.* No existing analyses or methods document these factors, but some analysts consider such factors on an ad hoc basis. ATHEANA provides both guidance and examples.

- *Evaluation of formal rules and emergency operating procedures expected to be used in response to the scenario.* All competent analysts examine plant procedures and consider their impact on operations. A few existing methods (see, for example, Refs. 6.5 and 6.6) encourage, as ATHEANA does, a rigorous review of procedures for potential problems with respect to specific scenarios.

Once again, many PRA analyses have considered some of the requirements of ATHEANA Step 5. The only aspect of the ATHEANA analysis that is particularly time-consuming is the formal mapping of the emergency procedures, including the identification of potential ambiguities and flagging of steps that might turn off system functions. Even so, the effort involved in a formal analysis of the procedures is not a major cost and the identification of potential vulnerabilities can be very important.

Steps 6 and 7: Search for Deviations and from Base Cases and Identify and Evaluate Complicating Factors

These two steps are unique to ATHEANA and comprise the search for error-forcing context. Most other methods do not search for context; rather, they assess it. Also, most other methods define the context in terms of the status of selected equipment modeled in the PRA and performance shaping factors (PSFs) such as stress, time available versus time required for action, training, and quality of procedures. Some of these methods narrowly constrain the set of PSFs.

As discussed in Part 1, the study of serious accidents suggests that accidents often occur when a strong error-forcing context both causes unsafe acts and precludes timely recovery. Such a strong context often includes plant conditions that go beyond the scenarios and equipment modeled in PRAs (e.g., failed instruments, unexpected control system actuation, and specific scenarios not thoroughly presented in training sessions). In order to extend the usefulness of HRA beyond merely providing risk estimates to assisting in risk management (where the understanding the causes of human error is needed to identify risk reduction strategies), identification of the error-forcing context is essential. The definition of context (and, therefore, the description of the causes of human error) used in traditional HRA methods typically is based upon insufficient factors.

Even for the purposes of simply estimating risk, failing to search for error-forcing context represents a gamble that the HRA method's quantification tools are based on data that adequately represent an average over the full range of weak and strong contexts. These contexts should apply to the kind of facility [i.e., commercial nuclear power plants (NPPs)] under analysis and its range of crew characteristics. That means that a human error probability should be calculated from human errors occurring in events that cover the span of contexts possible in the NPP and that the contexts (weak to very strong) occur in the same proportion as in the NPP. Thus there are several difficulties: current NPP experience is not extensive enough to have covered the range of possible contexts thoroughly enough to support such an approach and, for data from other facilities, it is difficult to argue that the contexts are comparable and in the proper proportion. Because events with very strong error-forcing context are the primary contributors to the probability of HFEs leading to serious damage, failure to have a proper representation of the average, will almost certainly lead to an underestimate of the risk.

Step 8: Evaluate the Potential for Recovery

All methods include modeling and quantifying recovery. However, many analyses treat the probability of recovery as independent of the original human failure event and previous recovery opportunities. Most HRA practitioners recognize that such treatment is a losing gamble, guaranteed to obscure important contributors to risk.

Dependencies caused by the overall context influencing both potential recovery actions and earlier HFEs is the theme of serious accidents. Consequently, the problem of evaluating the probability for the initial HFE as an average over all contexts is compounded when the opportunities for non-recovery are considered. Average evaluation of initial HFEs, combined with average evaluation of recovery, will miss the risk-driving cases that are linked through a single strong context.[2]

Steps 9 and 10: Issue Resolution (including Quantification) and Incorporation into PRA

The ATHEANA process includes the two traditional steps of quantification and incorporation of the HFE in PRA. In addition, the ATHEANA process recognizes that qualitative analyses may be the desired end-product of an HRA. Because the ATHEANA method provides more specific, credible, and soundly-based causes for human failures, the qualitative insights provided by ATHEANA can have more practical uses than those provided by some previous HRA methods.

The ATHEANA quantification method is still under development. The current approach was developed for cases when the context is strongly error-forcing. In such cases, a judgment-based evaluation of probability that considers fully the plant conditions and performance shaping factors (based on potential error mechanisms and error types) is preferable to a data-based method where the data are not specific to the context.

When a traditional HRA quantification method is used (i.e., a "context averaged" method as discussed earlier), care must be exercised to ensure that the quantification process uses human error probabilities truly based on a full range of contexts around the plant state and PSFs specified for the action being quantified. Often, however, the extremes in the full range of contexts (i.e., the "tails" of the context distribution) are omitted from consideration. For example, when events such as the TMI-2 accident or Chernobyl are removed from the NPP data, because their causes have been "fixed," no severe context events remain and the data are skewed toward optimistic values.

---

[2]This implies that if a context averaged evaluation of the probability of the HFE was used, proper consideration of recovery will be difficult, if not impossible. Even if a very conservative view of recovery is taken (e.g., consideration of only a single recovery possibility and using a pessimistic evaluation of its probability of success) evaluation of the probability of recovery cannot be guaranteed to be realistic. The combination of a less likely, but more severe context HFE, with little or no chance of recovery, may be a much greater contributor to risk.

6.4.1 Summary

ATHEANA is a thorough process for identifying, analyzing, and documenting human failure events and contexts that make them more likely. At a high level, the ATHEANA steps are required by all approaches to HRA and involve four areas: specification of the problem, search for HFEs, search for (or identification of) context, and quantification.

The only area where the details of ATHEANA involve significantly more effort than other methods is the search for context. Many of the other methods omit steps in this process or offer a quantification approach that is intended to represent an average result over a wide range of possible contextual conditions. Depending on the intended use of the HRA/PRA and the potential impact on risk, simplifications may be reasonable, but the reduction in information provided by such simplifications should be consciously recognized.

6.5 References

6.1 M. Barriere, W. Luckas, D. Whitehead, A. Ramey-Smith, D. Bley, M. Donovan, W. Brown, J. Forester, S. Cooper, P. Haas, J. Wreathall, and G. Parry, *An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues*, Sandia National Laboratories, NUREG/CR-6093, June 1994.

6.2 S.E. Cooper, W.J. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report L-2415/95-1, Upton, NY, December 21, 1995.

6.3 G.W. Hannaman and A.J. Spurgin, *Systematic human action reliability procedure (SHARP)*. EPRI NP-3583. Palo Alto, CA: Electric Power Research Institute, 1984.

6.4 D.J. Wakefield, G.W. Parry, A.J. Spurgin, and P. Moieni. *Systematic human action reliability procedure (SHARP) enhancement project, SHARP1 methodology report*. EPRI TR-101711. Palo Alto, CA: Electric Power Research Institute, 1992.

6.5 J. Julius, E. Jorgenson, G.W. Parry, and A.M. Mosleh, "A procedure for the analysis of error of commission in a Probabilistic Safety Assessment of a nuclear power plant at full power," *Reliability Engineering and System Safety* **50**: 189-201, 1995.

6.6 D.J. Wakefield, "Application of the human cognitive reliability model and confusion matrix approach in a probabilistic risk assessment," *Reliability Engineering and System Safety*, **22**: 295-312,1988.

7 PREPARATION FOR APPLYING ATHEANA

This section describes the preparatory activities required for applying the ATHEANA process. They include:

- selection of analysis activity (i.e., retrospective analysis, prospective analysis, or both)
- selection and training of the multidisciplinary team who will apply ATHEANA
- collection of background information
- planning for use of simulator exercises in applying ATHEANA

While it is assumed that the activities typically performed in preparing to perform an HRA (e.g., plant familiarization, gaining an understanding of the PRA model) also are performed in applying ATHEANA, these activities are not discussed here. For a discussion of the requirements of a "quality" HRA, refer to Part 4, Chapter 14 of the IPE Insights Report, NUREG-1560 (Ref. 7.1) and NUREG-1602 (Ref. 7.2).

7.1 Select the Analysis Activity

ATHEANA can be used in the following three activities:

(1) retrospective analysis
(2) prospective analysis, or
(3) both retrospective and prospective analysis

For retrospective analysis, the scope of the analysis is an actual plant event. Section 8 provides additional guidance regarding the characteristics of the events that might be chosen for an ATHEANA analysis. In general, the event chosen should have a scenario with one or more post-initiator human failures that if not corrected could have resulted in a plant functional failure with the potential to lead to core damage. The plant functional failure may have been previously modeled in the PRA as an HFE or it may not have been. The purpose of the retrospective analysis may be to update the PRA or the HRA database, or to respond to the event with corrective action, or both.

For a prospective analysis, the purpose of ATHEANA is to support the analysis of post-initiator HFEs. This is because in the event histories examined during the development of ATHEANA, it was the post-initiator HFEs that represented plant functional failures with the potential to lead to core damage. In ATHEANA, pre-initiator or initiator human actions become significant only when they create dependencies that can interfere with successful post-initiator actions. Such pre-initiator or initiator human actions are found during the identification of error-forcing contexts (EFCs).

7.2 Assemble and Train the Multidisciplinary Team

ATHEANA is applied by a multidisciplinary team, under the leadership of the HRA analyst. It is essential that the ATHEANA team be composed of people with sufficient knowledge and experience

to supply the information and answer the questions involved in the ATHEANA process. As a minimum, the members of an effective team of analysts must have the following expertise:

- familiarity with the issues in behavioral and cognitive science
- understanding of the ATHEANA process
- knowledge of the plant-specific PRA, including knowledge of the event sequence model
- understanding of plant behavior, especially thermal-hydraulic performance
- understanding of the plant's procedures (especially emergency operating procedures) and operational practices
- understanding of operator training and training programs
- knowledge of the plant's operating experience, including trip and incident history, backlog of corrective maintenance work orders, etc.
- knowledge of plant design, including man/machine interface issues inside and outside the control room

Therefore, it is recommended that the analyst team include the following types of technical staff members:

- an HRA analyst
- a PRA analyst (preferably the accident sequence task leader)
- a reactor operations trainer (with expertise in simulator training)
- a senior reactor operator
- a thermal-hydraulics specialist

Other plant experts should supplement the expertise of the analysts as needed, to provide additional plant information required for the ATHEANA process, participate in simulator trials or talk-throughs, and support the collection of information needed for HFE quantification.

The HRA analyst serves as the team leader and is also the principal expert on behavioral and cognitive science, the ATHEANA knowledge base, and the ATHEANA process. In particular, the HRA analyst must perform the following functions:

- Provide interpretation and guidance to the team as needed, in order to ensure that the objectives of ATHEANA, and of the HRA and PRA overall, are met.
- Facilitate the collection of information needed to supplement the experience and expertise of the team.

- Collect or facilitate the collection of information needed to quantify the HFEs identified with ATHEANA.

The HRA analyst also has the responsibility of training other team members on ATHEANA. The following topics should be addressed during team training:

- the character of severe accidents
- the underlying principles and objectives of ATHEANA
- the basic principles of behavioral and cognitive science, as utilized in ATHEANA
- the confirmation of the ATHEANA perspective from the review of operational experience
- the basic approach to event analysis (in the ATHEANA perspective, see Ref. 7.3)
- the ATHEANA process
- any previous demonstrations of ATHEANA

The analyst team should also review at least two operational events and talk through an existing application of ATHEANA. One of the operational events might be one that has occurred at their plant. Another event might be one that has been analyzed and documented in the database that was developed to support ATHEANA [i.e., the Human-System Event Classification Scheme (HSECS) database (Ref. 7.3)], or in other ATHEANA documents, or in Appendix A of this report. The event reviews should help the team become more familiar and comfortable with the ATHEANA terminology (e.g., situation assessment, error-forcing context and its elements) and help them understand and appreciate the ATHEANA perspective. The talk-through of a demonstration serves a similar purpose, but also provides an opportunity for the team to better understand the ATHEANA process.

The products of this step are the identification and training of the team members for the application of ATHEANA at a specific plant. Team training includes not only knowledge of the ATHEANA principles and process but also review and understanding of operational events using the ATHEANA perspective.

7.3 Collect Background Information

This step is performed principally to support the prospective ATHEANA process described in Section 9 (i.e., that used to perform an HRA). However, some benefit may be gained by performing parts of this step in preparation for retrospective ATHEANA analyses (i.e., the event analyses described in Section 8). This step is similar to that which has been traditionally performed in HRAs. Also, similar to traditional HRAs, this step should be performed throughout the ATHEANA process, rather than at a single time.

Just as in traditional HRAs, the HRA analyst should collect plant information that is generally relevant to an HRA (e.g., system design, plant layout, procedures, operations, training, maintenance). In addition, related information relevant to any specific issue that is going to be addressed should be identified and collected. The entire team of analysts should be familiar with this information, in

addition to the existing PRA model, its documentation, and results. To the extent individual analysts are not experts regarding each of these information sources, it may be necessary to identify additional staff to support the team. The purpose of this more traditional collection of HRA background information is to develop a general understanding of the operator's performance environment for the specific plant.

In addition to the more traditional collection of background information, the ATHEANA process requires and incorporates operational experience from both the overall nuclear power industry and the specific plant. Initially, this additional information provides "feed material" for the creative thought process involved in later ATHEANA steps. In particular, examples of unsafe actions (UAs) and challenging contexts from anecdotal experience will serve as templates for either similar or generalized UAs and associated EFCs that must be identified in the ATHEANA process.

Also, the information-collecting activity provides a vehicle for identifying, recording, and incorporating into the HRA any operational or performance concerns that plant personnel (especially operators, trainers, and operations staff) may have that often cannot be accommodated by previous HRA/PRA methods. For example, a common concern among operators is the ability to successfully respond to certain support system failures (e.g., loss of instrument air initiators) that cause degraded conditions and loss of indicators and/or may involve difficult and lengthy equipment restoration activities. Later in the ATHEANA process, detailed, plant-specific operational information is required to support the identification of UAs and EFCs. Such information may include the following examples:

- temporary procedures or operating practices used when the plant status or configuration is different than normal (due to, for example, equipment or indicator unavailabilities, including configurations requiring NRC waivers from limiting conditions for operation (LCOs)

- equipment or indicators with either a recent or long history of degraded or failed performance or condition

- operators' formal or informal priorities regarding which indicators to rely on (and why)

- instances of multiple failures, especially due to dependencies (both human and equipment)

- plant-unique initiators (considered in more detail than the PRA initiator categories) that have or can cause significant operational burdens and difficulties (e.g., the biannual, twice-a-day grass intrusions in the Salem 1 circulating water intake structure; see Augmented Inspection Team (AIT) Report Nos. 50-272/94-80 and 50-311/94-80 [Ref. 7.4])

While the detailed information that will be required cannot be entirely anticipated (and therefore can be collected as needed), it is important that the team include plant personnel who have general knowledge of past and current plant-specific hardware and operator performance. During performance of the ATHEANA process, such personnel can help, during team discussions, to identify likely or credible problems that can be later expanded and verified by more thorough

information collection (perhaps through the assistance of supporting plant personnel). It also may be beneficial for the analysts (led by "experts" on the team) to perform a general review of past and current plant-specific operational issues and concerns that have affected or could affect hardware (including indicators) and/or operator performance.

The ATHEANA team leader or HRA analyst is ultimately responsible for collecting the background information needed and circulating it among the analyst team for review before the analysis begins. This is done in order to assist the team in becoming familiar with important human performance contributions and contextual factors in past accidents and serious precursor events and potential plant-specific vulnerabilities that could produce challenging situations for operators.

This step yields the following products:

- reference lists for background information
- lists of source information expected to be used later in ATHEANA
- contact lists of plant personnel who have or are expected to support the analyst team with relevant plant-specific knowledge (including personnel involved in planned simulator exercises)
- notes regarding potential unsafe actions and challenging or error-forcing contexts that should be considered in later ATHEANA steps

7.3.1 Review and Collection of Anecdotal Experience

The review and collection of relevant anecdotal experience should include both plant-specific and industry wide experience. Plant-specific information may be derived from the following sources:

- site incident or trip reports
- plant documentation supporting licensee event reports (LERs)
- results of simulator exercises (including debriefing interviews of operators and trainers)
- systematic assessment licensee performance (SALP) reports
- interviews of knowledgeable plant personnel (especially those in training and operations)

Eventually, it is anticipated that a link will be created between a computerized version of the ATHEANA application guidance and an industry wide experience base. ATHEANA users will access these combined functionalities which will be updated periodically with new information. However, at present only this report provides ATHEANA guidance and the experience base is not completely developed. Information used to develop this experience base may be derived from the following sources:

- event-based reports [e.g., NRC augmented inspection team reports, NUREGs, Office for Analysis and Evaluation of Operational Data (AEOD) human performance reports; Institute

of Nuclear Power Operations (INPO) reports]

- selected full-text LERs
- NRC and industry information bulletins
- NRC Accident Sequence Precursor Program reports
- Human-System Event Classification Scheme (HSECS) database developed to support ATHEANA (Ref. 7.3).

Until the experience base that will support ATHEANA is available, users should refer to the following sources:

- event information in the ATHEANA knowledge base, Part 1, Section 5
- events summarized in Appendix A of this report

In addition, the following references can support the user's effort:

- Cooper, S.E., W.J. Luckas, Jr., and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report L-2415/95-1, Brookhaven National Laboratory, December 21, 1995.

  This report describes the database structure used to analyze operational events in support of ATHEANA. It also provides a thorough analysis of three PWR full-power events, under the database structure.

- Barriere, M., W. Luckas, D. Whitehead, A. Ramey-Smith, D. Bley, M. Donovan, W. Brown, J. Forester, S. Cooper, P. Haas, J. Wreathall, and G. Parry, *An Analysis of Operational Experience During Low-Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues*, NUREG/CR-6093, BNL-NUREG-52388, Brookhaven National Laboratory, SAND93-1804, Sandia National Laboratories, June 1994.

  Appendix B provides the results of the analysis of a number of PWR shutdown events under an earlier database structure. It also provides summary statistics on relevant aspects of these events. Although the events occurred during shutdown, the multidisciplinary factors affecting human performance are relevant to full-power HFEs.

- Barriere, M.T., J. Wreathall, S.E. Cooper, D.C. Bley, W.J. Luckas, and A. Ramey-Smith, *Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies*, NUREG/CR-6265, BNL-NUREG-52431, Brookhaven National Laboratory, August 1995.

While primarily theoretical, this report presents analyses of a number of real events to illustrate principles. Chapters 3, 4 and 5, as well as Appendices A, B, and C present aspects of specific events and summary statistics from event reviews.

- S.E. Cooper, A.M. Ramey-Smith, J. Wreathall, G.W. Parry, D.C. Bley, W.J. Luckas, J.H. Taylor, and M.T. Barriere, *A Technique for Human Error Analysis (ATHEANA)*, NUREG/CR-6350, BNL-NUREG-52467, Brookhaven National Laboratory, May 1996.

  Section 5.3, *Understanding [the causes of unsafe actions] Derived from Analyses of Operational Events*, summarizes key aspects of five actual events that are used to illustrate unsafe actions and important error-forcing context elements.

- NRC AEOD, *Engineering Evaluation: Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features*, AEOD/E95-01, Washington, D.C., July 1995.

  This report identifies 14 events in 41 months in which operators inappropriately bypassed engineered safety features (ESFs). Summaries of some of these events (which somewhat overlap with events analyzed in other sources) are provided. AEOD concludes that the number of events found indicates a potentially persistent problem that has not yet been addressed. Most of the inappropriate bypasses would be considered errors of commission by ATHEANA.

- J.V. Kauffman, G.F. Lanik, R.A. Spence, and E.A. Trager, *Operating Experience Feedback Report–Human Performance in Operating Events*, U.S. Nuclear Regulatory Commission, NUREG-1275, Vol. 8, Washington, DC, December 1992.

  A report of sixteen onsite multidisciplinary studies of human performance (1990–1992) following accident scenarios (e.g., stuck open safety-relief valve, positive reactivity insertion, and partial loss of instrument air).

- Roth, E.M., R.J. Mumaw, and P.M. Lewis, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, NUREG/CR-6208, Westinghouse Science and Technology Center, Pittsburgh, PA, July 1994.

  This report differs from the others. Rather than reporting on actual plant events, it gives the results of a set of experiments performed to understand and document the role of higher-level cognitive activities (e.g., diagnosis, situation assessment, and response planning) in cognitively demanding emergencies, even when the use of highly prescriptive emergency operating

procedures is required. The experiments were performed using training simulators at two plants. Up to 11 crews from each plant participated in each of two simulated emergencies, for a total of 38 cases. The emergencies included an interfacing system loss-of-coolant scenario and a loss-of-heat sink scenario. In each of the scenarios, operators needed to use higher-level cognitive activities to control situations not fully addressed by the procedures. About 10% of the crews never formed the correct situation assessment. The authors point out that "if higher-level cognitive activities must play a role in difficult scenarios, there are important implications for the kinds of training, procedures, displays, and decision aids that need to be provided to control room operators...as well as for human reliability analysis."

- NRC detailed reports on events involving significant human performance problems published as a result of site visits and interviews immediately following the events [e.g., augmented inspection team reports, integrated inspection team (IIT) reports, and AEOD human performance reports].

  These detailed reports are described in NUREG/CR-6265 (Ref. 7.4), because they are rich sources of information that helped establish the multidisciplinary framework used by ATHEANA and helped in developing the guidance in the current report. A sampling of these reports that were particularly useful is given below.

  - U.S. Nuclear Regulatory Commission AEOD Human Factors Team Report - Catawba, Unit 1 - March 20, 1990, "On-Site Analysis of the Human Factors of an Event," May 1990.
  - U.S. Nuclear Regulatory Commission, AEOD Human Factors Team Report Braidwood, Unit 1 - October 4, 1990, "On-Site Investigation and Analysis of the Human Factors of an Event," October 1990.
  - U.S. Nuclear Regulatory Commission, AEOD Human Factors Team Report-Oconee, Unit 3 - March 9, 1991, "On-Site Analysis of the Human Factors of an Event (Loss of Shutdown Cooling)," May 1991.
  - U.S. Nuclear Regulatory Commission, AEOD Human Factors Team Report - Crystal River, Unit 3 - December 8, 1991, "On-Site Analysis of the Human Factors of an Event (Pressurizer Spray Valve Failure)," January 1992.
  - U.S. Nuclear Regulatory Commission, AEOD Human Factors Team Report - Prairie Island, Unit 2 - February 20, 1992, "On-Site Analysis of the Human Factors of an Event (Loss of shutdown cooling)," March 1992.
  - U.S. Nuclear Regulatory Commission, AEOD Special Evaluation Report, "Review of Operating Events Occurring During Hot and Cold Shutdown and Refueling," December 4, 1990.
  - U.S. Nuclear Regulatory Commission, Generic Letter No. 88-17, "Loss of Decay Heat Removal," October 1988.

- U.S. Nuclear Regulatory Commission, Inspection Report No. 50-306/92-005, Prairie Island, Unit 2, "Loss of RHR (February 20, 1992)," Augmented Inspection Team Report, March 17, 1992.
- U.S. Nuclear Regulatory Commission, Inspection Report No. 50-275/91-009, Diablo Canyon, Unit 1, "Loss of Off-Site Power (March 7, 1991)," Augmented Inspection Team Report, April 17, 1991.
- U.S. Nuclear Regulatory Commission, Inspection Report No. 50-287/91-008, Oconee, Unit 3, "Loss of RHR (March 9, 1991)," Augmented Inspection Team Report, April 10, 1991.
- U.S. Nuclear Regulatory Commission, Inspection Report No. 50-456/89-006, Braidwood, Unit 1, "Loss of RCS Inventory via RHR Relief Valve (December 1, 1989)," Augmented Inspection Team Report, Dec. 29, 1989.
- U.S. Nuclear Regulatory Commission, NUREG-1269, "Loss of Residual Heat Removal System," (Diablo Canyon, Unit 2, April 10, 1987), June 1987.
- U.S. Nuclear Regulatory Commission, NUREG-1410, "Loss of Vital AC Power and the Residual Heat Removal System During Midloop Operation at Vogtle Unit 1 on March 20, 1990," June 1990.

The focus of reviewing and collecting anecdotal experience should be on those events or incidents that either were or had the potential to be challenging to operators. Because the U.S. nuclear power industry has experienced only one at-power, serious accident (i.e., that at TMI-2), all of these events or incidents will be accident precursors. Consequently, the analyst team should not only examine the unsafe actions and contextual elements of these precursors events and incidents but also should postulate what additional complicating factors may be needed to create an error-forcing context and cause an associated unsafe action at their specific plant. In addition, ATHEANA users should recognize that an HFE defined through ATHEANA will consist of at least two unsafe actions: an initial unsafe act and a failure to recover. Each of these actions will have an error-forcing context (although there may be overlap or dependencies between these two EFCs).

Three types of EFCs can be differentiated by their effect on operator performance:

(1) cognitively demanding situations
(2) executionally problematic situations
(3) situations that are both cognitively demanding and executionally problematic

The description of the first type of EFC mimics the terminology used by Roth et al. in NUREG/CR-6208 (Ref. 7.5). In this type of EFC a situation is created in which the operators' thinking becomes faulty, leading to failures in situation assessment and/or response planning. EFCs that cause both of these failures are considered together because these types of failures are often coupled. As discussed in Part 1 and illustrated by the events discussed in the sources recommended, cognitively demanding situations can result from the following EFCs, among others:

- instrumentation and/or indicator problems (e.g., combinations of previously undiscovered failures, historically unreliable indicators, unavailable indicators)

- multiple hardware failures, especially in combination with instrumentation and/or indicator failures

- accident sequences that differ dramatically from "nominal" in the timing of plant behavior, the order of expected plant responses, and the availability and reliability of equipment

- unusual initiators or accident progressions, especially those similar to more familiar or recently occurring accident sequences

- unexpected or unrecognized interactions among hardware, especially for complicated systems or plant design features less well understood by operators, such as instrumentation and controls (I&C)

- dependencies among hardware failures, operator actions, and/or management and organizational factors (including those that cross temporal phases such as dependencies between pre-existing failures or initiating events and post-initiator operator actions)

- spurious or false information, indications, or activations that divert operator attention

The second type of EFC creates situations in which, while the operators' thinking is correct, plant behavior, design, and/or configuration hinder operators from successfully performing their chosen mitigative measures (i.e., execution failures). EFC elements that can create executionally problematic situations include the following examples:

- multiple hardware failures or unavailabilities (including pre-existing failures)

- unusual plant configurations

- plant design features (e.g., interlocks) that are difficult or time-consuming to recover if unintentionally triggered, disabled, etc.

- less than the usual amount of time to perform needed actions (owing to an unusual accident initiator or progression)

- execution requires communication among different locations and multiple operators, consists of many steps; or there are other workload, coordination, or communication burdens

The third type of EFC is, of course, a combination of the first two types.

7.3.2 Additional Plant-Specific Information Needed for ATHEANA

As stated earlier, it is difficult to anticipate the additional plant-specific information that will be needed before the unsafe action and EFC search steps in the ATHEANA process. However, in order to assist in the initial identification of potentially challenging situations for operators, it would

be helpful to identify the following types of plant-specific information:

- equipment with historical or recent problems (e.g., frequent failures, degraded performance, unavailability)
- instrumentation or indicators with historical or recent problems (e.g., frequent failures, miscalibrations or drift, degraded performance, unavailability)
- plant-unique initiators
- uniquely high or low frequencies of specific initiators
- recent history of specific initiators and common accident dynamics and/or progressions,
- plant-unique design features that are potentially troublesome
- "informal rules," developed from operational experience, training, and good practice, that can override or supersede formal rules contained in plant procedures
- operational practices or preferences not obvious from the review of procedures (e.g., preferential use of a particular indicator owing to its perceived historical reliability)

It is admittedly difficult to state what plant-specific sources will be most helpful in providing the above types of information. However, team members who represent training and operations are expected to identify the last two types of information from their knowledge and experience. Operators, trainers, and other operations personnel should also be interviewed.

A variety of possible sources may address the first four information types, including the knowledge and experience of team members; maintenance work records; trip history; plant-specific incident reports; and interviews of maintenance and testing personnel, systems engineers, and field and control room operators.

7.3.3 Other Information Needed Later in ATHEANA

During the course of applying ATHEANA, the need for other information and information sources may surface. However, to the extent possible, the resources needed (both staff support and information) should be identified early in the process. Plant resources that may be needed later include the following:

- consultation with training staff, individually and, perhaps, in groups (in addition to the expertise provided by team member(s) who represent the operator training department)
- simulator exercises and associated debriefing interviews of operators and trainers (see Section 7.4)

As noted earlier, the training staff can assist the analysts in identifying and understanding past or potential situations that have negative impacts on operator performance.

7.4 Prepare to Conduct Simulator Exercises

Simulator exercises and interviews with operators can be used to support the ATHEANA processes associated with identifying unsafe actions, tenable error mechanisms, and EFCs. To the extent that accidents being examined in a retrospective analysis can be simulated, it may possible to get additional insights about why unsafe actions occurred during the event. In general, however, the use of simulators as described below is related to performing a prospective analysis and the analyst team should make arrangements to use the plant simulator to support this process.

The particular roles fulfilled by use of simulator exercises in ATHEANA are as follows:

- a focused opportunity to discuss with teams of operators and other training staff the important characteristics of the context used in the exercise
- an opportunity to observe the styles of teamwork and problem-solving and general operating strategies for operating crews
- an ability to test the extent to which the context appears to be "error-forcing," either as modeled in the exercise or with additional elements as discussed with the operators and trainers
- an opportunity to evaluate the potential failure probability of the crew in the context of the event as modeled

Each of these roles is further discussed below.

As well as the inputs provided by operations trainers during the brain-storming of the ATHEANA process, the walk-through of scenarios in a simulator setting can provide an excellent opportunity to obtain inputs from personnel who are extremely familiar with the plant systems. The simulator can be stopped at key points in the scenario and the operators asked about what they believe is happening and what they expect to see next. They can be asked questions about what effect different kinds of information displays may have, why some information may be discarded, and why they may chose to deviate from a procedure or plant practice. Such discussions can also be held in a post-simulation debriefing with the operators. In either case they can provide insights into how the operators' collective situation assessment and decision-making processes work in the context of the scenario. These insights can be used to identify stronger and more likely EFCs and to provide information about additional ways in which the failures of concern could occur.

It is recognized in the ATHEANA process that the styles of working as a group and problem-solving can vary among crews and among different plants. For example, some facilities place more

emphasis on strict compliance with each step of the early emergency procedures. Such compliance has the considerable merit of systematically addressing each potential problem in turn. However, in highly dynamic events, it also has the potential for delaying responses or for some of the early dynamic characteristics to be overlooked. Therefore, for a plant that follows such a policy, a fast-paced event or an event with complex early dynamics is likely to be possibly more "error forcing." However, for a plant where such strict adherence is not emphasized so much, events that may lead operators to depart from the early procedures are perhaps more error forcing. By observing a crew's performance in the simulator, it is possible to view the style of the crew and decide how a particular scenario might be more error forcing because of the style.

The simulator exercises can be used to test the extent to which the context appears to be "error forcing," either as modeled in the exercise or with additional elements obtained from operators and trainers during the debriefing. By observing how crews transition through the decision-making points in the scenario, it is possible to detect from the discussions typically taking place among crew members where possible points of failure exist. For example, a crew in a simulator may exhibit successful problem-solving at a critical point in a scenario that relies on a unique experience or some highly specialized knowledge (for example, how a particular sensor works). In such cases, it may be judged that other crews without this knowledge may find such a scenario highly problematic, and thus the scenario may be considered error-forcing for most crews.

Given the limitations of generalizing the results of simulator exercises to actual accident conditions, it is suggested that simulators not be used as a direct source for data to quantify the likelihood of failures for a given context. However, the simulator can provide an opportunity to gain insight about the potential failure probability of the crew. In other words, the behavior of the crew and the extent to which they find the context to be problematic can provide qualitative information to help judge the likelihood of errors. For instance, if during an event the crew found no hesitation in taking a UA and the event was accurately simulated within the limits of training simulator technology, this provides empirical evidence to support selection of a comparatively high failure probability. Perhaps more important are the reflections of the crew on the scenario following the exercise. Their view on the difficulty of the scenario, the significance of the context, and possible changes in context that would have made the situation even more error forcing can be invaluable. Such changes in context could include different philosophies of operation and training that exist at other plants, used to exist at their own plant, or are being contemplated.

In conclusion, under the right conditions the use of the simulator allows the analysts to confirm the tendencies predicted in analysis and uncover unforeseen conditions that may alter their conclusions. It also provides some degree of validation that the combinations of plant conditions and PSFs (i.e., the predicted EFCs) are indeed challenging to operators and are likely to result in the predicted HFEs. The tenability of potential error mechanisms, such as operator biases, may be inferred from observing the exercises, and ideas can be obtained for how the EFCs might be altered to provide an even greater tendency to perform the undesired human actions.

In addition, post-simulation discussions with the operators can be used to gain insights about the operators' perceptions, expectations, and thought processes (even when they are successful in

responding to the specific simulated scenario) and may provide guidance for identifying stronger and more realistic EFCs. In particular, when trying to determine whether certain error mechanisms contributed to an operator's responses, strategically asked questions may allow such inferences to be made. Finally, it should also be recognized that the actual responses of the crews during simulations and the accompanying discussions would be very relevant to the quantification of the potential HFEs, given the EFCs.

7.5 Conclusion

Once the above activities are completed or prepared for in the case of simulator exercises, analysts can proceed to either Section 8 for guidance on performing a retrospective analysis or to Section 9 for guidance on performing the ATHEANA prospective analysis. However, before beginning a prospective analysis, it is highly recommended that some experience in performing retrospective analyses be obtained in order to get a better understanding of the ATHEANA perspective and general approach.

7.6 References

7.1 U.S. Nuclear Regulatory Commission, *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance*, Volumes 1, 2, and 3, Division of Systems Technology - Office of Nuclear Regulatory Research, NUREG-1560, Washington, D.C., October 1997.

7.2 U.S. Nuclear Regulatory Commission, *The Use of PRA in Risk-Informed Applications*, Division of Systems Technology - Office of Nuclear Regulatory Research, NUREG-1602, Washington, D.C., June 1997.

7.3 S. Cooper, A. Ramey-Smith, W. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, Brookhaven National Laboratory, Technical Report L-2415/95-1, December, 21, 1995.

7.4 AIT Report, Salem Unit 1, April, 7, 1994, *Loss of Condenser Vacuum (and Loss of Pressure Control - RCS Filled Solid)*, Report Nos. 50-272/94-80 and 50-311/94-80, U.S. Nuclear Regulatory Commission, 1994.

7.5 E.M. Roth, R.J. Mumaw, and P.M. Lewis, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, Westinghouse Science and Technology Center, NUREG/CR-6208, Pittsburgh, PA, July 1994.

8 RETROSPECTIVE ANALYSIS

This section provides guidance for applying ATHEANA in a retrospective analysis of actual plant events. The results of the analysis may be formatted to expand the human event database for future HRA use or as the basis for understanding the factors affecting human performance and proposing corrective actions to reduce the likelihood of similar events in the future.

8.1 Overview

The retrospective application of ATHEANA to analyzing actual plant events provides analysts with a tool for augmenting the HRA database for future use in PRAs and for identifying key corrective actions to diminish the likelihood of similar events occurring in the future. The use of ATHEANA for a retrospective analysis is a departure from other methods of analyzing plant incidents because ATHEANA is designed to identify human failure events (HFEs) as modeled in PRAs[1] and their underlying causes.

ATHEANA postulates that unsafe human actions occur within an error-forcing context that can be specifically identified. The PRA must be able to identify these error forcing contexts in order to estimate how likely these conditions are and the likely consequences in terms of inappropriate human actions or inactions. The error forcing contexts are the conditions that plant management and staff can influence. Identifying the contexts will help them control the conditions that lead to unsafe acts (UAs). The ATHEANA retrospective analysis provides a detailed sketch of the error forcing contexts.

The process is iterative and subjective, relying on contemporaneous records of the event as well as subjective recall of the events and its causes. The analysts will find that they may retrace the same information many times before obtaining a cogent and logical description of the event and the human contribution to the failures that occurred during the event.

The elements of the retrospective analysis are similar to the prospective analysis (see Section 9), but the starting place is quite different. Whereas the prospective analysis works from the defined functional failures in the PRA to identify functional failure modes that could be caused by rational human behavior, the retrospective analysis begins with the actual scenario to identify the functional failures that were caused by human behavior. The prospective analysis postulates error-forcing contexts using a rule-based search process, while the retrospective analysis sifts through the event data to uncover the error forcing-contexts.

The following steps comprise the retrospective analysis process:

---

[1] As discussed in Section 1, we must think of a PRA as a general approach for framing, analyzing, and understanding risk and safety, rather than a particular set of tools such as the event tree/fault tree analysis common in the nuclear power industry. By a PRA, we mean examining risk through a process of successive approximations, beginning with a structuring of possible scenarios that could lead to damage and continuing, first with a judgment-based evaluation of the risk, and then with successively more rigorous calculations as dictated by the seriousness of the situation, practice in the associated industry, and available resources. This broad view of a PRA is not new to ATHEANA [see, for example (Ref. 8.1 and Ref. 8.2)].

(1) Identify the undesired event. The act of clearly identifying the undesired event provides a defined scope for the analysis.

(2) Identify the functional failures, the HFEs, and the UAs.

(3) Identify the causes of the UAs, including plant conditions and performance shaping factors (PSFs)

(4) Document the results.

The desired result of the retrospective analysis can be summarized in a flow chart. An example of results from an ATHEANA retrospective analysis is shown in Figure 8.1. The information presented in the Appendix A retrospective analysis A.1 is summarized in the ATHEANA framework in this flowchart. The analysis is performed largely in the reverse direction of the flow, i.e., the HFEs and UAs are identified before the information-processing failure, PSFs, and contributing plant conditions. The representation in Figure 8.1 demonstrates the ATHEANA principle that HFEs are heavily dependent upon plant conditions and PSFs.

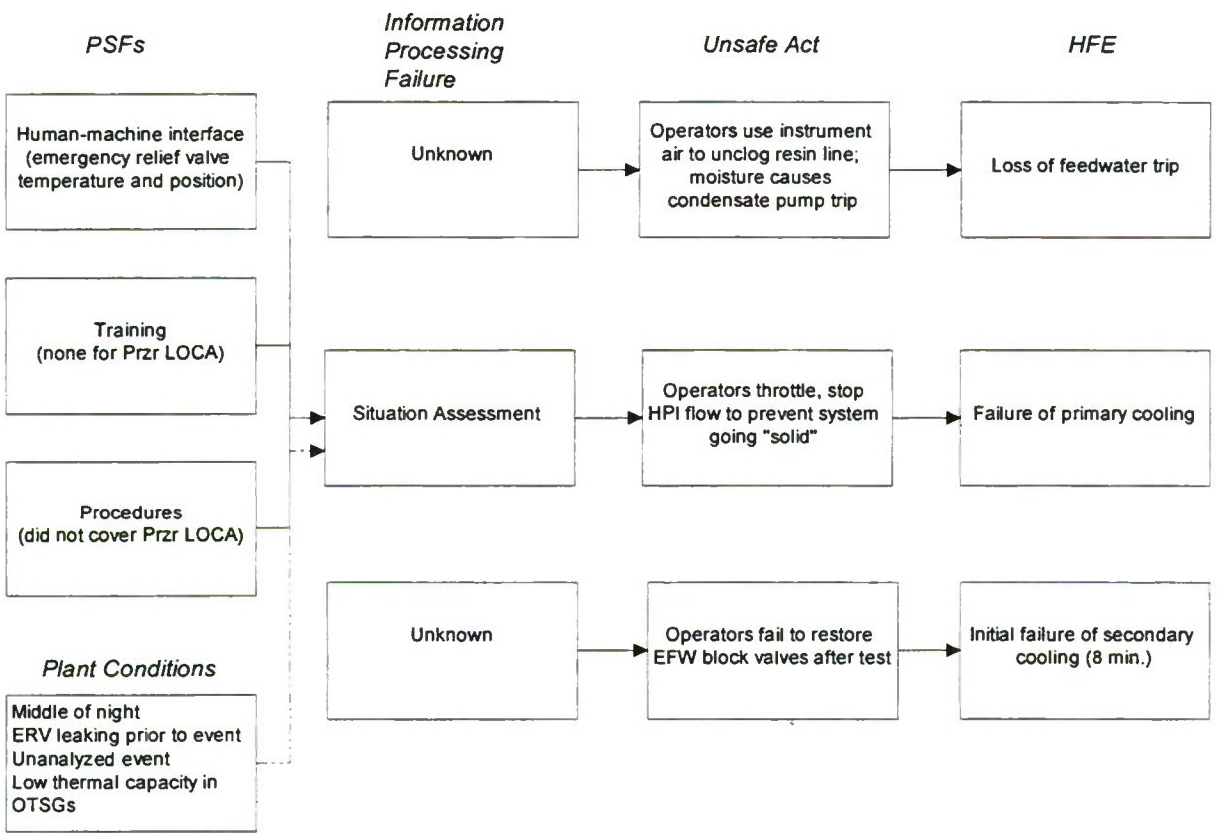


Figure 8.1 TMI-2 Represented in ATHEANA Framework

8.2 Identify and Describe the Undesired Event

The plant event defines the scope of the analysis. Undesired events will typically have the following characteristics:

- severe or potentially severe consequences
- operation outside the boundaries of good operation
- extensive operator control of the plant

The analysts must fully describe the scenario of the event. Any of the event summaries used for the retrospective analyses in Appendix A may be used as an example for this step. This is not a trivial undertaking inasmuch as the background information gathered as described in Section 7 may provide incomplete or conflicting information about the event.

The analysts next list the initial plant conditions and the resultant accident conditions just prior to recovery. These are the key plant parameters that must be controlled for safe operation. Suggested parameters to be included are:

Initial conditions:

- primary or reactor system parameters (power level, system temperature, pressure, water level, chemistry, etc.)
- evolution and activities
- configuration
- preexisting operational problems
- initiator

Accident conditions:

- primary system parameters
- automatic responses
- failures
- human-system interactions
- defeated defenses

To provide further insight as to the unique aspects of the event, it is recommended that the analysts identify the surprises during the event from the analysts' perspective; these are plant or human responses that seem surprising, given the situation. They could be plant response to certain actions, robustness of the plant, speed of response, unexpected operator response, etc.

8.3 Identify the Functional Failures, the HFEs, and the UAs

The analysts next identify the functional failures that occurred during the undesired event. Functional failures are modeled in the PRA and can be function, system, or component failures. Functional failures can occur for many reasons and may be stated generally. Section 9 of this report

provides guidelines for identifying functional failures. The retrospective analysis examples in Appendix A do not specifically identify the functional failures, but it is recommended that the analysts do so to facilitate the identification of the human failure events and uncover the UAs that caused the HFE. For instance, in the Crystal River Unit 3 spray valve failure event, Section A.2, the functional failure is failure of RCS pressure control.

An HFE is a functional failure that is the result of one or more unsafe human actions. UAs are actions inappropriately taken by plant personnel or actions not taken when needed that result in a degraded plant safety condition. The term "unsafe act" does not imply that the human was the cause of the problem. Indeed, the analysis of operational events avoids inference of blame by looking for the circumstances and conditions that set up people to take actions that are unsafe.

Each HFE has associated UAs that define the specific ways in which plant, system, or equipment functions are failed by human actions or inactions. The analysts will examine the information gathered prior to the analysis to understand the human actions taken that lead to the potential HFE. For example, UAs could be:

- turning off running equipment
- bypassing signals for automatically starting equipment
- changing the plant configuration so it defeats interlocks that are designed to prevent damage to equipment
- excessive depletion or diversion of plant resources (e.g., water sources)

If a PRA-related functional failure has occurred that was not previously modeled as an HFE, the event provides an incentive to revise the existing PRA. If no PRA-related functional failure has occurred, the event is not directly risk significant. Nevertheless, its information on the cause of failures in human performance may be useful.

The analysts begin the identification of the functional failures and UAs by constructing an event diagnosis log. The event diagnosis log lists in chronological order the plant conditions and operator actions from the initiation of the event until the recovery and stabilization of the plant at the end of the event. Much of the information gathered prior to the analysis will be brought together to construct this log. The analysts should spend the requisite effort in creating a complete fact-driven diagnosis log, continuing with information gathering until anomalies and gaps in the chronology are filled. The log is the most useful deductive piece of the analysis and will be referred to frequently by the analysts to postulate the causes of the UAs. Examples of the event diagnosis log are provided in Appendix A.

The diagnosis log will provide the information to isolate the plant functional failures, the HFEs, and the UAs that caused the HFE. To isolate these ATHEANA elements, the analysts label key actions and equipment failures in the diagnosis log as follows:

- unsafe acts (U): actions that lead to the HFE
- nonerror, nonrecovery actions (H): normal actions taken by plant staff that neither lead to plant recovery nor contribute to the HFE
- recovery actions (R): actions taken by plant staff to mitigate the event and put the plant in a safe or stable condition
- equipment failures (E): equipment that failed to operate when automatically or manually initiated or equipment that operated incorrectly

Each operator action and equipment failure that appears to contribute to exacerbating or mitigating the consequences of the identified undesired event should be listed in a table and graphically depicted in a chronological relationship of the actions and failures of the event. This relationship is displayed for the events analyzed in Appendix A. Thus, as illustrated in the appendix, the key contributions to the event's outcome are presented on the event timeline, identified in a UAs and other events table, and in the diagnosis log. The analysis of undesired events to this point will usually require iteration. Dependencies among the actions and events are identified in the human dependencies table. Dependent actions and events have a strong influence on error-forcing context (Ref. 8.3).

Figure 8.1 of the TMI retrospective analysis provides one example of the relationship between the HFE and the UAs. A similar presentation constructed for the Crystal River Unit 3 spray valve failure event is shown in Figure 8.2.

8.4 Identify the Causes of the UAs

The key analysis for the ATHEANA process is determining the causes of the UAs by identifying information-processing failures and the error-forcing context composed of the PSFs and significant contributing plant conditions.

8.4.1 Information Processing Failures

The analysts will not be able to precisely determine what the operators were thinking when they took the UAs. When reasonable, the analysts will postulate what caused the operator to take the UA(s) based on the surrounding conditions, statements of the operators, etc. The psychological discussion in Section 4 of this report may be helpful to the analysts in postulating the causes. More often, only the failures in information processing, evidenced by the operators' behavior, can be assessed. The typical ones are listed below:

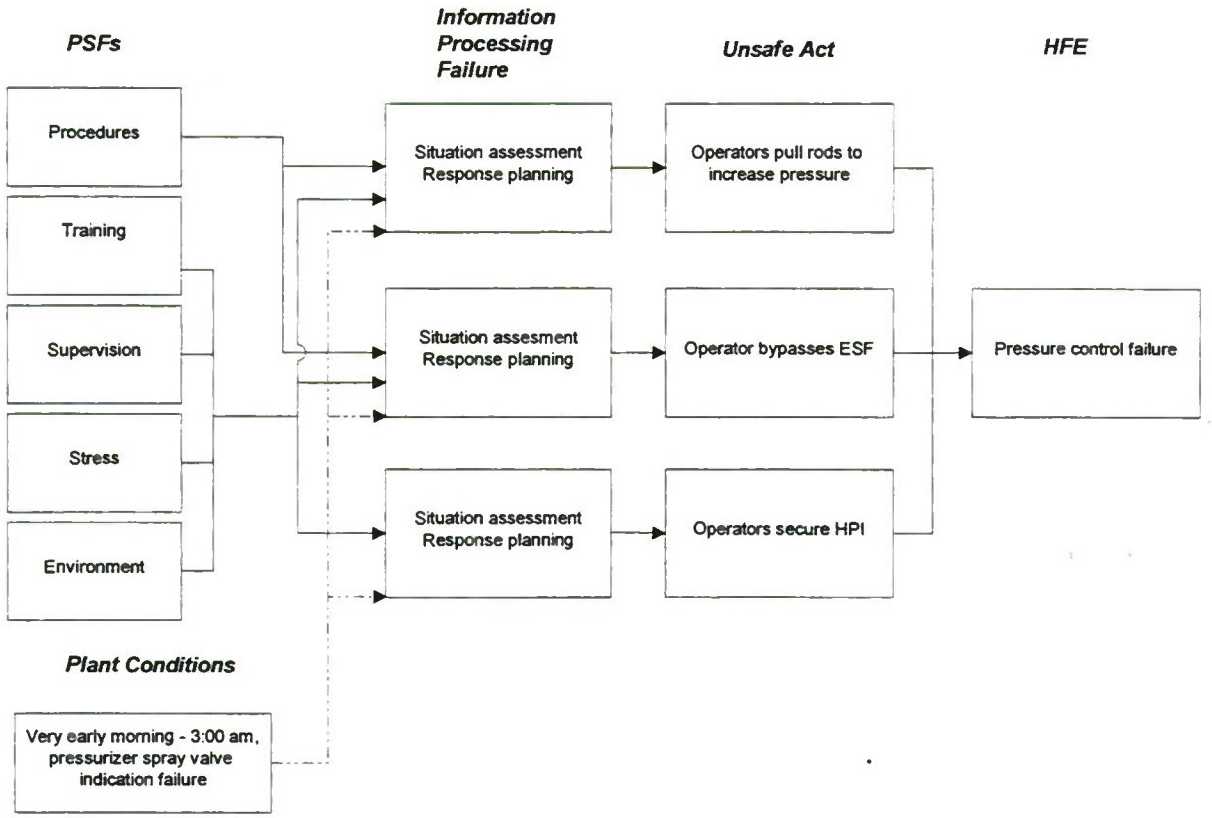


Figure 8.2 Crystal River Unit 1 Represented in ATHEANA Framework

- Monitoring and detection
  - operators unaware of actual plant state
  - operators unaware of the severity of plant conditions
  - operators unaware of continued degradation in plant conditions

- Situation assessment
  - information is erroneous or misleading
  - plant indicators are misinterpreted
  - plant or equipment behavior is misunderstood
  - similarity of the event to other better-known events leads operator to form an incorrect situation model

- Response planning
  - operators select nonapplicable plans
  - operators follow prepared plans that are wrong or incomplete
  - operators do not follow prepared plans
  - prepared plans do not exist, so operators rely upon knowledge-based behavior
  - operators inappropriately give priority to one plant function over another

- Response implementation
  - important procedural steps are missed
  - miscommunication
  - equipment failures hinder operators' ability to respond

Refer to Section 5 for a discussion of these factors applied to the specific events and to Appendix A for completely worked-out examples.

8.4.2 Performance-Shaping Factors

The analysts sift through the event information gathered to identify PSFs that, when combined with plant conditions, might reasonably be expected to cause the error mechanism and a UA. In other words, the analysts look for factors that helped to set up the operator to make an error. Examples of PSFs identified in event analyses include:

- human performance capabilities at a low point
- time constraints
- excessive workload
- unfamiliar plant conditions and/or situation
- inexperience
- nonoptimal use of human resources
- environmental factors and ergonomics

The underlying causes of the PSFs may be such things as training, poor or incomplete procedures, time of day, organizational factors, or poor human–system interfaces. Section 5.2.2 of this report provides background on PSFs. Based on this analysis, it is useful for the analysts to summarize what the most negative influences on the event actions appear to be or are mentioned by participants in the event, as well as the most positive influences on the event. See Appendix A retrospective analyses for examples.

8.4.3 Significant Plant Conditions

As part of the error-forcing context, the analysts should also summarize the most significant plant conditions that differ from expected plant conditions. These would include, for example:

- extreme or unusual conditions
- contributing preexisting conditions
- multiple hardware failures
- transitions in progress

8.5 Drawing Conclusions

The analysts draw together, for each UA, the plant conditions and PSFs that they believe caused the failure of information processing for the unsafe act. It may turn out that there is more than one error mechanism for each UA act as demonstrated in the analyses in Appendix A.

The analysts' evidence of the error-forcing context, the combination of plant conditions and PSFs, is presented so that an independent reviewer can draw the same conclusion regarding the team's assessment of the cause of the UA. The presentations used in the analyses in Appendix A or summarized as in Figures 8.1 and 8.2 are reasonable ways to present the evidence. For each event analyzed, there could be one or more HFEs identified, each with one or more contributing UAs. The representation of the event may be complex. The analysts have the responsibility of making it as clear and straightforward as possible.

8.6 Document the Results of the Analysis

Using the examples in Appendix A and Figures 8.1 and 8.2 as templates, the analysts document their discussions, rationale, and findings.

8.7 References

8.1 Magee, R.S., E.M. Drake, D.C. Bley, G.H. Dyer, V.E. Falter, J.R. Gibson, M.R. Greenberg, C.E. Kolb, D.S. Kosson, W.G. May, A.H. Mushkatel, P.J. Niemiec, G.W. Parshall, W. Tumas, and J. Wu, *Risk Assessment and Management at Deseret Chemical Depot and the Tooele Chemical Agent Disposal Facility*, Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, National Research Council, National Academy Press, Washington, DC, 1997.

8.2 Isselbacher, K.J., A.C. Upton, J.C. Bailar, K.B. Bischoff, K.T. Bogen, J.I. Brauman, D.D. Doniger, J. Doull, A.M. Finkel, C.C. Harris, P.K. Hopke, S.S. Jasanoff, R.O. McClellan, L.E. Moses, D.W. North, C.N. Oren, R.T. Parkin, E.D. Pellizzari, J.V. Fodricks, A.G. Russell, J.N. Seiber, S.N. Spaw, J.D. Spengler, B. Walker, and H. Witschi, *Science and Judgment in Risk Assessment*, Committee on Risk Assessment of Hazardous Air Pollutants, National Research Council, National Academy Press, Washington, DC, 1994.

8.3 M.T. Barriere, W.J. Luckas, J. Wreathall, S.E. Cooper, D.C. Bley, and A.M. Ramey-Smith, *Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies*, NUREG/CR-6265, Brookhaven National Laboratory, Upton, NY, August 1995.

9 DETAILED DESCRIPTION OF PROCESS

9.0 Introduction

This section provides guidance for applying the ATHEANA prospective search process. Figure 9.1 is a flow diagram showing the major steps in the process. Figure 9.1a provides a key to the meaning of different shaped boxes in Figure 9.1 and in the remaining figures in the section. Because the performance of Steps 9 and 10 (i.e., quantification and interpretation of findings) involves management decisions and is very closely tied to the issue being addressed (see Step 1), these steps are discussed in Section 10.

The ATHEANA prospective process is designed to be used for a wide range of applications, from a complete HRA analysis to support a new PRA, to addressing a particular risk-related issue, as discussed in Section 1. Appendices B through E provide examples of ATHEANA applications for the following initiators:

- loss of main feedwater
- loss-of-coolant accident (LOCA)
- small LOCA
- loss of service water

The guidance given in this section should be used in conjunction with the illustrative examples given in these appendices.

9.1 Step 1: Define and Interpret the Issue

The purpose of this first step is to define the objectives of the analysis, i.e., why it is being performed. ATHEANA can support a wide range of HRA applications from complete PRAs to special studies focused on specific issues. In the nuclear power industry, because most plants have already performed a PRA, the issues for which the PRA will be extended using ATHEANA will usually focus on the significance of human contributions to risk and safety that are particular areas of concern to the NRC or plant management. In such applications, the issue to be addressed usually defines a relatively narrow scope of analysis.

ATHEANA may be useful in addressing operator performance concerns in risk-significant situations of many varieties. Since ATHEANA provides both qualitative and quantitative insights, both PRA and non-PRA applications are possible. ATHEANA applications for prospective analysis can, for example:

- provide an HRA to support a new PRA

- assist in the expansion of the original PRA scope to address issues of new concern (e.g., the impact of cable aging)

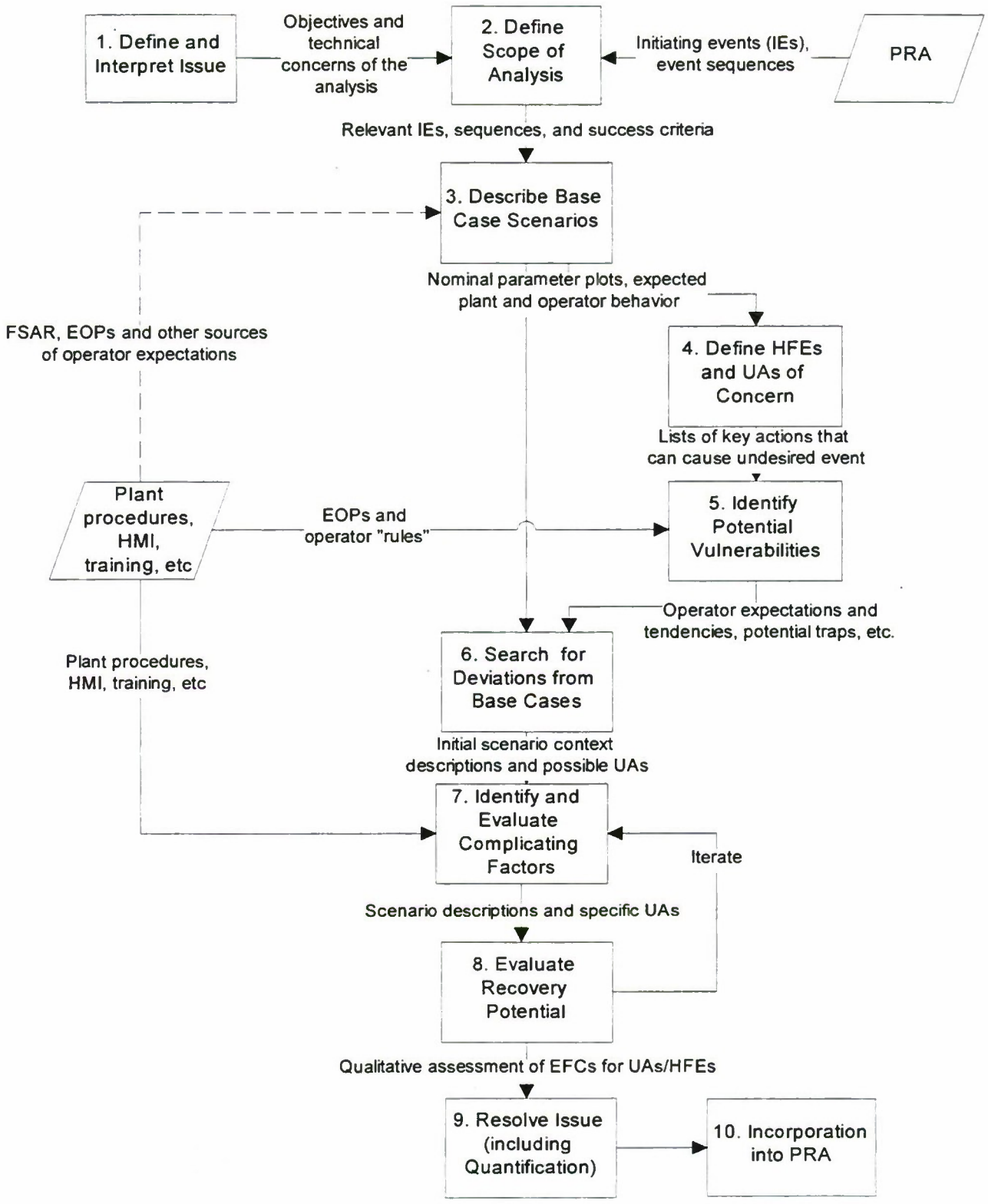


Figure 9.1 ATHEANA Prospective Search Process

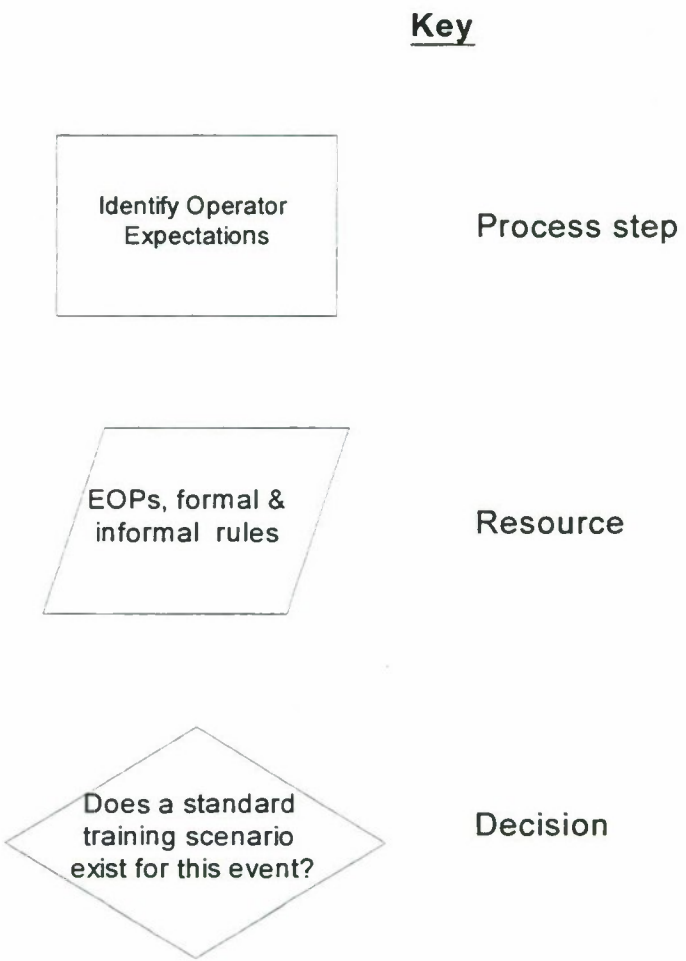


Figure 9.1a Key for the Meaning of the Box Shapes in Figures 9.1- 9.6

- assist in upgrading PRA studies for the purposes of risk-informed regulation (e.g., preparing submittals)
- refine existing PRAs and HRAs (e.g., fire PRAs, low-power and shutdown PRAs, internal events PRAs, especially with respect to errors of commission)

A wide range of such application issues was discussed in Section 1. In addition, Appendices B through E provide illustrative examples of ATHEANA for specific issues. For example, Appendix B investigates potential operator vulnerabilities to inappropriately shutting down AFW pumps in scenarios involving loss or serious degradation of steam generator cooling flow during full-power operation. On the other hand, Appendix C performs a more general investigation of the possible "physics" deviations to a LLOCA that might adversely affect operator response. The four appendices demonstrate that there is a broad range of issues that can be investigated using ATHEANA.

9.1.1 Guidance for Step 1

Sources of Issues. The ATHEANA analysis begins when the analysts are tasked to address specific issues as a result of problems or questions related to the impact of human performance on risk. Sources for the analysis request could include:

- regulators or government officials
- utility management
- utility technical staff, including the PRA/HRA and operating experience groups
- members of the public

Clearly Define the Issue. Questions and issues provided to the ATHEANA analysts for resolution often are phrased in vague or very general terms. To avoid wasted resources and disappointed interest groups, it is essential that the analysts work with the source to reach agreement on a clear, technical statement of the issue in unambiguous terms amenable to analysis.

Interpret the Issue in the Context of a PRA. For the analysis to proceed, the issue should be interpreted in terms of the PRA. This risk-informed interpretation will form the basis for many of the following steps of analysis.

In this risk-informed interpretation, we must think of a PRA as a general approach for framing, analyzing, and understanding risk and safety, rather than a particular set of tools such as the event tree or fault tree analysis common in the nuclear power industry. (References 9.1 and 9.2 provide a discussion of this perspective.) By PRA, we mean examining risk through a process of successive approximations, beginning with a structuring of possible scenarios that could lead to damage and continuing, first with a judgment-based evaluation of the risk, and then with successively more rigorous calculations, as dictated by the seriousness of the situation, practice in the associated industry, and available resources.

9.1.2 Products of Step 1

The output of this step is a succinct description of the issue to be analyzed, indicating, to the extent practicable, the boundaries for the analysis, the overall goal of the analysis, and the relationship of the issue to risk and the PRA, if one is available.

9.2 Step 2: Define the Scope of the Analysis

This step limits the scope of the analysis by applying the issue defined in Step 1 and if necessary for practical reasons, further limits the scope by setting priorities on characteristics of event sequences. Although ATHEANA can be used for both PRA and non-PRA applications, the process for setting priorities is based upon plant-specific PRA models and general concepts of risk significance. The first limitation is to select the initiating event classes and associated initiators to be analyzed. Later restrictions in scope are then considered for each initiator selected, balancing analysis resources against specific project needs.

9.2.1 Guidance for Step 2

The flow of the analysis in this step is sketched in Figure 9.2 and described in the following paragraphs.

Scope Limitations Provided by the Issue. The issue itself usually provides the primary scope limitation. In many cases, the issue limits the scope so narrowly that little or no additional restrictions are necessary to permit a manageable ATHEANA analysis. For example, the illustrative case presented in Appendix C limits the analysis to a single initiator, the large LOCA. In other cases, we may only be interested in:

- certain specific functional failures
- only certain specific human failure events, or
- certain specific unsafe acts

Developing Further Scope Limitations by Setting Priorities. The ATHEANA analysts will decide which initiators, event trees, and human failure events to analyze first. Priorities can be established, either by developing an overall plan or schedule for the analysis, or by determining an analysis scope that represents a significant resolution of the issue and is consistent with currently available resources.

Setting priorities is an iterative process over Steps 2, 3, 4, 6, and 7 and uses information from:

- the PRA (initiators, event trees, plant functions and their associated systems and equipment)
- the emergency operating procedures
- the events or scenarios that concern the plant staff (e.g., operations manager, trainers)

- operational experience
- resources available to perform the analysis

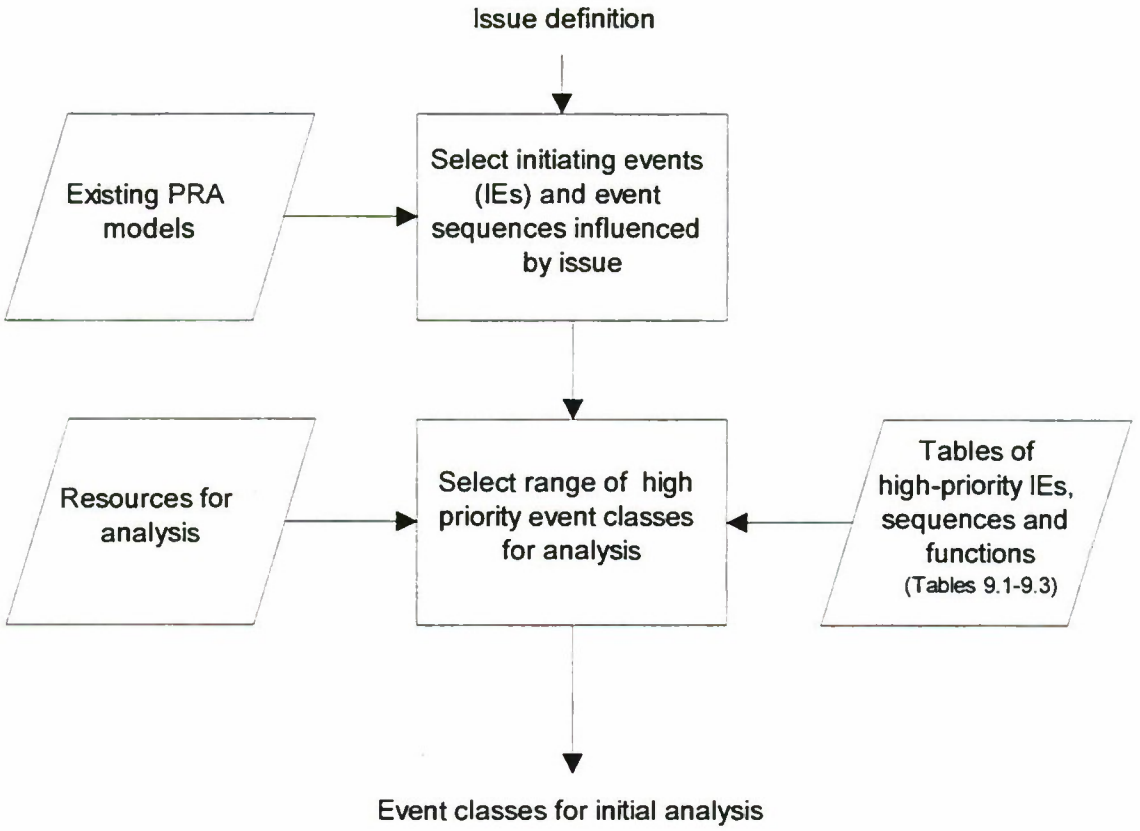


Figure 9.2 Step 2 - Describe the Scope of the Analysis

Because it is always necessary to select the initiating events for analysis, we provide guidance on these events before describing the approach for setting priorities.

Specific Guidance for Selecting the Initiating Event Classes and Relevant Initiators. The issue itself may limit the selection of initiating events. Otherwise, priorities must be developed based on the likely risk significance of the initiating event. It is always necessary to select specific initiating events for analysis. In a nuclear plant PRA, the generally accepted definition of an initiating event is:

> *Any event that perturbs the steady state operation of the plant, if operating, or the steady state operation of the decay heat removal system during shutdown operations, thereby initiating a transient within the plant. (Initiating events trigger sequences of events that challenge plant control and safety systems).*[1]

In this document, classes of initiating events are distinguished from the specific initiator since more than one initiator may trigger a sequence of events that lead to the same initiating event class (e.g., a transient). A generic list of initiating event classes and associated initiators is provided in Table 9.1. Other references for initiator lists include the plant-specific final safety analysis report (FSAR), the plant-specific probabilistic risk assessment (PRA), plant-specific and vendor safety analyses, plant-specific and industry generic event history, and other generic references (e.g., Ref. 9.3).

The ATHEANA process also recognizes two different types of initiating events because of the way they may affect human performance:

- direct initiating events
- indirect initiating events (all of which eventually or immediately lead to one or more direct initiating event, which is the point where steady-state operation is disrupted)

Direct initiating events are those that meet the generally accepted PRA definition given above. The base case scenarios for these initiators are usually straightforward, well documented, and follow a predictable sequence of events. Indications that the event has occurred are reasonably quick, direct, and often easily discernable. Also, they are well supported by emergency procedures and training. The expected and essential associated human actions are generally modeled in the HRA of the PRA.

---

[1]Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, Proposed final draft to be released for public comment, American Society for Mechanical Engineers (ASME) RA-S-1999 Edition Draft #9, January 21, 1999.

Indirect initiating events begin with some *starting event*[2] that causes or starts a sequence of events that lead to a standard initiating event. Sometimes there is substantial delay before steady-state operation is perturbed (i.e., until a standard initiating event occurs). Early indications of these events are often subtle, perhaps misleading, and often it is difficult to determine the extent of the effects of such events. For instance, these events could cause propagating damage to plant equipment before a reactor trip (or other initiator) occurs. These characteristics provide a greater challenge for operators to understand the nature of the event and the resulting plant status. Starting events include many of the support system initiating events (e.g., loss of service water and loss of instrument air) and environmental events (e.g., fires, floods, and earthquakes). By the time a reactor trip actually occurs and the operators enter the EOPs, substantial confusion and conditions causing bias and dependencies may already exist.

In most cases, the issue selected in Step 1 will help determine what initiating event classes and initiators should be selected. For example, if the issue is to analyze the risk from fires, then the analysts should choose the initiators that best represent or are most affected by fire events. It is a typical assumption in PRAs that fires lead to a reactor trip and subsequent loss of feedwater, and in some cases loss of offsite power can be assumed. Unless the ATHEANA analysts can identify other specific initiators because of particular vulnerabilities (for example, support system components), these initiators are a suitable starting point for investigating the risk from fires. If the issue selected does not require or imply which event type(s) should be selected, then the analysts should develop priorities for the initiating event classes.

Table 9.1 Generic List of Initiating Event Classes and Associated Initiators

Initiating Event Class	Example Initiators
Transients (internal) – with and without feedwater available	Loss of offsite power (SBO) Loss of main feedwater Loss of vacuum Turbine trip Reactor trip MSIV closure Loss of circulating water
LOCA	Large Small Medium

[2]Current PRAs are somewhat self-contradictory in using the term "initiating event." They typically define an initiating event as described earlier, then in the initiating event analysis and in the subsequent PRA, they identify starting events (our second class) such as fire and loss of service water as initiating events. Such events clearly fail to meet the definition of initiating event given above: They cause no immediate trip of the turbine and reactor; and they cause no immediate departure from steady-state operation. Because there is no practical significance of this logical inconsistency when plant hardware systems are modeled, the PRA community has largely ignored it. However, the distinction is remarkably significant when modeling human operator response. The two classes of event sequences present very different challenges to the operators.

Table 9.1 Generic List of Initiating Event Classes and Associated Initiators (Cont.)

Initiating Event Class	Example Initiators
Support system failures	Loss of HVAC Loss of service water Loss of instrument air Loss of dc bus Loss of ac bus Loss of instrument bus Loss of component cooling water Loss of reactor building closed cooling water
External events	Fires Seismic disturbance Floods Winds
Other/special	Interfacing systems LOCA Anticipated transient without scram (ATWS) Steam generator tube rupture (SGTR) Feedline break Reactor vessel (RV) failure (e.g., pressurized thermal shock)
Alternative modes	Low power and shutdown

Specific Guidance for Setting Priorities. Priorities for examining different initiators and event trees are used to further restrict the scope of the analysis and focus it on potentially higher-risk events. The existing plant-specific PRA model, including event trees, fault trees, success criteria, initiating events and event frequencies, should be used along with Tables 9.2 and 9.3 to establish plant-specific priorities. The ATHEANA analysts also may find the excerpts from operational experience given in Part 1, Tables 5.6 and 5.7, which together can serve as templates or guidance for defining error-forcing contexts, useful in identifying high-priority initiators and event trees.

Table 9.2 provides a generic list of accident sequence characteristics that have potentially high risk significance from the human perspective. This list is based upon behavioral science principles, operational experience reviews (see, for example, those given in Part 1), and PRA principles. For example, operators can develop expectations regarding the event type (based upon initial accident symptoms) and its likely progression for events that occur relatively frequently (or recently). Operators can develop similar expectations for initiators and accident sequences that have a wide range of possible conditions or trajectories. In addition, the PRA may consider only certain nominal conditions or trajectories out of a broad spectrum. However, if a different event (but with some similar initial symptoms) occurs or if an event follows a significantly different trajectory than expected, then a potentially challenging situation is created for operators that can lead them to take incorrect actions.

Challenging situations also can be created by events that have the potential for creating complex, hidden, or unfamiliar plant conditions. Such conditions may include multiple hardware failures, especially those that are dependent; confusing, contradictory, or remote indications (including those wide-spread problems that can be caused by fires or seismic events); and confusing plant behavior (especially that due to degraded performance, rather than catastrophic failure, support system failures, and unusual plant configurations). If the time to core damage (or failure of a plant function) is relatively short, the ability of operators to break out of their initial mindset (i.e., expectations) and to correct any associated initial actions is limited. The opportunity for operator recovery of initial actions is similarly limited if a single functional failure leads directly to core damage and that function can be failed by operator intervention. Note that the list of ATHEANA-suggested priorities for initiators or accident sequences contains generalized descriptions of error-forcing context elements (e.g., unusual, hidden, or unfamiliar plant conditions).

Table 9.3 takes the analysis one level below that of Table 9.2, identifying the characteristics of plant functions and associated systems that have potentially high risk significance from the human perspective. It is based on the same principles as Table 9.2. The specific priorities the analyst assigns to particular characteristics in Tables 9.2 and 9.3 depend on a number of factors ranging from the particular plant design and how that affects plant response to the way individual members of operating crews interact at the specific plant under analysis. The latter was perhaps the most important lesson learned from observing plant crews in the simulator during the early trials of ATHEANA. The analysts must identify characteristics of the operating practices at the plant that make some kinds of UA-EFC pairs more or less likely, then set priorities to bring forward the more likely failure paths. A key step in this process will be observing crews in action in the simulator. Key factors to consider include teamwork, reliance on and confidence in the procedures and the plant computer, the style of formal and informal communication, the way in which the team keeps track of its progress, and how its members interact to verify the appropriateness of completed and planned actions.

Table 9.2 ATHEANA-Suggested Characteristics of High-Priority Initiators or Accident Sequences

Characteristic of Scenario	Comment/Example
Short time to damage	Large-break loss-of-coolant accident (LLOCA) initiator in the context of PRA
Unfamiliar	Not specifically analyzed in FSAR, not specifically included in operator training
Single functional failure goes to damage	Long-term cooling (e.g., failure of changeover to recirculation mode) in scenarios requiring this function
Distraction that separates control room team	Fire requires someone from the control room staff to function as a fire-fighting crew member
Forces independent action by one member of team	Fast response is required with little time for stepwise communication

Table 9.2 ATHEANA-Suggested Characteristics of High-Priority Initiators or Accident Sequences (Cont.)

Characteristic of Scenario	Comment/Example
Potential for complex and/or hidden or unfamiliar conditions	No salient evidence or reminders; dependencies or dependent failures, especially where cause and effects are far removed from each other; confusing secondary (PWRs) or support system failures; fires; seismic events
Multiple (maybe conflicting) priorities	Operators must select among or use multiple procedures (or other rules).
Wide range of accident responses, plant dynamics/conditions represented	Confusion with similar but less complex situations
Relatively high-frequency events	Transients, small-break loss-of-coolant accident (SLOCA) in the context of PRA

Next the analysts can establish priorities for the plant functions and associated systems and equipment required in response to accident initiators. The ATHEANA analysts should use the existing, plant-specific PRA model and the examples of accident characteristics given in Table 9.2. In addition, they should use the examples of characteristics given in Table 9.3 to identify potentially high priority plant functions and systems that have these characteristics. The analysts also may find the excerpts from operational experience given in Part 1, Tables 5.6 and 5.7, which can serve as templates for error-forcing contexts, useful in identifying high-priority plant functions, systems, or unsafe actions. Later, in Step 4, the high-priority HFEs associated with the high-priority functions and systems can be identified.

Table 9.3 ATHEANA-Suggested Characteristics of High-Priority Systems and Functions

Characteristics	Example
Short time to damage	No injection in a LOCA, failure of boron injection systems in anticipated transient without scram (ATWS)
Single functional failure goes to damage	No injection in a small LOCA, failure to isolate a large interfacing system LOCA
Function needed early in accident response	Inhibit automatic depressurization system (ADS) in BWR ATWS, injection in certain-sized LOCAs, boron injection in ATWS

Table 9.3 ATHEANA-Suggested Characteristics of HighPriority Systems and Functions (Cont.)

Characteristics	Example
Little or no redundancy of systems and equipment that can perform plant function	Pressure-operated relief valves (PORV) and high-pressure injection (HPI) in feed-and-bleed, low-pressure injection or recirculation system for all recirculation modes
Dependencies between redundant systems and equipment that can perform plant function	Effects of loss of reactor building closed cooling water to support high- and low-pressure coolant injection
Paucity of action cues creates high potential for confusion and complications	Events that involve unfamiliar plant conditions; similarity to other plant conditions; wide range of plant conditions and dynamics and accident response represented; cause and effects are far removed from each other; involves instrumentation and control (I&C) (about which operators are often least knowledgeable)
Functional failure has immediate effect and plant impact	Subcriticality
Functional failure can include an irreversible plant or equipment damage that has no easy recovery options or none	Failure to inhibit an emergency and full blowdown using the instrumentation and control ADS during a BWR ATWS; EOCs for inappropriate starts or stops of equipment
Human-intensive accident response important principally for EOCs	Steam generator tube rupture (SGTR) sequences, ATWS sequences

9.2.2 Products of Step 2

The output of this step is a set of selected initiators (or overall classes of initiators, if desirable) for which the issue (from Step 1) is to be analyzed. This provides some boundaries for the analysis and therefore an overall context, as well as a relationship to a PRA. In addition, the development of priorities on scenarios and plant functions is used in Steps 3, 4, and 6 to guide the analysis.

9.3 Step 3: Describe the Base Case Scenario

In this step the base case scenario is summarized and defined for a chosen initiator(s). The base case scenario:

- represents the most realistic description of expected plant and operator behavior[3] for the selected issue and initiator

[3] However, it is recognized that a range of conditions within the definition of the base case scenario is possible.

- provides a basis from which to identify and define deviations from such expectations in Step 6

Figure 9.3 is a process flow diagram that shows the detailed tasks required for this step. An overview of these tasks is provided in Section 9.3.1. Following the overview, more detailed guidance for developing the base case scenario is provided.

9.3.1 Overview of Step 3

As stated above, the purpose of this step is to define and characterize a base case scenario that will be used in later ATHEANA analysis steps. Table 9.4 operationally defines what a base case scenario is. For example, the ideally defined base case scenario:

- has a consensus operator model (COM)
- is well defined operationally
- has well-defined physics
- is well documented in public or proprietary references
- is realistic

Each of the characteristics of an ideal base case scenario is described briefly below.

Consensus operator model: Operators develop mental models of plant responses to various PRA initiating events through training and experience. If a scenario is well defined and consistently understood among all operators (i.e., there is a consensus among the operators), then there is a consensus operator model. Note that given the current high reliability of operations, with zero to one trips per year at each plant, most operators licensed within the past five years will have no direct experience with even the most common trip scenarios. For more seasoned operators, direct experience is becoming increasingly remote. Therefore, it is likely that the consensus operator model will be that seen routinely in the plant simulator.

Well defined operationally: A scenario is well defined operationally if the scenario has been addressed in procedures, training, operational or simulator experience, and the specific equipment and expected operator responses are well understood.

Well-defined physics: If the plant behavior has been thoroughly analyzed in thermal hydraulics, neutronics, or other calculations, the physics of the scenario is considered well defined. This characteristic, along with the characteristic of being well documented, is termed the "reference analysis" for a scenario.

Well documented: If the scenario (including thermal hydraulic, (T-H) neutronics calculations, etc.) has been fully described in public or proprietary information sources, it is considered to be well documented. Such documentation, often found in plant FSARs or PRA supporting documentation, represents the reference analysis for a scenario.

Realistic: If the scenario description is consistent with how the plant really works, it is considered realistic. However, since the scenario is initially defined at the level of an initiating event, a broad range of plant behavior is represented. Consequently, the scenario description may be realistic for the whole class or for only one example within a class (and not for all of the others within the class).

Table 9.4 shows two situations for defining a base case scenario: the ideal case and less than ideal cases. This table also illustrates that the base case scenario may be defined differently for different cases, depending upon what information resources are available. Table 9.4 also provides the analysts with some options for how to develop the base case scenario when the information available is weak. Choices among these options are value judgments in which management, policy, or resources may be the deciding factors.

Figure 9.3 shows the approach for performing this step. This approach recognizes that there are preferred information sources and that these sources are not always available. The preferences are described below and summarized in Table 9.4.

The first preference is to define the base case scenario so that it corresponds with the consensus operator model. Consequently, the first task is to determine if there is a consensus operator model. If there is a COM, it should be described using appropriate plant-specific resources. If there is no COM because operators have no expectations for this scenario, the analysts should proceed to the task of identifying and describing any reference analyses.

As shown in Figure 9.3, regardless of whether there is a consensus operator model, the next task in this step is to determine if there is a reference analysis for the scenario. This task is needed, for different reasons, in both instances.

A reference analysis is needed if there is a consensus operator model because, from a thermal hydraulic point of view, such scenarios are not always well defined and documented in the open literature. For some initiating event types, a reference analysis will be provided in the plant's FSAR Chapter 14 or 15 safety analysis (although other sources, such as supporting calculations for a PRA, may be available and appropriate). The reference analysis that most closely approximates the consensus operator model should be selected for use in this step. In this instance, as shown in Figure 9.3, the descriptions of the consensus operator model and the reference analysis together comprise the base case scenario.

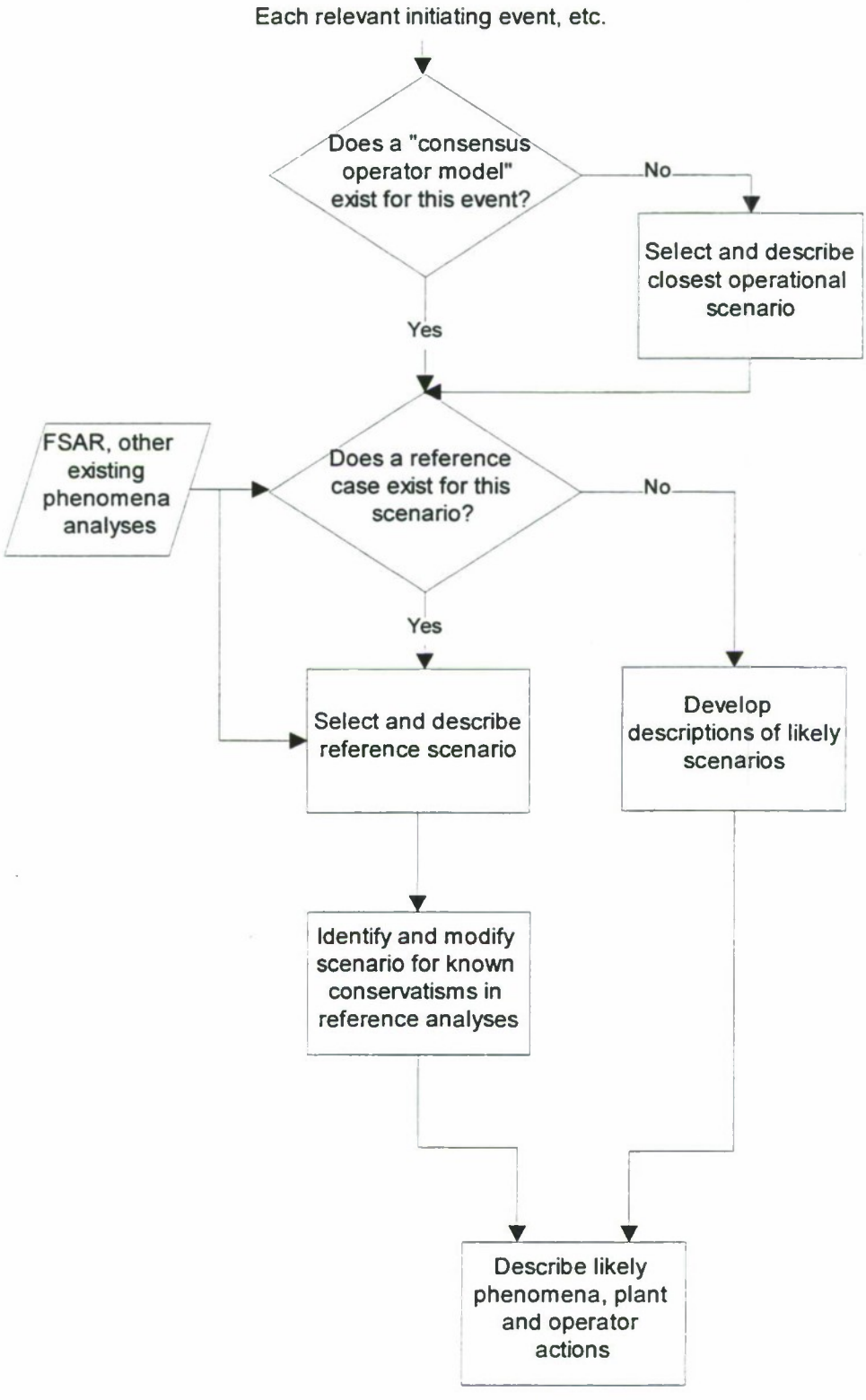


Figure 9.3 Step 3 - Describe Base Case Scenario

Table 9.4 Development of the Base Case Scenario

Example of types of Base Case[a]	Characteristics of a base case scenario					Options for Development when Information is Weak[c]
	Consensus Operator Model (COM)	Well defined Operationally	Reference Analyses		Realistic[b]	
			Well-defined Physics (T-H and neutronics)	Well documented Public or Proprietary Sources		
Ideal	Exists	Yes	Matches COM	Yes, public	Yes	N/A[d]
When the ideal is not available, another type of base case must be developed	In some cases, there may be no COM, or it may not be well-defined operationally. Examples in Appendices B–E describe some specific cases.		There may be no reference analysis that directly applies to the COM. Sometimes analyses will be available to the analysts, but not to others. Some tie to a reference analysis is needed to allow understanding and quantification of deviations from a T-H well-defined condition.		If the COM is not a realistic model of how the plant will actually respond, the operators' situation assessment is obviously flawed.	The project has many choices when the options for the base case do not include the "ideal." These include such possibilities as: 1. Judgmentally adusting the reference case to make it realistic and to make it match the COM 2. Funding additional reference case analysis 3. Selecting likely human activities, if the COM is not well defined 4. Surveying operators and trainers, if the COM is not readily apparent 5. Selecting an arbitrary base case and treating all other identifiable scenarios as deviations

[a] In all cases, a base case must be identified. The deviation analysis of Step 6 will proceed from this base case. The significance of deviations from the base case will involve evaluation of the base case and its relationship to the COM.

[b] "Realistic" should address whether it is realistic for the whole class or only one example in the class (and far off for all others).

[c] Choices among these options are value judgments, i.e., management decisions; resources or policy may be deciding factors.

[d] N/A = Not applicable.

In the instance where there are no operator expectations, reference analyses alone are used to develop the base case scenario.

As shown by the right-hand branching in Figure 9.3, in some cases there may be no FSAR analyses or other referenceable sources to approximate the consensus operator model or otherwise define a base case scenario. This often occurs for the starting events (see Step 2, Section 9.2 for definition) that are indirect causes of plant trips, such as the support system initiators and the external events. (Note that operators may not expect these events either.)

For these situations, it only may be possible to construct a base case scenario from either a most likely scenario or simply an arbitrary scenario. For such situations, the scenario description still should be realistic, based on available knowledge and expert judgment.

9.3.2 Detailed Guidance for Step 3

Figure 9.3 shows that there are five tasks that must be performed in Step 3:

(1) Identify and describe the consensus operator model.
(2) Identify and describe relevant reference analyses.
(3) If necessary, describe modifications to reference analyses.
(4) If there are no reference analyses, describe possible scenarios for the selected initiator.
(5) Describe the resulting base case scenario.

The description of the base case scenario is the end result of these tasks and is developed using existing information sources and an understanding of accident behavior. The principal sources of information needed for the tasks in Step 3 are:

- plant-specific FSAR
- other reports or documents that describe the design basis
- other plant-specific safety analyses (e.g., thermal-hydraulic analyses)
- vendor safety analyses
- plant-specific procedures [especially (EOPs)]
- vendor or generic emergency procedures
- basis documents for procedures (e.g., vendor emergency response guidelines)
- operator experience (both simulator training and actual operations)
- operator training material and its background documentation
- plant staff, especially operations, operator trainers, and those responsible for thermal-hydraulic analyses
- plant-specific and industry generic operating experience

Each of the five tasks in Step 3 is described below.

9.3.2.1 Identify and Describe the Consensus Operator Model

In order to perform this task, the analysts first should collect information from operator trainers and plant-specific operating experience to determine if there are operator expectations for the initiating event selected. Based upon the operator expectations identified, the analysts should determine if there is a consensus operator model.

If there is a COM, then the analysts should develop a description of the model using appropriate plant-specific resources. In some cases, there may be no COM, but multiple operator opinions. If this is the case, then analysts should select and describe the scenario that most closely matches (operationally) these various opinions, or define multiple base case scenarios for investigation. If there is no COM because operators have no expectations for this scenario, the analysts should proceed to the task of identifying and describing any reference analyses.

Input from operator trainers is especially important to this task since they are likely to be knowledgeable about both operational and training experience of the operating crews. If the resources allow them, interviews of operators can yield additional, useful information for this task.

9.3.2.2 Identify and Describe Relevant Reference Analyses

The reference analysis is a detailed engineering analysis of the neutronics and thermal hydraulics of a scenario. The analysts should identify the reference analyses that most closely match the consensus operator model, if one exists. If there is no COM, but multiple operator opinions, then analysts have to identify as many reference analyses as are needed to best represent the scenario or scenarios selected in the previous task. If there is no COM because operators have no expectations for this scenario, a reference analysis should be selected based upon the analysts' judgment, especially with respect to the realism of the scenario.

In describing the reference analyses, analysts should not only describe the applicable scenario but also provide appropriate citations of the referenceable information source in order to facilitate documentation and traceability. For example, if the initiator is included in the FSAR, a description of the reference case should begin by citing the applicable FSAR sections. In the description, direct quotation of the FSAR may be desirable to avoid ambiguity and to facilitate traceability.

9.3.2.3 Describe Modifications to Reference Analyses

If both a consensus operator model and a reference analysis have been identified, they should be compared to determine if the reference analyses should be modified to better represent operator expectations. Whether or not there is a consensus operator model, if the referenceable scenario information contains known conservatisms, such as FSAR analyses, these conservatisms may need to be relaxed in order to help describe an expected and/or more realistic scenario. In addition, more realistic (or likely) plant behavior and equipment interactions should be identified. Recommended

resources for performing the modifications to the reference analyses include operations staff, operator (simulator and classroom) trainers, and staff responsible for thermal-hydraulic calculations.

Particularly where it is based upon safety analyses, such as those documented in the FSAR, the reference analysis will not take credit for, nor account for, the effects of nonsafety, normally operating equipment. Generally, the consensus operator model will assume operability of both safety-related and normally operating systems. Where the operation of this nonsafety equipment does not affect the overall plant response in the scenario of interest, the consensus operator model and the reference analysis will be essentially the same, such as in the large loss-of-coolant accident example given in Appendix C. However, where the continued operability of the normally operating equipment does affect the plant response, at least to some degree, the consensus operator model and the reference analysis can be different, as illustrated in the loss of main feedwater (LMFW) example given in Appendix B. In the latter case, it will be necessary to modify any reference analysis information to fit the consensus operator model. For example, for the LMFW, most other transients, and the small LOCA, the nonsafety control systems (e.g., the condenser and atmospheric steam dumps) control the secondary and primary system thermal-hydraulic responses. The FSAR safety analysis does not include these systems, i.e., it assumes that they are not available. Therefore, in all reference analyses, the primary and secondary system parameters controlled by the steam generator steaming rate (heat removal) may be quite different than those in the consensus operator model. In other words, the base case scenario in these cases is developed from the consensus operator model and a modified version of an associated reference analysis.

9.3.2.4 Describe Possible Scenarios for the Selected Initiator (if no Reference Analysis)

As shown in Figure 9.3, in some cases, there may be no FSAR analyses or other referenceable sources to approximate the consensus operator model or otherwise define a base case scenario. This often occurs for the starting events (see Step 2, Section 9.2 for definition) that are indirect causes of plant trips, such as the support system initiators and the external events. (Note that operators may have no expectations for these events either.) These starting events are causes of standard initiating events (such as turbine trip, reactor, and small LOCA) and they complicate those initiating events by:

- disabling or degrading systems useful in mitigating the initiating event
- creating a slowly and apparently randomly degrading situation that is not part of normal design, training, and procedural expectations
- being one of many possible instances of the starting event, each leading to decidedly different event and parameter progressions, or
- creating other elements of context that can increase the likelihood of the occurrence of an unsafe act

For these situations, it only may be possible to construct a base case scenario from either a most likely scenario (based on plant-specific or generic operational experience, supplemental analysis, and judgment of trainers and analysts, if possible) or simply an arbitrary scenario (if the range of possible scenarios is too broad, as in the loss of service water example given in Appendix E). For such situations, the scenario description still should be realistic, based on available knowledge and expert judgment.

9.3.2.5 Describe the Base Case Scenario

As discussed in Section 9.3.1, the base case scenario is based upon the consensus operator model and relevant reference analyses, if both a COM and reference analysis exist. In the ideal case where both exist, then the description of the base case scenario should include:

- a list of assumed causes of the initiating event
- a brief, general description of the expected sequence of events, starting before reactor trip
- a description of the assumed initial conditions of the plant
- a detailed description of the expected sequence and timing of plant behavior (as evidenced through key functional parameters) and plant system and equipment response
- the expected trajectories of key parameters, plotted over time, that are indications of plant status for the operators
- any assumptions with respect to the expected plant behavior and system or equipment and operator response (e.g., equipment assumed to be unavailable, single failures of systems assumed to have occurred)
- key operator actions expected during the scenario progression

As indicated above, key functional parameters should be considered in the description of the base case scenario. These are generally those functional parameters found in the EOPs and used by the operators to assess plant status and to make decisions about what actions need to be taken. Note that for a specific issue or initiator, some parameters may not be particularly relevant to identifying and analyzing possible human failure events (HFEs) associated with the issue or event. In such cases, those parameters may be eliminated from the base case description of plant behavior. However, care should be taken in eliminating any functional parameters since an unexpected response in seemingly unrelated parameters could induce interesting HFEs. Examples of key functional parameters are:

- reactor power
- turbine or generator load
- electric power

- instrument air
- service water (and similar systems)
- reactor coolant system (RCS) level and pressure
- core heat removal (e.g., T_{avg}, core outlet temperatures, subcooling margin)
- steam generator level and pressure
- containment pressure and temperature
- radiation
- ventilation
- equipment conditions (e.g., vibration, fluctuating current, high temperature, or other signs of imminent damage)
- other key parameters addressed in plant-specific EOPs

The expected operator behavior for the base case scenario is important for the use of ATHEANA. This can be determined from the plant behavior described above, a review of relevant procedures and training, and the relevant, key functional parameters. Expected operator actions should be part of what is described for the base case scenario.

9.3.3 Product of Step 3

The product of this step is a description of the base case scenario containing the information listed in Section 9.3.2. Table 9.5 illustrates how the base case scenario might be developed for examples of different situations regarding information availability. For instance, Table 9.5 provides three options for developing a base case scenario for the loss of main feedwater example. In Appendix B, the second option of adjusting the reference analyses to be more realistic and better match the consensus operator model was used. Also, Appendices B through E describe more specifically and in more detail some examples of such situations and the resulting base case scenarios.

9.4 Step 4: Define HFE(s) and/or UAs

Possible HFEs and/or UAs can be identified and defined in this step. However, Step 1 may have already defined an HFE or UA as being of interest. Alternatively, the deviation analysis, recovery analysis, or quantification performed in later steps may identify the need to define an HFE or UA. Also, recovery analysis or quantification may require development and definition of operator actions at a different level (e.g., unsafe action versus HFE). Consequently, the ATHEANA analysis may require iteration back to this step. To the extent possible, the information that would be needed in any of these cases is provided in this step.

Table 9.5 Examples of Base Case Scenario Development

Example of types of Base Case[a]	Characteristics of a base case scenario					Options for Development when Information is Weak[c]
	Consensus Operator Model (COM)	Well-Defined Operationally	Reference Analyses		Realistic[b]	
			Well-Defined Physics (T-H & neutronics)	Well-Documented Public or Proprietary Sources		
Ideal	Exists	Yes	Matches COM	Yes, (publicly available)	Yes	Not needed
Loss of main feedwater	Exists	Fairly well defined	An FSAR scenario is probably the best choice, but it will differ from the COM	Yes, is the FSAR version used (i.e., public)	Probably not (e.g., missing control systems)	1. Use FSAR as reference case without modification, recognizing problems 2. Adjust the reference (i.e., FSAR) analyses to be realistic and match COM 3. Do new T-H analyses (or use propriety analyses) to serve as the reference
Fires, external events	No COM. Too many open-ended possibilities	No	No	Many mechanistic and PRA analyses of fires, but no single scenario	Many realistic models of fire progression; many bounding analyses of particular fire consequences.	Reasonable base cases, if not COMs: 1. Many fire PRAs assume a loss of feedwater or turbine trip initiator due to fire. 2. Earthquake PRAs often use a turbine trip as their base case, because of the seismic trip. For more severe earthquakes, loss of offsite power and LOCAs are used, depending on specific vulnerabilities.

Table 9.5 Examples of Base Case Scenario Development (Cont.)

Example of types of Base Case1[a]	Characteristics of a base case scenario					Options for Development when Information is Weak[c]
	Consensus Operator Model (COM)	Well-Defined Operationally	Reference Analyses		Realistic[b]	
			Well-Defined Physics (T-H & neutronics)	Well-Documented Public or Pro-prietary Sources		
Loss of service water	No	No	Partially	Partial information	For a subset of possibilities with a broad range possibilities	1. Survey operators and trainers[d] 2. Make arbitrary choice if no reference case or operator opinions.

[a] In all cases, a base case must be identified. The deviation analysis of Step 6 will proceed from this base case. The significance of deviations from the base case will involve evaluation of the base case and its relationship to the COM.

[b] In other words, the way the plant would really work. However, "realistic" also should address whether it is realistic for the whole class or only one example in the class (and far off for all others).

[c] Choices among these options are value judgments; management or policy may be deciding factors.

[d] This activity is performed as part of Step 5 to identify if there is a consensus operator model.

A "human failure event" is a PRA term that requires PRA concepts for its definition. On the other hand, an "unsafe action" is not specifically tied to a PRA, but allows the analysts to bridge the gap between human behavior and the PRA mode. Definitions for both these terms are:

Human failure event: A basic event that is modeled in the logic models of a PRA (event and fault trees), and that represents a failure of a function, system, or component that is the result of one or more unsafe actions.

Unsafe action: An action inappropriately taken or not taken when needed, by plant personnel that results in a degraded plant safety condition.

9.4.1 Guidance for Step 4

This guidance is written with the assumption that first HFEs will be identified in the ATHEANA process, then UAs. However, as noted above, iterations back to this step may require only one of these identifications. Regardless, the information and approach for the identification of HFEs and UAs, given in separate subsections, remain the same.

HFE definitions are based upon the relevance to the issue or event being addressed and the requirements for plant response to the initiating event. HFEs are typically of a functional nature (e.g., shutdown secondary cooling) and may be sufficient to address the issue identified in Step 1. Other times, it may be more beneficial to define specific unsafe actions [e.g., put LPCI (low-pressure coolant injection) pumps in pull-to-lock] in order to represent the issue of concern. In either case, these are the undesirable operator actions for which the ATHEANA process is being used to determine error-forcing contexts that may make the actions plausible or even likely.

Performance of this step requires the following inputs:

- the issue definition from Step 1
- the plant-specific PRA model, especially event trees and success criteria
- description of the base case scenario from Step 3
- (if necessary) additional knowledge and information regarding accident response, general plant design and operation, and system design and operations

9.4.1.1 Defining HFEs

To the extent the PRA is used to aid in the definition of relevant HFEs or UAs, it may be desirable to transform any systemic event trees into functional event trees if the issue definition is broad and not specific to any one system. When redefining these event trees, functions that are represented both explicitly and implicitly in the event tree should be considered, including passive plant functions. In addition, some plant functions shown as event tree headings represent more than one system (under either an AND or OR gate) and these other systems (and sometimes human actions) also should be identified and noted (or shown explicitly).

The following systematic process leads to the identification of HFEs. Some of these tasks may have been performed in the previous steps (e.g., identify the functional success criteria). Also, the selected issue may allow some of these tasks to be omitted. With these exceptions, HFEs can be identified for each function represented in the event tree for the relevant initiator by:

(1) identifying whether the function is:
- needed, or
- undesired with respect to the accident response requirements for the specific initiator or sequence

(2) identifying the system(s) or equipment that perform the function

(3) identifying the pre-initiator status of the system(s) or equipment (e.g., normally operating, standby, passive)

(4) identifying the functional success criteria for the system(s) or equipment

(5) identifying the functional failure modes of the system(s) or equipment

(6) deciding if either errors of commission, errors of omission, or both types of errors are relevant to the selected issue

(7) identifying applicable descriptions of possible human failures that can be developed into candidate human failure event descriptions

Tables 9.6 and 9.7 serve as guides for the ATHEANA analysts in performing these tasks. However, the guidance given is intended to be illustrative rather than exhaustive. Table 9.6 also contains examples of systems, given in the far right column, that may have the characteristics shown in the other columns of the table. Similarly, examples of human actions that can fail plant systems or equipment by different functional failure modes are shown in Table 9.7. Both tables should be used to trigger ATHEANA analysts' discussions on which of the examples given are applicable and on other possible success criteria, failure modes, and human failures.

Table 9.6 can be used to accomplish the first six tasks listed above. In the first column of Table 9.6, the ATHEANA analysts must identify whether each plant function in each event tree for the relevant initiator is needed or undesired. Next, the systems or equipment that perform these functions must be identified. Then, the tasks associated with the remaining columns are performed for each of these systems. In the third column, the likely pre-initiator status of each system is identified. (However, the ATHEANA analysts should remember that some initiators can change the status of systems. In such cases, the immediate post-initiator status is more relevant than the pre-initiator status.) After having determined the pre-initiator status, the ATHEANA analysts must determine the functional success criteria and functional failure modes that are appropriate for each system. Table 9.6 (fourth and fifth columns) provides examples of PRA functional success criteria and PRA functional failure

Table 9.6 Functional Failure Modes Based upon PRA Requirements[a]

Function Required in PRA? (1)	Systems that Perform Function (2)	Pre-Initiator Status (3)	Functional Success Criteria (4)	Functional Failure Modes (5)	Functional Failure Mode Category[b] (6)	Example Systems
(a) Needed		Standby	Equipment automatically actuates (short mission time)	Equipment fails to initiate or actuate automatically	1	RPS, accumulators
			Equipment automatically actuates and continues to operate for duration of mission time (longer mission times)	Equipment fails to initiate or actuate automatically	2	HPI, LPI, AFW, CS, CI
				Equipment fails to continue to operate for duration of mission time	3	
			Equipment manually actuated and continues to operate for duration of mission time	Equipment fails to be manually initiated or actuated when required	4	HPR, LPR, RHR, SDC
				Equipment fails to continue to operate for duration of mission time	3	
		Standby or Operating	Equipment manually operated as necessary to control plant parameters for duration of mission time	Equipment manually not actuated when required	4	PORVs, ADS
				Equipment fails to continue to operate for duration of mission time	3	MFW, Condesate, AFW, HPI, LPI, RCPs, CVCS, SLC
				Equipment fails to be controlled or operated as required	5	
		Passive	Equipment maintains required status	Equipment status inappropriately changed	6	
(b) Undesired		Operating	Equipment stopped and remains stopped for duration of mission time	Equipment fails to stop automatically	7	RCPs

Table 9.6 Functional Failure Modes Based upon PRA Requirements[a] (Cont.)

Function Required in PRA? (1)	Systems that Perform Function (2)	Pre-Initiator Status (3)	Functional Success Criteria (4)	Functional Failure Modes (5)	Functional Failure Mode Category[b] (6)	Example Systems
		Standby	Equipment maintains pre-initiator (or immediate post-initiator) status	Equipment fails to remain stopped for required duration Equipment fails to be stopped manually Equipment fails to maintain desired status Equipment status changes spuriously and inappropriately	8 9 10 11	SLC, SI, CI, CS

[a] Acronym's: HPI-high pressure injection; LPI-low pressure injection; AFW-auxillary feedwater; CS-core spray; HPR-high-pressure recirculation; LPR-low-pressure recirculation; RHR-residual heat removal; SDC-shutdown cooling; PORVs-power-operated relief valves; ADS-automatic depressurization system; MFW-main feedwater; RCPs-reactor coolant pumps; CVCS-chemical and volume tank coolant; SI-safety injection.

[b] Note that the numbers assigned in column 6 to the functional failure made categories provide a link to the associated rows in Tables 9.7 and 9.9a-3.

Table 9.7 Examples of Likely Human Failures and Human Failure Modes by PRA Functional Failure Mode

PRA Functional Failure Modes (5)	Functional Failure Mode Category (6)	EOC or EOO? (7)	Example Human Failures (8)	Transfer to Unsafe Action Table for Step #7
Equipment fails to initiate/actuate automatically	1	EOC	Equipment inappropriately removed from automatic control Equipment inappropriately removed from armed or standby status	Table 9.9a
	2			
		EOO	Automatic actuation fails, and no backup, manual startup	Table 9.9d
Equipment fails to continue to operate for duration of mission time	3	EOC	Equipment inappropriately terminated Equipment inappropriately isolated or aligned Equipment output and/or resources inappropriately diverted Equipment output and/or resources inappropriately depleted	Table 9.9b
Equipment fails to be manually intiated or actuated when required	4	EOC/EOO	Equipment fails to be actuated when required Equipment inappropriately actuated	Table 9.9c
Equipment fails to be controlled or operated as required	5	EOC/EOO	Equipment fails to be operated or controlled Equipment inappropriately operated or controlled	
Equipment fails to maintain desired status	6	EOC/EOO	Equipment status inappropriately changed Fails to maintain integrity Inappropriately breached integrity	Table 9.9e
	10	EOC	Equipment inappropriately operated	Table 9.9b
Equipment fails to stop automatically	7	EOC	Equipment inappropriately removed from automatic control	Table 9.9a
		EOO	Automatic stop fails, and no backup, manual stop	Table 9.9d
Equipment fails to be stopped manually	9	EOO	Equipment fails to be stopped when required	Table 9.9c
Equipment fails to remain stopped for required duration	8	EOC	Equipment inappropriately restarted (and continues to operate)	Table 9.9b
		EOO	Equipment spuriously restarts, and no backup, manual stop	Table 9.9d
Equipment status changes spuriously and inappropriately	11	EOO	Spurious actuation, with no backup stop of equipment Spurious reconfiguration, with no backup realignment	

modes associated with different types of systems of equipment based upon functional need and pre-initiator status. The ATHEANA analysts should begin by considering those functional success criteria and failure modes represented explicitly in the plant-specific PRA. In order to complete this activity, however, the analysts should try to identify additional important success criteria and failure modes. Such criteria may be implicit in the PRA model, or may be indicated in emergency operating procedures or operating practice. A review of anecdotal experience also may be helpful in these activities. Finally, the ATHEANA analysts should determine the functional failure mode categories (sixth column) applicable to each system.

Since most systems or equipment have multiple operational requirements for success (e.g., automatic actuation, continued operation for required mission time, control of operation during mission time) and therefore multiple opportunities for failure, it is important that ATHEANA users identify all of the functional success criteria and functional failure modes that apply to a specific system or piece of equipment when using Table 9.6. For example, for needed, standby systems, the ATHEANA analysts must consider all of the example functional success criteria associated with a standby pre-initiator status and the functional success criteria associated with a standby or operating initial status. However, since Table 9.6 contains some redundancy in identifying functional failure modes, the specific path for finding applicable functional failure modes is not important.

The results of the sixth column in Table 9.6 are used in Table 9.7 to perform the last two tasks listed above. With the seventh column of Table 9.7, the ATHEANA analysts can focus the remaining analysis steps on either errors of commission or errors of omission.[4] This seventh task is inserted at this point in the analysis since the issue selected for the ATHEANA HRA analysis may be limited to only certain human failure modes (e.g., only EOCs, or only EOCs and nonbackup types of EOOs). By inserting this decision point, the investigation of possible human failures can be limited to only those associated with the human failure modes that are relevant to the selected issue. The eighth column of Table 9.7 provides examples of human failures that are either EOOs or EOCs and that are categorized by the system functional failures shown in the sixth column. The ATHEANA analysts should review the examples provided in Table 9.7 to determine which are applicable for the function and system or equipment being considered. In addition, the example failures in Table 9.7 should be expanded using the ATHEANA analysts' understanding of the system or equipment design and operational features. It also is important that any ideas generated by the ATHEANA analysts regarding specific unsafe actions and associated error-forcing contexts be documented along with the results of ATHEANA steps.[5] (As noted earlier, it is possible that the recovery analysis performed in Step 8 or other steps in the ATHEANA analysis will require a human failure event to

[4] The terms "error of omission" and "error of commission" are PRA terms that are associated with different system failure modes. These terms also are useful in differentiating between human events that may already be modeled in the PRA and those that may not have been considered before. Section 1.4.2.1 provides more discussion on the usefulness of the EOO and EOC classifications.

[5] Experience suggests that the ATHEANA analysts will most easily think at the level of unsafe actions and error-forcing contexts, rather than in terms of HFEs. Consequently, thinking ahead to unsafe actions and error-forcing contexts is not discouraged, but should be documented as it occurs. In this way, such ideas will be preserved for future use while maintaining the systematic nature of the search process, which is desirable.

be decomposed into unsafe actions. If so, this decomposition will be performed in Step 8 if it is not performed in this step.)

The example human failures given in the eighth column of Table 9.7 are used to develop candidate human failure events, as defined for the plant-specific PRA. Based upon the identified, relevant human failures, several candidate HFEs are expected to be identified for each system and equipment. Using the example human failures given in Table 9.7, these HFEs should be defined in the context of the plant-specific PRA. The associated descriptions of these candidate HFEs should have one of the following general formats:

Error of omission:
*Operators fail to (*action verb for functional failure mode *) system X*

Error of commission:
*Operators inappropriately (*action verb for functional failure mode*) system X*

9.4.1.2 Defining Unsafe Actions

Because of possible differing needs for definitions of unsafe actions, multiple approaches for this task must be provided. As in the definition of HFEs, the issue of interest for ATHEANA analysis may specify an unsafe action. If such is the case, no further investigation is required for the identification of an unsafe action. On the other hand, the need for decomposition of HFEs into unsafe actions may not be recognized until recovery analysis or quantification steps are performed. The requirements imposed by these steps may even provide some indications as to what types of unsafe actions are relevant. In this case, an abbreviated process for defining an unsafe action is needed. Finally, the analysts may require a rigorous identification of all unsafe actions associated with an HFE.

For the case in which the abbreviated process is sufficient, Table 9.8 is provided to assist the analysts in identifying and defining unsafe actions. Example unsafe actions are provided for generalized equipment functional failure modes. (Table 9.8 was developed from Tables 9.9a-e which are used in the rigorous UA search approach.) The examples given are not meant to be exhaustive but merely illustrative and may help identify additional unsafe actions or functional failure modes.

Table 9.8 Example Unsafe Actions for Generalized Equipment Functional Failure Modes

Equipment Functional Failure Mode	Example Unsafe Action(s)
Failure of automatic actuation	Operators take equipment out of armed or standby status Operators change equipment configuration from armed, standby, or normal state Operators bypass or suppress automatic signals Operators disable automatic signals or sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators disable or fail equipment Operators reset signal setpoints
Inappropriate actuation	Operators actuate equipment prematurely (i.e., too soon) Operators prematurely release or unsuppress equipment automatic initiation signals Operators manually actuate equipment (when not needed) Operators manually actuate equipment automatic control
Failure to control	Operator control of equipment results in: Underfeeding or filling — Overfeeding or filling Undercooling — Overcooling Underpressure — Overpressure Reactivity decrease — Reactivity increase Integrity breach
Failure of manual initiation or actuation	Operators never actuate equipment Operators actuate equipment too late Operators release or unsuppress equipment automatic initiation signals too late Operators fail to perform backup, manual startup after automatic actuation fails (recovery)
Inappropriate termination	Operators stop (e.g., pumps stopped Operators both stop and disable equipment for future service (e.g., pumps in pull-to-lock) Operators disable or fail equipment (e.g., due to operation outside of design parameters) Operators stop and realign equipment out of required armed or standby configuration or lineup Operators stop equipment and bypass or suppress automatic signals Operators stop eqipment and disable automatic signals or sensors Operators stop equipment and take automatic signals out of armed status Operators stop equipment and reset signal setpoints
Inappropriate isolation	Operators re-align equipment (e.g., valves repositioned) Operators actuate equipment automatic isolation signals Operators actuate equipment automatic reconfiguration signals

Table 9.8 Example Unsafe Actions for Generalized Equipment Functional Failure Modes (Cont.)

Equipment Functional Failure Mode	Example Unsafe Action(s)
Inappropriate diversion or depletion of resources	Operators realign equipment (e.g., valves repositioned) Operators operate equipment outside design parameters (e.g., over RHR design pressure, resulting in flow diversion through lifted relief valves, ISLOCAs, etc.) Operators do not adequately control equipment that competes for resources before or during operation of required equipment Operators do not control equipment early in accident
Failure to terminate	Operators never stop equipment Operators stop equipment too late Operators release or unsuppress equipment automatic initiation signals for stop too late Operators fail to perform backup, manual stop after automatic stop fails (recovery) Operator fail to perform backup, manual stop after spurious start or re-start (recovery)
Inappropriate status change	Operators manually actuate or start equipment Operators manually realign equipment Operators manually override equipment automatic isolation signals Operators manually actuate equipment automatic control Operator actions (e.g., operator fails to operate or control, operator inappropriately operates or controls) from other categories result in failure to maintain integrity , inappropriately breached integrity, etc.

If the analysts cannot describe an HFE at the level of a functional failure mode (such as that given in Table 9.8), then a more rigorous approach to identifying unsafe action should be used. This more rigorous approach is performed using Tables 9.9a-e, along with links to Table 9.7, which concluded the identification of HFEs in the previous task. Tables 9.9a-e (found at the end of Section 9) allow the analysts to identify the different ways in which the operators could produce the effects characterized by the failure modes used to define HFEs. The last column of Table 9.7 guides the analysts to different tables (Tables 9.9a-e) based upon functional failure mode. (Categories of failure modes are used in the tables to make transfers between tables easier for the analysts.) Tables 9.9a-e provide example unsafe actions for different human failures. The examples given in these tables should be used in discussions or brainstorming sessions in conjunction with an understanding of design and operational characteristics of plant systems and with the plant experience (both simulator and operational), industry experience, and plant knowledge of the ATHEANA analysts to identify applicable unsafe actions and generate other possible unsafe actions. Because in some cases more than one category of functional failure mode will lead to the same example of unsafe actions, the analysts should not be overly concerned about what category leads them to the applicable examples.

Most of the example human failures and UAs result directly in a functional failure. However, the control failures (i.e., functional failure mode category 5) addressed in Table 9.9c more often involve the effect of equipment failures on plant functions. For example, undercooling in the context of the high-pressure injection (HPI) system can be the result of too little HPI flow (e.g., too few trains operated or overthrottling) or of the HPI pumps being turned off or not operated frequently enough. The dependent effects between systems and support systems (including shared resources) also must be considered. Consequently, the ATHEANA analysts also should use the following sets of guide words in identifying indirect effects of failure modes:

Examples of key plant parameters to be controlled:

- Temperature
- Pressure
- Level
- Volume
- Flow or flow rate
- Reactivity
- Subcooling margin (PWR)

Example control failures:

- Too much or little (e.g., throttling, quantity)
- Too soon or late (timing)
- Too fast or slow (rate)
- Too many or few times (frequency)
- Too short or long (duration)
- Too many or few trains (quantity and rate)
- Under or overthrottling (quantity and rate)

The ATHEANA analysts should keep in mind that there may be many different ways in which a failure mode may be activated. For example, the operator can take the following inappropriate actions:

- not use (e.g., fail to start) a system
- make it difficult to use a system (e.g., put pumps in pull-to-lock or deplete system resources)
- damage (even permanently) system equipment

The reasons an operator may do these things and the potential for eventual recovery also are different. Later steps in the process that lead to the identification of the error-forcing context address these reasons. However, as in previous steps, the analysts should document for later use any ideas generated during this step regarding reasons for UAs and EFCs.

9.4.2 Products of Step 4

The products of Step 4 include:

- a list of HFEs, and their associated descriptions relevant to the issue and for each event tree (or selected initiator) in the PRA
- (possibly) UAs associated with each candidate HFE

9.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

This is a preliminary step to the searches for the deviations from the base case scenario that are identified in Steps 6 and 7. In particular, analysts are guided to find potential vulnerabilities in the operators' knowledge base for the initiating event or scenario(s) of interest that may result in the HFEs or UAs identified in Step 4. For example, the implications of operator expectations and the associated potential pitfalls (i.e., traps) inherent in the initiating event or scenario(s) that may represent vulnerabilities in operator response are identified.

The information that is obtained in this step should be put on a mental or literal blackboard for use in later steps, especially Step 6. In this way, analysts will be reminded of and guided to the more fruitful areas for deviation searches, based upon the inherent vulnerabilities in the operators' knowledge base for the initiator or scenario of interest.

As illustrated by Figure 9.4, potential traps inherent in the ways operators may respond to the initiating event or base case scenario can be identified through the following:

- investigation of potential vulnerabilities in operator expectations for the scenario
- understanding of a base case scenario timeline and any inherent difficulties associated with the required response
- identification of operator action tendencies and informal rules
- evaluation of formal rules and emergency operating procedures expected to be used in response to the scenario

Guidance for identifying potential traps using each of these approaches is given below. The individual trap searches are discussed separately, although some of these searches overlap. Finally, all of the identified potential vulnerabilities are summarized and aggregated.

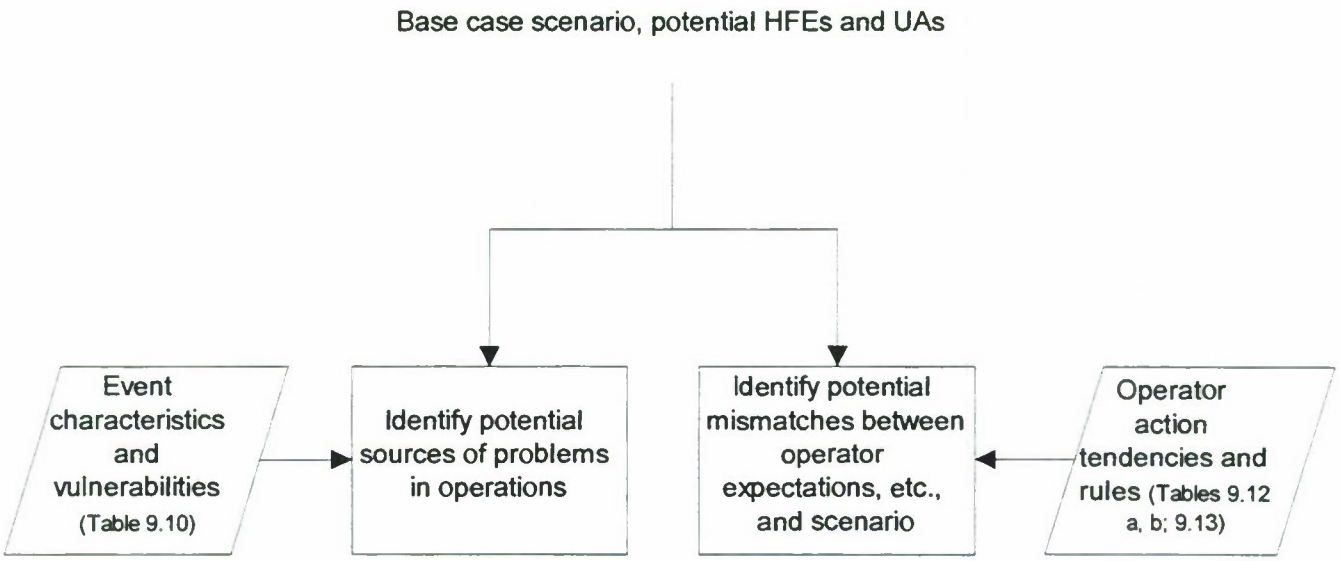


Figure 9.4 Step 5 - Identify Potential Vulnerabilities

9.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

Potential vulnerabilities in operator expectations can be anticipated by examining the characteristics of the initiating event in two different ways:

(1) with respect to operator biases that may triggered
(2) with respect to whether the initiating event is categorized as a direct or indirect initiator

Reason (Ref. 9.4) has identified two particular kinds of *heuristics*[6] having particularly powerful effects on people when they must make decisions about events, which in turn can affect the kinds of choices operators make during abnormal conditions. These are the *representativeness heuristic* and the *availability heuristic* (see the glossary for further explanations). These two heuristics lead to specific biases that affect the choices people make. The three most common biases associated with these heuristics that relate to control-room operations during abnormal conditions are:

[6] A *heuristic* is a way of mentally taking a shortcut in recognizing a situation and taking an action. Heuristics normally allow people to quickly select the most plausible choices first and the less plausible choices later.

- *Recency* operators are biased to recall or bring to mind events that have occurred recently or are the subject of recent operational experience, training, or discussions

- *Frequency* operators are biased to recall or bring to mind events that are frequently encountered in operations in situations that appear (even superficially) to be similar to the scenario being analyzed

- *Similarity* operators are biased to recall or bring to mind events that have characteristics (event superficial) similar to the scenario, particularly if the event brought to mind is a classic event used in training or discussed extensively by the operators

In later steps, these biases can be used to help identify, for example, the more likely incorrect situation assessments where operating crews may overlook or become preoccupied with particular parameters.

Different initiating events differ with respect to how recently and frequently they are encountered and how similar they may be to recent or frequent events. As a result, different operator biases, expectations, and behaviors will be more likely than others for a specific initiating event.

Table 9.10 incorporates this recognition by indicating what potential vulnerabilities may result from different event characteristics. To use Table 9.10, analysts first should review the base case scenario defined in Step 3 and the general event or initiator type for the scenario. (Examples of general event types are shown in the right-hand column of Table 9.10.) Then, the general event type for the base case scenario should be compared with the event characteristics shown in the left-hand column of Table 9.10. More than one event characteristic may apply to a specific scenario. Next, the analysts should identify the potential vulnerabilities associated with the event characteristics that apply to the base case scenario's general event type. Potential vulnerabilities include mismatches between the actual event and operator expectations for the event, mismatches between the actual event and the rules that operators expect to apply for the event, and events for which operator knowledge is limited and rules or training do not apply. Analysts should identify possible deviations from the base case scenario that would tend toward the vulnerabilities identified from the table. Finally, the analysts should describe the vulnerabilities and possible deviations as specifically as possible, so these descriptions can help guide the deviation analysis in Step 6.

In Step 2, direct and indirect initiating events were defined and discussed. For direct initiating events, the base case event sequences that follow the initiator are generally analyzed in the FSAR with an additional failure, and other conservatisms, and thermal-hydraulic analysis may be performed in support of the plant PRA. These scenarios are straightforward, following a predictable sequence of events if there are no additional failures or interventions. Therefore, they are well supported by emergency procedures and training. The expected and essential associated human actions are generally modeled in the HRA of the PRA. These events by themselves do not pose any

difficulties in operator responses. In order for scenarios involving HFEs that are triggered by direct initiating events to become significant contributors, some significant deviation in the physics of the base case must occur. The next step in the ATHEANA analysis examines a wide range of possible deviations. Those deviant scenarios that both introduce challenging cognitive situations and have potentially reasonable frequencies of occurrence (not negligible) are passed on for further ATHEANA analysis.

Indirect initiators, on the other hand, including support system initiating events (e.g., loss of service water and loss of instrument air) and environmental events (e.g., fires, floods, and earthquakes) often have four very troublesome characteristics:

- lack of specificity as to the cause and effects of starting events
- lack of detailed engineering analysis
- ill-defined dynamic progression
- lack of directly applicable EOPs that account for the systems and dependencies introduced by such events

For example, while there are extensive analyses of seismic capacity, fire protection, cooling water requirements, etc., they are all based on design rules. That is, if an earthquake produces no greater acceleration than the designed amount, the structures, systems, and components (SSCs) are assumed to function as designed. Or, if any single active failure occurs, a sufficient amount of equipment will have sufficient cooling to provide required safety functions. Also, unlike the direct initiating events, indirect events are more stochastic in nature. Because the accident progression following indirect initiators can be ill defined and dynamic, formal procedures may not provide complete operator guidance for responses to accidents. These types of events (e.g., failures of support systems that lead to initiators) can be outside the design basis, and associated procedural guidance often does not address the underlying cause(s) of the failure. Furthermore, operators are likely to expect the most benign of scenarios following an indirect initiating event (on a frequency basis) and therefore might be unaware or unwilling to believe the severity of a serious indirect initiating event. For indirect initiators, the operators may not have any expectations, or even if they do, there are so many possibilities that there is a good chance that their expectations will not be correct. This makes these types of events troublesome and such events should be investigated further in the next step. Although the base case scenario may already be outside operator expectations, a systematic process for identifying the characteristics of important deviations should be performed in the next step to define these scenarios.

Table 9.10 Event Characteristics and Potential Vulnerabilities

Event Characteristic	Potential Vulnerabilities	Example Event Types
General event type occurs relatively frequently.	Mismatch between actual event and what operators expect; mismatch between actual event and the informal and formal rules that the operators expect to apply; because event occurs frequently, a conditioned response is possible; or, response may become routine and may not account for deviations from expected scenario	Transients
General event type is trained for relatively frequently.	Mismatch between actual event and what operators expect; mismatch between actual event and the informal and formal rules that the operators expect to apply; because event occurs frequently, response may become routine and may not account for deviations from expected scenario	Transients, LOCAs
General event type represents a wide range of possible plant behavior.	Mismatch between actual event and the informal and formal rules that the operators expect to apply; operator expectations may be different than actual event.	Transients, LOCAs, support system failures, external events
General event type is rare and/or is trained for infrequently.	Rules and training may not apply or exist; operator knowledge and experience are limited.	Support system failures, external events
General event type is rare and/or cannot be trained for realistically (i.e., no simulator training).	Rules and training may not apply or exist; operator knowledge and experience are limited	Fires, low power and shutdown.
Event type encompasses a plant-specific operational problem that occurs relatively frequently over a period of time.	Mismatch between actual event and operator expectations; because event occurs frequently, conditioned response is possible; mismatch between actual event and the informal and formal rules that the operators expect to apply (because the rules do not provide guidance in the case of an event with the operational problem).	Examples of plant-specific operational problems: feedwater control, seasonal grass intrusions in service water intake structure.
General event type often involves initiator-induced or mode-induced dependent failure of equipment response.	Rules provide limited guidance on alternatives to and how to restore needed equipment.	Fires, other external events, shutdown operations, support system failures.

Table 9.10 Event Characteristics and Potential Vulnerabilities (Cont.)

Event Characteristic	Potential Vulnerabilities	Example Event Types
General event type typically or often requires ex-control room actions (beyond alignment of shutdown cooling with RHR, etc.).	Rules may require coordination and communication of multiple people in multiple locations under adverse and unfamiliar conditions; rules provide limited guidance on alternatives to and how to restore needed equipment.	Fires, other external events, shutdown operations, support system failures, low power and shutdown events.

9.5.2 Time Frames of Interest

A review of the reference case analysis will generally reveal natural time frames for the scenario with respect to plant behavior, plant symptoms, system response, and operator response. These usually align with the following phases of the scenario:

- initial conditions or pretrip scenario[7]
- initiator and nearly simultaneous events
- early equipment initiation and operator response
- stabilization phase
- long-term equipment and operator response

A concise presentation of these natural time frames can be helpful, exposing the bases for many of the equipment success criteria and clearly identifying periods of minimal and maximal vulnerability to inappropriate human intervention. Table 9.11 presents a useful display of the time frames associated with the base case scenarios of the loss of main feedwater and large LOCA examples of Appendices B and C. A comparison of the two examples makes it clear that the actual timing of the natural phases are scenario specific and, likewise, the likelihood of HFEs in these phases.

After the analysts have prepared a table of their own time frames of interest, similar to our Table 9.11, it should be posted on their blackboard, available for constant reference during the prospective analyses of Step 6. It will be especially useful in keeping in mind the base case sequence of events, their timing and possible vulnerabilities in equipment success criteria and human responses as deviations from the base case are considered, as well as the potential for particular contexts disrupting information processing by the operators. After deviant scenarios are identified in Step 6, a comparison with the respective base case time frames will point the way to fruitful selection of HFEs, unsafe acts and error-forcing contexts.

[7] For starting event initiators, the pretrip phase may be a complex scenario itself.

Table 9.11 Relevant Time Frames for the Examples of Appendices B and C

Time Frame	Loss of Main Feedwater (MFW) Scenario, Appendix B		Large LOCA Scenario, Appendix C	
	Major Occurrences	**Influences on/by Operators**	**Major Occurrences**	**Influences on/by Operators**
Initial conditions	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention
Initiator or/ simultaneous events	Loss of MFW Reactor scram or turbine trip	Operators may identify MFW problems and manually trip the plant.	Reactor power prompt drop Pressure drops below safety injection (SI) initiation point	These events are over before the operator even recognizes what is happening
Early equipment initiation and operator response	0-2 minutes Auxiliary Feedwater (AFW) start SG pressure control per blowdown Other auto equipment responses	Operators verify initial responses per EOPs; particularly, AFW start in this case. Operators may even manually start AFW before it auto starts.	0-20 seconds Break flow is complete Pressure drops to essentially zero Containment pressure has peaked and is falling ECCS flow begins Accumulator flow occurs	During this time frame the operator is checking parameters and ensuring that appropriate standby equipment has started. Some early decisions in the EOPs may have occurred.
Stabilization phase	2 minutes - 1 hour Heat sink restored (SG levels and pressure) Plant conditions restabilize Some throttling and shutting down of equipment (e.g., AFW) begins	Operators likely to throttle and even shut down some AFW pumps to avoid overcooling or respond to lack of cooling (& enter other EOPs) if heat sink apparently not restoring. Perform other actions as necessary (e.g., pressurizer heater on or off) to keep plant stabilized.	1-3 minutes Core reflood begins at about 30 seconds and has reached stable conditions Fuel temperatures have peaked and are falling	During this time, the operators have moved into the LOCA EOP and have passed a number of decision points.
Long-term equipment and operator response	>1 hour Unnecessary equipment shutdown Achieve hot or cold shutdown	Operator shuts down unnecessary equipment and transitions plant to hot or cold shutdown.	Isolation of the accumulators Shift to cold leg recirculation cooling Shift to hot leg recirculation cooling Repair and recovery	During the 20 minutes until switchover to cold leg recirculation cooling, the operators are occupied with confirmatory steps in the EOPs. Any complications beyond the base case scenarios can affect their performance. This longer time frame extends to days and months. There are no critical operations concerned with the base case scenario. Problems during this phase would be the concern of a low-power and shutdown PRA.

9.5.3 Operator Tendencies and Informal Rules

Tables 9.12a and 9.12b show the typical, required types of actions (called "operator action tendencies") for off-normal conditions of key functional parameters typically used to determine plant status. These operator action tendencies are based on the formal emergency and abnormal operating procedures and related training that is received, as well as informal practices and rules that are also part of the operator psyche. In Table 9.12a, a representative summary is provided, based on a review of typical pressurized water reactor (PWR) emergency procedures. The table should be useful for most PWRs. Table 9.12b provides a similar summary for boiling water reactors (BWRs). However, since the operator action tendencies shown in these tables should be considered generic, plant-specific rules should be reviewed to verify and supplement these actions.

In considering operator tendencies, the analysts should identify those tendencies that may lead to the HFEs or UAs of interest and the corresponding plant conditions that may lead to those tendencies. The plant conditions can therefore potentially set up the operators to follow the tendencies and so should be examined as part of the next step in the ATHEANA process.

In addition, in this step, the analysts should identify any informal rules that may be relevant as possible contributing factors to inducing the HFEs or UAs of interest. For example, an informal rule may exist among the operating staff that a certain indicator should not be trusted since it often sticks and thus reads incorrectly during dynamic situations. If the analysts can identify a way that following this or other informal rules could contribute to an error-forcing context that might induce an HFE or UA, this should be identified as a potential vulnerability and examined further in the next step of the process.

Table 9.13 provides examples of informal rules to assist the analysts in identifying such rules for their specific plant. The examples are broken down into three categories of possible operator activity: plant interventions (e.g., selection of unsafe actions), information processing (e.g., monitoring), and understanding of plant conditions and configurations (e.g., equipment status). The possible source of the informal rule (e.g., training, experience) is shown. The examples indicate what aspects of the operators' knowledge base may be the source of an informal rule. Consequently, the possible sources can guide analysts in discovering (probably through interviews of operators and operator trainers) what informal rules may be used.

9.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

The evaluation of formal rules and emergency operating procedures begins by tracking those elements of the EOPs (or other formal rules) that are most relevant to the scenario. (See Ref. 9.5 for a related approach.) A flowchart or logic diagram format can be used to accomplish this tracking, distinguishing between procedure steps in which decisions are made and steps where actions,

Table 9.12a Summary of Operator Action Tendencies (PWRs)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Plant Level: Reactor power	Too high or increasing	Rods in or Emergency borate (inject)
Turbine/generator load	Not tripped	Trip / Run back /close main steam valves
Key Supports: Electric power	Partial or total loss	Restore (use emergency diesels if necessary) or realign
Instrument air	Partial or total loss	Restore or realign
Cooling water systems	Partial or total loss	Restore/realign/augment
Reactor Coolant System (RCS) (primary): Pressurizer (RCS) level	Too low or decreasing	More RCS injection or less letdown
	Too high or increasing	Less/stop injection or more letdown
Pressurizer (RCS) pressure	Too low or decreasing	More RCS injection / isolate possible LOCA paths / stop pressurizer sprays and turn on heaters / decrease cooldown
	Too high or increasing	Turn on pressurizer sprays and turn off heaters / increase cooldown / provide relief with pressure operated relief valves ((PORVs), vents)
Core heat removal (e.g., T_{avg}, core outlet temps, subcooling)	Too low or decreasing (insufficient)	Increase RCS forced flow (unless voiding evident) / more RCS injection / increase cooldown
	Too high or increasing (overcooling)	Decrease RCS forced flow / less/stop injection / close any open PORVs/vents / decrease cooldown
Steam Generators - S/G (secondary): S/G Level	Too low or decreasing	More S/G feed (i.e., increase cooldown) / use feed and bleed
	Too high or increasing	Less S/G feed (i.e., decrease cooldown) / possible isolation of main steam
S/G Pressure	Too low or decreasing	Decrease steam dump (i.e., decrease cooldown) / isolate (especially if high radiation indicative of tube rupture)
	Too high or increasing	Increase steam dump or provide main steam relief (i.e., increase cooldown)
Containment: Containment pressure	Too high or increasing	Increase fan cooling / isolate containment / containment spray
Containment temperature	Too high or increasing	Increase fan cooling / isolate containment / containment spray
Radiation	Indicating	Isolate source or area

Table 9.12a Summary of Operator Action Tendencies (PWRs) (Cont.)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Ventilation	Too little or rising temperature	Regain / open doors/ use portable equipment
Other: Equipment condition	Signs of imminent damage (vibration, fluctuating current, high temperature)	Shut down or isolate

[a] This is defined relative to what is expected at the time in the scenario when the operator is responding to the functional parameter of interest. Note that the operator may respond to a parameter early in the event and again later in the event and so forth. The expected absolute reading or trend of the parameter could be different for the early and later responses. The off-normal condition is defined relative to each expectation at each time.

[b] It is recognized that the specific actions will depend on the absolute reading and rate of change in the parameter and the specific procedural guidance for the conditions observed. These are, however, the typical types of actions that are called out to be performed, depending on the specific circumstances.

Table 9.12b Summary of Operator Action Tendencies (BWRs)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Plant Level: Reactor power	Too high or increasing	Rods in / emergency borate/ level-power control
Turbine or generator load	Not tripped	Trip / Run back / close steam valves
Key Supports: Electric power	Partial or total loss	Restore (use emergency diesels if necessary)/realign
Instrument air	Partial or total loss	Restore or realign
Cooling water systems	Partial or total loss	Restore/realign/augment
Reactor Pressure Vessel: Level	Too low or decreasing	More vessel injection / depressurize /vessel flooding/ isolate containment / containment flooding
	Too high or increasing	Reduce feedwater or less-stop injection
Pressure	Too high or increasing	Provide relief (turbine bypass, safety relief valves (SRVs)...)

Table 9.12b Summary of Operator Action Tendencies (BWRs) (Cont.)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Containment: Suppression pool temp.	Too high or increasing	Suppression pool cooling sprays or depressurize
Suppression pool level	Too high or increasing	Use pool drains / terminate external injection / depressurize
	Too low or decreasing	Provide pool makeup or depressurize
Drywell pressure	Too high or increasing	Isolate LOCA and containment / drywell spray / venting / depressurize
Drywell temperature	Too high or increasing	Increase drywell cooling / drywell spray / depressurize
Radiation	Indicating	Isolate source/area / depressurize
Ventilation	Too little and/or rising temp	Regain / open doors/ use portable equipment
Other: Equipment condition	Signs of imminent damage (vibration, fluctuating current, high temperatue)	Shutdown / isolate

[a] This is defined relative to what is expected at the time in the scenario when the operator is responding to the functional parameter of interest. Note that the operator may respond to a parameter early in the event, and again later in the event, and so forth. The "expected" absolute reading or trend of the parameter could be different for the early and later responses. The off-normal condition is defined relative to each expectation at each time.

[b] It is recognized that the specific actions will depend on the absolute reading and rate of change in the parameter and the specific procedural guidance for the conditions observed. These are, however, the typical types of actions that are called out to be performed depending on the specific circumstances.

monitoring, or verification is performed. Examples of such flowcharts are contained in Appendices B through E. Note that this simplified flowchart is not meant to duplicate the EOPs. However, it does highlight:

- the location of branch points from the most applicable procedure to other procedures
- where specific steps exist that call for stopping equipment that is particularly germane to the scenario
- where a major reconfiguration of equipment is called out

The EOPs or other formal rules define the expected responses the operators will take, depending on the scenario progression. However, the above points in the EOPs could be particularly vulnerable to operator error so that a "wrong" procedure is entered, or equipment is shut down or reconfigured inappropriately. Therefore, at each decision point or where otherwise deemed beneficial, information is provided that summarizes the following to provide clues as to possible pitfalls:

Table 9.13 Examples of Informal "Rules" Used by Operators

How operators use rules	Informal[a]	
	Training	Other Sources of Informal Rules
Plant Interventions		
Selection and justification of unsafe action(s)	Keep core covered Always follow your procedures Don't go solid in pressurizer	Good Practice Protect pumps (e.g., stop if no lube oil pressure, no cooling, runout, deadheaded, cycling) Old Practice Safety injection (SI) on low pressurizer level Folklore A good operator always beats autoactuation Never feed water into an overheated vessel Conflict Alternatives have negative consequences Success seems imminent
Information Processing		
Monitoring[b] (i.e., what indications to monitor, when to monitor, etc.)	Which instruments to use Which (and in what order) to respond to alarms Check redundant indications (especially alarmed conditions)	Experience Which instruments to use (may not be all that are available)
Interpretation (part of situation assessment)	Believe your indications	Good practice Question diagnoses (e.g., if unexpected response, restore your last action) Experience (plant-specific) Some indications are more reliable than others. Some indications always give false readings. Recent history of plant/equipment/instrument performance
Understanding Plant Conditions and Configurtions		
Equipment status	Indications of performance. Believe your tagout system	Folklore Pumps in runout overspeed Multiple failures in one system are not possible

Table 9.13 Examples of Informal "Rules" Used by Operators (Cont.)

How operators use rules	Informal[a]	
	Training	Other Sources of Informal Rules
Instruments/indications	Instruments are very reliable	Folklore Indication readings correspond directly with actual plant state or behavior Indications are independent

[a] Including training, guidance for good operating practice, old practice (i.e., previous operating practice), experience, invented rules of thumb (referred to as "folklore").

[b] Including both data-driven and knowledge-driven monitoring.

- actions to be taken
- potential for ambiguity
- a judgment on the significance of taking the wrong branch or inappropriate action.

Existing EOP flowcharts may be used or extended for the purposes of this activity. For example, some vendor emergency guidelines, which form the basis for emergency operating procedures, contain procedure flowcharts. Also, similar diagrams may have been developed as part of previous PRA or HRA efforts (e.g., Refs. 9.5, 9.6). Since development of these flowcharts may be time-consuming, use of existing work is preferable. Unless the procedures are changed, the flowcharting has to be done only once.

9.5.5 Product of Step 5

The product of Step 5 is a summary or aggregation of the information collected in this step. As we proceed into the searches of Step 6, the analysts keep all of this information at hand, i.e., on their blackboard, available for ready reference at each stage of the searches. Using this information, the analysts can identify potential vulnerabilities. In turn, the analysts can use these potential vulnerabilities as guides to the more fruitful aspects to search when developing deviations from the base case scenario in the next step.

9.6 Step 6: Search for Deviations from the Base Case Scenario

The record has shown that no serious accidents have occurred for a base case (or expected) scenario. On the contrary, past experience indicates that only significant deviations from the base case scenario are troublesome for operators. Thus, in Step 6, the analysts are guided in the identification of deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). In serious accidents, these deviations are usually combinations of various types of unexpected plant behavior or conditions. Categories of such plant deviations are given below.

9.6.1 Overview of Step 6

The search schemes in this step guide the analysts in finding physical or "physics" deviations. These are real deviations in plant behavior and conditions. In contrast, deviations in perceived plant behavior and conditions, whether due to indicator failures or failures in operator perception, are addressed in Step 7. Analysts may identify performance-shaping factors (PSFs) and explanations for human behavior (e.g., error mechanisms) along with these plant conditions. The combination of plant conditions (including the deviations), along with resident or triggered human factors concerns, defines the error-forcing context (EFC) for a human failure event that is composed of one or more unsafe actions. The next step, Step 7, builds upon or refines this initial EFC definition by identifying other possible complicating factors (including possible hardware failures) and resident or triggered human factors concerns (e.g., mismatches between deviant plant behavior or conditions and procedures or other job aids).

There are three possible outcomes from this and the next step that would result in scenarios and EFCs that are passed on for further analysis in the recovery and quantification steps:

(1) The EFC is strongly defined by physical deviations (i.e., Step 7 is not needed to define the EFC).

(2) The physical context is reasonably strong, but the frequency is low. However, there are similar scenarios with higher frequencies.

(3) The physical context is not severe enough to make the HFEs or UAs likely, but additional factors (such as additional hardware or indications failures identified in Step 7) could create an EFC.

Figure 9.5 illustrates the tasks and task flow for this step. Four search schemes are used to identify characteristics that should be contained in a deviation scenario:

(1) Identify physical deviations from the base case scenario (e.g., how can the initiator be different?)

(2) Evaluate rules with respect to possible deviations

(3) Use system dependency matrices to search for possible additional causes of the initiator or the scenario development

(4) Identify what operator tendencies and error types match the HFEs and UAs of interest.

After each of the search schemes has been exercised, the analysts should review and summarize the characteristics of a deviation scenario (or potentially important deviations) that were identified in the searches. With these combined results, the analysts then develop descriptions of deviation

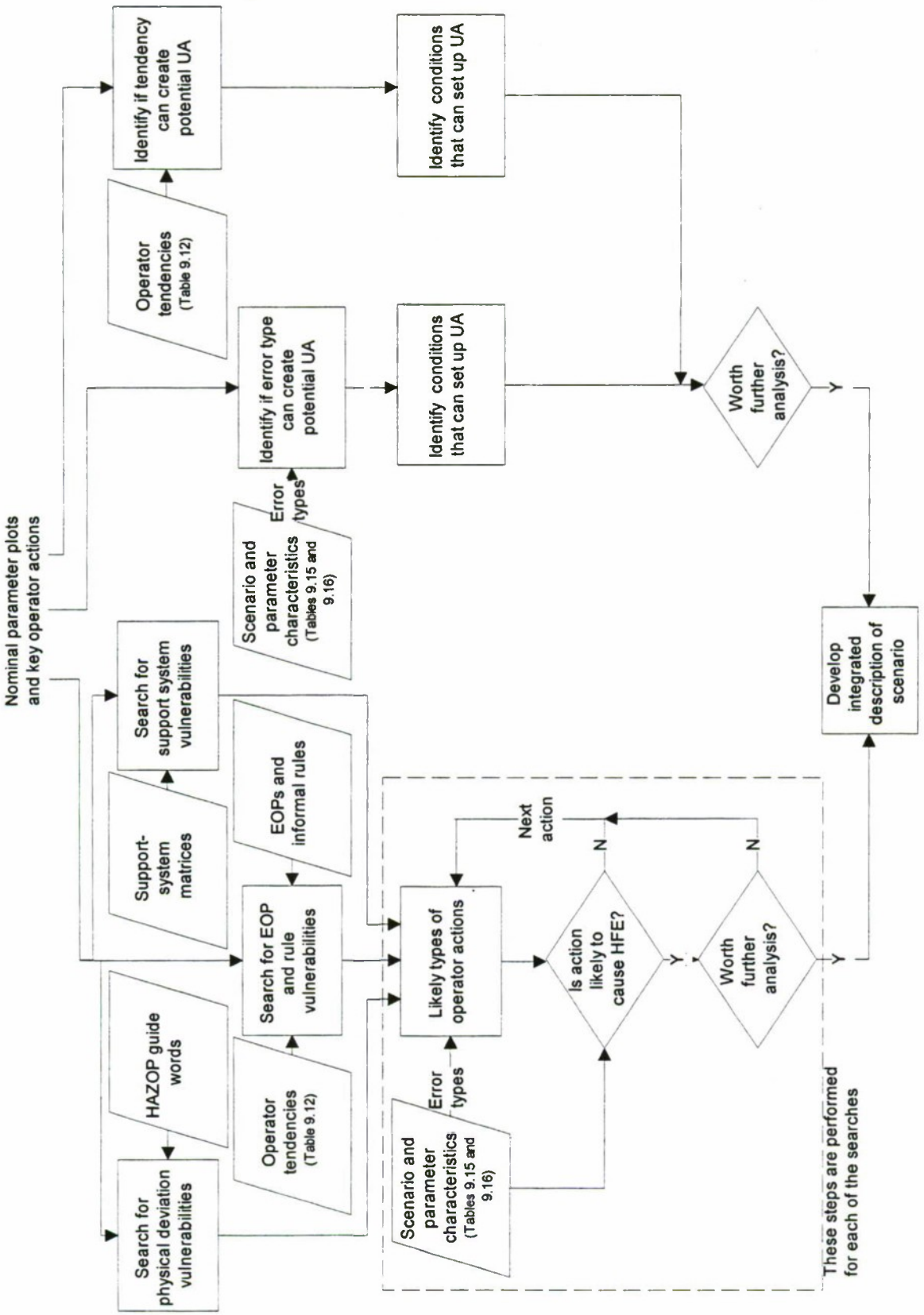


Figure 9.5 Step 6 - Search for Deviations from Base Case Scenario

scenarios and associated HFEs or UAs. These deviations also become the initial error-forcing contexts for the HFEs or UAs.

The search schemes are not wholly independent. In general, all search schemes should be tried, and in the order given above. However, the different schemes are not equally fruitful for different classes of initiating events (or for direct versus indirect initiating events). Because of built-in redundancies in the search schemes, the fourth search, or "operator tendencies and error types" search, can be viewed as a sort of catch-all search that may identify deviations that eluded the previous searches. Also, the first three searches identify plant conditions and rules (i.e., aspects of the plant) that are deviation characteristics first, then try to identify possible error types or operator tendencies (i.e., aspects of the human) that are associated with these characteristics. In the fourth search, the approach is reversed; possible error types and operator tendencies that could cause HFEs or UAs of interest are identified first, then the plant conditions and rules associated with such inappropriate operator responses are identified. A happy consequence of the redundancies in the search schemes is that analysts should not be surprised if the same deviation characteristics are identified using different search schemes or if different analysts find the same or similar deviations using different search schemes.

Each of the four search schemes for identifying physical deviations is described below. However, the common tools or resources that underlie these schemes are described first.

9.6.2 Tools Underlying the Search Schemes

As noted above, the four search schemes for identifying physical deviations are not independent. Part of this dependency, or redundancy, is by design to help the analysts in identifying significant deviations. Variations in how the search schemes are applied (see Appendices B through E for examples) also account for some of this dependence. Finally, the same tools or information underlie all four schemes, although they are used differently in the different schemes.

These tools or information resources are:

- the identified potential vulnerabilities from Step 5
- EOP flowcharts
- operator tendencies
- informal rules
- support system dependencies
- human information processing tendencies or characteristics
- familiarity with thermal-hydraulic response

The use of EOP flowcharts, operator tendencies, and informal rules was introduced in Step 5. The identification of physical deviations performed in this step expands upon those tasks. Understanding of plant thermal hydraulics also was important to the performance of previous steps (as well as

previous PRA studies). The two other tools are new to the process. The investigation of support system dependencies is an extension of that which has been performed for many PRAs already. The investigation of human information processing tendencies allows the potential for human vulnerabilities to guide the analysts to physical deviations that may be particularly troublesome for operators.

9.6.3 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

Three tasks are performed in this first search:

(1) Guide words are used to identify and define how the scenario may deviate from the base case.

(2) Relevant EOPs are checked for technical validity for the identified deviations.

(3) Possible error types or inappropriate operator response are identified by matching the plant conditions associated with identified deviations.

The example analyses given in Appendices B through E can be used as a guide for performing this search.

This first search begins by using guide words to identify and define how the scenario may deviate from the base case, thereby causing complexities that may contribute to EFCs. While the focus of this search is on deviations from the initiator in the base case, the analysts should not limit this search if deviations associated with subsequent accident responses are discovered. The use of guide words is common in other types of safety investigations, especially HAZOPs (HAZard and OPerability studies) performed in the chemical processing industry (see, for example, Ref. 9.7). Since the guide words are used only to stimulate the analysts' thinking, it is not particularly important how or by what guide words deviations are identified.

The following is a list of suggested guide words that seem appropriate for the identification of physical deviations and a very basic interpretation of each guide word:

Guide Word	Meaning
No or not	A deviation that negates the base case scenario
More	A deviation that represents a quantitative increase
Less	A deviation that represents a quantitative decrease
Late/never/early	A deviation that represents a change in expected timing
Inadvertent	Same as "as well as"
Too quick/slow	A deviation that represents a change in the expected speed or rate
Too short or long	A deviation that represents a change in the expected duration
As well as	A deviation in which something in addition to the base case occurs
Part of	A deviation in which only some of what is expected occurs

Reversed	A deviation that is the logical opposite of the base case
Repeated	A deviation that represents a repetitiveness of what is expected

Note that this list is degenerate for some scenarios (e.g., under LLOCA IE "more" = "early" = "quick" = "short"). Also, the analysts are likely to find that a short set of guide words is easiest to use.

Considering the potential vulnerabilities identified in Step 5 (Section 9.5.1), the analysts should apply the suggested guide words to the initiating event or the scenario as a whole to determine whether changes in the initiator or scenario (i.e., deviations) could result in operator actions relevant to the HFEs or UAs of interest. Illustrations of how these guide words are applied are shown in the example analyses in Appendices B through E. In applying each guide word, the analysts identify how the initiator or overall scenario could be different from the base case (i.e., a possible deviation) as suggested by the guide word, as well as the potential significance of each deviation. Based on their reasonableness and potential significance, those deviations that could seemingly contribute to an overall context that might induce the HFEs or UAs of interest are reviewed even further.

For the physical deviations that are identified, the analysts then should ask if the deviation could be caused by a single operator activity, particularly a "slip"or "lapse" that is difficult to recover or is unrecoverable.[8] Such actions may be caused by traditional human factors problems (e.g., human–system interface) or by operators misreading or misinterpreting indications. Regarding the misreading or misinterpretation failures, such misperception failures should not occur unless:

- the scenario progression is fast or confusing
- something about the misperception breaks down the team concept, encouraging independent action
- some other aspect of context has already broken down team communication
- confusion about the current state of the plant exists and one operator's misperception (or misdiagnosis) is accepted by all team members (see, for example, the Crystal River 3 event in Appendix A)

In addition, analysts may find the examples of psychological reasons for response implementation failures given in Table 9.14 generally helpful. The discussions given in Sections 4.1.4 and 4.3.4 also may be helpful in identifying possible slips or lapses and their justifying causes.

[8] Equipment can be defined as unrecoverable if it cannot be actuated in the time available because it is locked out, disabled, irreparably damaged by the operator action, or otherwise precluded from operation by conditions following the operator action. The identification of unrecoverable failures will rely upon the analysts' knowledge of scenario timing and hardware and system design, dependencies between systems and equipment, operator controls, etc.

After the characteristics of deviations have been identified using the guide words, the analysts should evaluate these, characteristics against relevant procedures to identify whether strict compliance with the procedures and the formal rules (rules defined in training as part of the expected response strategy for the scenarios) will lead to any HFEs because of timing or parameter-value mismatches with the assumptions in the procedures. If no mismatches are identified from the evaluation, then the procedures are technically correct. If mismatches are identified, the procedures are **not** technically correct. Such mismatches should be analyzed in a later step as an initial EFC (although analysts should complete the remaining searches in this step to identify other potentially significant deviations).

Finally, the analysts should identify which UAs and HFEs of interest are supported by the deviation characteristics identified. For each deviation characteristic identified with the guide words, the analysts should review Tables 9.12a or 9.12b (from Step 5), Tables 9.15a and b (scenario characteristic tables), and Tables 9.16a and b (the parameter characteristic tables). While the results obtained using these tables are similar, the structure and content of the tables are different. Consequently, the reviews of Tables 9.12, 9.15, and 9.16 are described separately below. Note that Tables 9.15 and 9.16 are found at the end of Section 9. A discussion of the underlying basis for the use of these tables is presented in Section 4.4.

Table 9.14 Failures in Response Implementation

Failures in Response Implementation	Search Questions to Identify EFC elements
Operators use incorrect indications, displays or controls	
• Displays separated from controls	Under what plant conditions must operators use controls that are separated from the related parameter displays and indications?
• Relevant displays and controls not easily identifiable (particularly ex-control room)	Under what plant conditions must operators use displays or controls that are not easily identifiable, such as being limited to a small number of CRTs or using poorly labeled local indicators or controls? Under what conditions are operators called on to use indicators or controls where the labels are unclear or wrong?
• Controls normally used in other contexts with other displays	Under what conditions must operators use indicators or controls that are located among similar-looking groups? Can the operators be required to use controls that are usually used in different operational contexts? In these cases it is possible for operators to inadvertently use the controls in the way that is normal for these other contexts but that is inappropriate under the accident conditions.

Table 9.14 Failures in Response Implementation (Cont.)

Failures in Response Implementation	Search Questions to Identify EFC elements
Operators use controls or read displays incorrectly • Controls operate in nonstandard manner • Displays have non-standard scales or display modes	Under what plant conditions must the operators use controls that have non-stereotypical operating modes? • "On" or "open" to the left • "Up" or "increase" to the left Under what plant conditions must the operators use displays that have nonstereotypical indicating modes? • "Up" or "increase" to the left Under what plant conditions must the operators use displays that have multiple display ranges? Under what plant conditions must the operators use displays that have multiple display modes (e.g., CRT displays)?
Multiple operators unable to perform task • Operators not available • Coordination not available or ineffective • Communications not effective between operators	Under what plant conditions can there be insufficient operators available to perform all the necessary tasks? • Operators performing other tasks Under what plant conditions can the response coordinator be preoccupied with performing other tasks? For what plant conditions can the coordinator be insufficiently trained? Under what conditions can the communication system be inoperable? Under what plant conditions can the communication system be unavailable? Under what conditions can the communication system be ineffective? • Blackout spots • High ambient noise Under what conditions can nonstandard or ineffective language pose a particular problem in operations (e.g., similar-sounding names and equipment numbers)?

In Tables 9.12a and 9.12 b (for PWRs and BWRs, respectively), key functional parameters and off-normal conditions in these parameters are related to operator action tendencies. The analysts should match each deviation characteristic with the affected functional parameters and off-normal conditions that best describe the deviation. Once a match is identified, then the tables show the analysts what operator tendencies are possible. Finally, the analysts should determine if the identified operator tendencies represent HFEs or UAs that are relevant to the issue of interest.

In Table 9.15a, descriptions of the scenario are related to categories of scenario characteristics. The analysts should match each deviation characteristic identified earlier in this step with the scenario descriptions that best describe the deviation. If a match is identified, then the analysts can use Table 9.15b to identify what error types are possible. In turn, the analysts should determine if any of the identified error types correspond to any of the HFEs or UAs that are relevant to the issue of interest.

Finally, the analysts should identify what error mechanisms are associated with the relevant error types. From the possible error mechanisms, the analysts should try to determine which error mechanisms might be applicable for the HFE or UA, associated plant conditions, and specific plant. (The analysts may find themselves thinking ahead to additional plant conditions, PSFs, informal rules, or other plant-specific features that might activate certain error mechanisms. Step 7 specifically addresses consideration of PSFs and additional plant conditions. As always, such thinking ahead is encouraged.)

Similarly, in Table 9.16a, questions to identify parameter characteristics relevant to the scenario are provided for three of the four information processing stages.[9] These parameter characteristics could have particular influences on operators and whether a UA may result. The analysts should review the parameter characteristics and associated questions for all three of the information processing stages addressed in Table 9.16a to determine which parameter characteristics or information processing stage best describes the above-identified deviation characteristics. If a match is identified, then the analysts can use Table 9.16b to identify possible error types for the parameter characteristic and associated information processing stage. Next, the analysts should determine if the identified error types correspond to any of the HFEs or UAs that are relevant to the issue of interest. Finally, the analysts should identify what error mechanisms are associated with the relevant error types. From the possible error mechanisms, the analysts should try to determine which error mechanisms might be applicable for the HFE or UA, associated plant conditions, and specific plant. Several aspects of Tables 9.15a and b and 9.16a and b should be noted. These tables provide analysts with a set of error types and mechanisms that may be relevant, given certain scenario characteristics, and provide some guidance for identifying (in Step 7) which PSFs may be particularly relevant when certain scenario characteristics and error mechanisms are likely to be operative. There is no assumption that the tables are all encompassing or that there are necessary and precise relationships among their elements. For example, it is not necessarily the case that a particular error mechanism will be associated with an identified characteristic or that a particular PSF will be related to a certain error mechanism. Thus the tables are to be used as guidance for possible factors and relationships to be considered rather than a specification of the precise relationship among factors.

9.6.4 Search of Relevant Rules

Paralleling the first search, three tasks are performed in this second search:

(1) Decision points in relevant formal and informal rules are evaluated against the deviations identified in the first step.

(2) Relevant EOPs are checked for technical validity for the identified deviations.

---

[9] It is assumed that the impact of parameter characteristics on the operators would be negligible during the fourth stage, response implementation.

(3) Possible error types or inappropriate operator responses are identified by matching the plant conditions associated with identified deviations.

Because the second and third tasks in this second search are identical to those performed in the first search, a description is not repeated here. The example analyses given in Appendices B through E can be used as a guide for performing this search.

This second search begins by duplicating the evaluation performed in Step 5, Section 9.5.4. However, in this case, decision points in relevant formal and informal rules are evaluated against the deviation characteristics identified in the first search of Step 6, rather than the base case scenario. The analysts also should identify plant conditions that represent deviations from the base case scenario that might trigger the use of formal or informal rules in ways that would lead to unsafe actions.

9.6.5 Search for Support System Dependencies

Paralleling the first two searches, three tasks are performed in this third search:

(1) Dependency matrices are reviewed and expanded to identify support system failures that also could lead to the deviation characteristics identified in the previous searches.

(3) Relevant EOPs are checked for technical validity for the identified deviations.

(3) Possible error types or inappropriate operator responses are identified by matching the plant conditions associated with identified deviations.

Because the second and third tasks in this search are identical to those performed in the first search, a description is not repeated here. The example analyses given in Appendices B through E can be used as a guide for performing this search.

The accident record has shown that serious events can be influenced by support system dependencies. For example, the event at TMI-2 was initiated by the closure of FW valves which, in turn, was caused by moisture intrusion in the instrument air system. Consequently, one potentially useful method of searching for plant conditions that produce error-forcing contexts is to investigate dependencies between support systems and both frontline safety systems and normally operating systems.

The significance of such dependencies is twofold:

(1) If the system or function failure that resulted in the reactor trip also is required post-trip, a complicated or unexpected support system dependency influence may complicate or delay operator response.

(2) The support system failure that ultimately caused the reactor trip may cause additional failures in responding systems (e.g., safety systems) that are complicated, unexpected, and difficult to diagnose, thereby affecting operator response.

Many IPEEEs and PRAs included dependency matrices as part of their documentation. Using and expanding upon these dependency matrices may be an effective way for investigating support system dependencies. For front-line safety systems, such dependency matrices may be sufficiently complete if they go down to the component level. However, dependencies between support systems and normally operating systems may not be addressed. So the analysts would need to expand the existing dependency matrix to include those component failures in normally operating systems that could be caused by support system failures. Probably the only normally operating systems that need to be added are those that, if failed, would require the reactor to trip.

Once the support system dependencies are identified, the analysts investigate what possible events might have resulted in the support system failure. In particular, the analysts should identify those failure causes that could have widespread effects on not only the system that failed and caused the reactor trip but also on frontline safety systems that are required for accident response.

As in the physics search described in Section 9.6.3, the analysts should investigate if there are any unrecoverable slips or lapses that could cause the plant conditions associated with the deviation characteristics identified through this search.

9.6.6 Search for Operator Tendencies and Error Types

As mentioned in Section 9.6.1, this fourth search is conducted essentially in reverse, compared with the first three searches. In other words, the first three searches identify plant conditions and rules (i.e., aspects of the plant) that are deviation characteristics first, then try to identify possible error types or operator tendencies (i.e., aspects of the human) that are associated with these characteristics. In this fourth search, the approach is reversed; possible error types of operator tendencies that could cause HFEs or UAs of interest are identified first, then the plant conditions and rules associated with such inappropriate operator responses are identified. This fourth search also can be considered a sort of catch all for deviation characteristics that might have eluded the previous searches.

This fourth search consists of two tasks:

(1) Operator tendencies that match HFEs or UAs of interest are identified
(2) error types that match HFEs or UAs of interest are identified.

In both tasks, the final activity is to identify the plant conditions and rules that can lead to the relevant tendencies and error types that are identified.

In addition, this search uses the tendencies and vulnerabilities uncovered in Step 5 and searches for deviations that would trigger those tendencies that would result in unsafe actions for the scenario.

As in the previous searches, the example analyses given in Appendices B through E can be used as a guide for performing this search.

First, the operator tendencies shown in Tables 9.12a or 9.12b (for PWRs or BWRs, respectively) should be reviewed. The tendencies that are relevant to HFEs or UAs of interest should be identified. For the relevant tendency (or tendencies), then look at Table 9.12a or 9.12b to find what key functional parameters and associated off-normal condition(s) correspond with the tendency (or tendencies). The analysts may need to translate these functional parameters and off-normal conditions, which are stated in generalized plant terms, into more specific conditions that relate to the scenario being examined. Then the analysts should try to identify how the plant conditions could be created so that the operator tendency (tendencies) is activated. The plant conditions specific to the scenario being investigated, and how these conditions are created, describe a deviation from the base case scenario that could lead to the tendency (or tendencies) of interest.

The search for error types is conducted in a similar way. First, the error types column in Tables 9.15b and 9.16b are reviewed. This review should focus on identifying any error types that match any of the HFEs/UAs of interest and that have not already been identified in the previous deviation searches in Sections 9.6.3, 9.6.4, or 9.6.5. For matches, the error mechanisms associated with the relevant error types should be identified. Next, the associated description of plant behavior (in the leftmost column of Tables 9.15b and 9.16b) should be identified. In the case of Table 9.15a, the generalized plant behavior is categorized by scenario characteristics. For Table 9.16b, generalized plant behavior is categorized by parameter characteristics. In both cases, the analysts should use these categories of characteristics in Tables 9.15a and 9.16a, respectively, to identify a general description of the scenario deviation. In Table 9.15a, a scenario description is used to generally describe the important scenario deviation. Using these general descriptions, the analysts should try to identify what realistic deviations from the base case scenario (in terms of both plant conditions and rules) could cause the plant behavior described in the leftmost column of Table 9.15a.

Such deviations also must lead to the associated error type given in Table 9.15b. In Table 9.16a, questions associated with the parameter characteristics are provided to lead the analysts to relevant deviations. The analysts should use these questions try to identify what realistic deviations from the base case scenario (in terms of both plant conditions and rules) could cause the plant behavior described in the leftmost column of Table 9.16a and the associated error type given in Table 9.16b. If plant conditions are identified, then the analysts should try to identify which of the possible error mechanisms might be activated for the relevant error types. (As in Section 9.6.3, the analysts may find themselves thinking ahead to what additional plant conditions, performance-shaping factors, etc. might activate error mechanisms, as well. Such thinking ahead is encouraged.) Table B-6 illustrates how this search for error types might be documented.

9.6.7 Develop Descriptions of Deviation Scenarios

In this task, descriptions of deviation scenarios are developed from the characteristics of deviation scenarios found in the four searches described above and guided by the potential vulnerabilities

identified in Step 5 (i.e., the information on the blackboard).

The analysts first should summarize all of the characteristics found in the four searches. These represent elements of error-forcing contexts (i.e., plant conditions, perhaps some PSFs, and supporting explanations for operator behavior associated with contextual elements).

Then the analysts should develop a scenario description that significantly deviates from the base case scenario and that would lead to the HFEs or UAs of interest. In order to develop the deviation scenario, the analysts should look at the summary of all the deviation characteristics identified and the vulnerabilities identified in Step 5, then ask the following questions:

- Which vulnerabilities identified in Step 5 are well supported by deviation characteristics?
- Can a reasonable scenario be developed that embodies as many of the deviation characteristics as possible?
- Are there any dependencies between the characteristics of the scenario?
- If there aren't any dependencies, is this scenario (thinking of the scenario as a chain of occurrences) so improbable as to be nonrisk significant (and therefore probably unrealistic)?
- If so, are fewer characteristics sufficient to define a deviation scenario?

Development of the deviation scenario requires knowledge about plant operations and thermal hydraulics so that the analysts can think up the chain of occurrences that will cause the parameter and equipment responses and timing of responses that match the deviation characteristics. The development of a deviation scenario also may be similar (although perhaps without the risk perspective) to that process used to develop simulator exercises by operator trainers. Consequently, the assistance of operator trainers and the plant simulator, if available, could be invaluable to this process. In earlier trials of the ATHEANA process, the operator training staff at a cooperating PWR plant assisted in the development of a deviation scenario. The plant's operator training staff used their knowledge, experience, and the plant simulator to develop, refine, and test the deviation scenario developed.

As indicated by the questions above, to the extent possible, analysts should try to incorporate multiple deviation characteristics that support the likely occurrence of the HFEs or UAs of interest. However, the analysts should try to avoid making up a deviation scenario that is so improbable that the HFE probability (that will be quantified in Section 10) is reduced to the point of insignificance. HFE probability can be reduced by the nature of or multiple characteristics. Consequently, the analysts may have to think ahead to the quantification task when developing a deviation scenario.

The analysts may find that multiple integration steps are required for developing the deviation scenario from the characteristics being used. For example, error mechanisms may have been

identified for each of the deviation characteristics, but the mechanisms identified may be degenerate, or only one or two mechanisms may be especially relevant in the global sense. As discussed in Section 9.6.3, the analysts may think ahead to what performance-shaping factors might be relevant or might be activated by the plant conditions. (Step 7 specifically addresses consideration of performance shaping factors.) If so, the analysts should try to identify which error mechanisms might be activated by these plant conditions and performance-shaping factors that define the deviation scenario.

In addition, the analysts may find that they have included some complicating factors (see Step 7) in the deviation scenario developed in this step. Such thinking ahead should not be discouraged. However, Step 7 still should be performed rigorously since the systematic search in this step may reveal factors that might not otherwise be thought of. An example of helpful ways to capture the results of Step 6 can be found in Section B.6.5 of Appendix B.

9.6.8 Products of Step 6

The products of Step 6 include the summary of the deviation characteristics found in the four searches and descriptions of deviation scenarios developed from the characteristics. The deviation scenario descriptions serve as an initial EFC that will be refined further in the next step.

9.7 Identify and Evaluate Complicating Factors and Links to PSFs

This step expands and further refines the EFC definition begun in Step 6. As shown in Figure 9.6, the analysts consider the following in this step:

- performance-shaping factors (PSFs)
- additional physical conditions, such as:
  - additional hardware failures, configuration problems, or unavailabilities
  - indicator failures
  - plant conditions that can confuse operators
  - factors not normally considered in PRAs

Like the previous section on developing the deviation scenario and EFC, this step may need to be performed iteratively with quantification (Step 10). In particular, the judgments that analysts will need to make regarding how many complicating factors to add to the EFC are best based upon quantification considerations (see Section 10.2).

If the EFC context identified in the previous step (i.e., Step 6) is judged to be sufficiently strong, then only PSFs triggered by this context (which, therefore, do not reduce the frequency or probability of the context) are identified in this step. If, on the other hand, the context identified in the previous step requires additional factors, then both categories of complicating factors are identified. Each category is discussed further below.

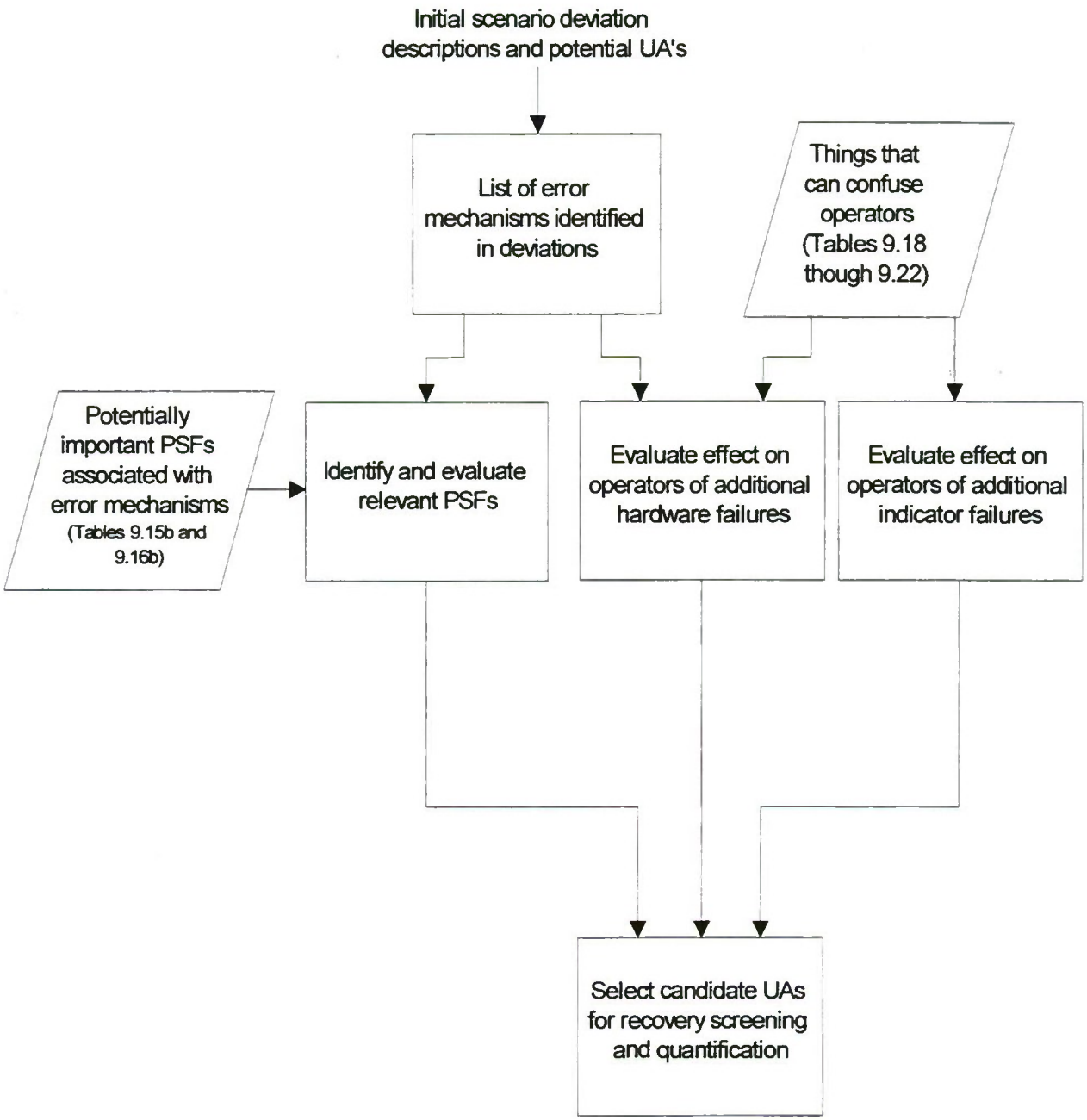


Figure 9.6 Step 7 - Evaluate Complicating Factors

9.7.1 PSFs

Because of the requirements of the various quantification methods that may be used in applying ATHEANA (see Section 10.2.2.2), the identification of relevant PSFs is an iterative step with quantification (if the issue of interest requires quantification). These are two types of PSFs that can add to the EFC initially defined in Step 6. These two types are:

- PSFs that are triggered by the already-defined context
- additional PSFs that are not specific to the context

PSFs that are triggered by the context identified in Step 6 include those that are linked to specific plant conditions and those associated with error types or mechanisms. Examples of triggered PSFs include:

- any relevant PSFs shown in the far right-hand column of Tables 9.15b and 9.16b that are associated with an identified error type or mechanism

- procedures that do not apply to the specific deviation scenario or are otherwise difficult to implement

- control panel layouts that make it difficult for operators to monitor plant status or perform required tasks in response to deviation scenarios (e.g., distributed control panels with shorter than the usual amount of time available)

- high operator workload because of multiple hardware failures, etc. in the deviation scenarios

In some cases, such as for the operator tendencies search in Section 9.6.6, the results of Step 6 may include only plant conditions and not error mechanisms. For these cases, analysts should look more globally for PSFs, using resources provided, such as the PSF list given above and the plant conditions that are used to describe the deviation scenario.

Additional examples can be found in Appendices B through E. Also, Section 5 provides examples of PSFs from operational experience in tabular form. Tables 5.1 through 5.4 provide a mixture of plant conditions and PSFs, while Table 5.5 provides principally PSF examples.

PSFs that are linked to specific plant conditions must be identified using knowledge of plant-specific design and operations as well as the description of the base case and deviation scenarios developed in the previous steps. In addition, the following is a list of commonly used PSFs and strategic factors that analysts can use to prompt their search for applicable PSFs:

- procedures
- training
- communication

- supervision
- staffing
- human–system interface
- organizational factors
- stress
- environmental conditions
- strategic factors such as multiple conflicting goals, time pressure, limited resources (see Section 4.2.3 for a discussion)

PSFs that are linked to error types or mechanisms specific to the deviation scenario context can be identified by reviewing Tables 9.15b and 9.16b. The far right-hand column in these tables provides lists of PSFs that are applicable for specific error types and mechanisms, given the context of the scenarios. If applicable error types or mechanisms were identified in Step 6 for the deviation scenario, the analysts should review the list of PSFs that apply to these error types or mechanisms. During this review, the analysts should determine if the PSF is applicable to the specific deviation scenario and the specific plant design and operation. Also, analysts should recall the note regarding the purpose and limitations of Tables 9.15a and b and 9.16a and b. For example, a particular PSF will not necessarily be related to a certain error mechanism. To repeat, the tables are to be used as guidance for possible factors and relationships to consider, as opposed to a specification of the precise relationship among factors.

In some cases, such as for the operator tendencies search in Section 9.6.6, the results of Step 6 may not include error mechanisms. For these cases, analysts should look more globally for PSFs, using resources provided such as the PSF list given above and the plant conditions that are used to describe the deviation scenario. PSFs identified in this way are context specific but have not been focused by an identified error mechanism.

The second type of PSF is identified through consideration of the deviation scenario definition and review of the list of PSFs. Examples of such PSFs (that are not specific to any deviation, although they can be plant specific) are:

- the impact of time of day on operator performance
- stress or workload (of nonspecific origin)
- general management directives or other guidance

The analysts are cautioned to be restrictive in adding PSFs that are not triggered or activated by the specific EFC. The point of addressing PSFs in this step is not to pile on a lot of PSFs or to address all possible PSFs. Rather, analysts should search for only those PSFs that might represent vulnerabilities that could contribute significantly to the EFC. For example, suppose the analysts identify for the specific plant being considered that operating crews are not yet using formalized communication as much as trainers would like. In addition, this deficiency seems to be a factor in somewhat challenging scenarios that the operating crews have faced in simulator training. In this

case, the judgment of the analysts (especially the input from operators and trainers) would be to add such a negative PSF to the existing EFC.

Another reason for being very restrictive in adding non-triggered PSFs is that such additions may lower the EFC probability. Initially, the analysts should focus on adding only those PSFs that are judged to increase the conditional probability of the unsafe action(s) associated with the HFE [i.e., increase the likelihood that the operators will take the associated inappropriate action(s)]. In fact, analysts may want to defer adding such PSFs until after some initial consideration of HFE quantification, including perhaps consultation with those who will provide the expert judgments needed in quantification. After this initial consideration of quantification, analysts can iterate back to this step to add PSFs, if necessary.

9.7.2 Additional Physical Conditions

Like the additional PSFs discussed above, more physical conditions can be added to the initial error-forcing context identified in Step 6. It is possible that if Step 6 is done very thoroughly, no new additional physical conditions (except those extraneous conditions that complicate the scenario and required operator response) may be found with this search. Also, if analysts desire, the additional resources (i.e., Tables 9.17 through 9.21) used in this search can be used earlier in the process (e.g., Step 6).

Also, like additional PSFs, such additional physical conditions may lower the probability or frequency of the HFE. Consequently, analysts should try to add only those plant conditions that are judged necessary to sufficiently strengthen the error-forcing context in order to increase the likelihood of unsafe operator actions. The addition of plant conditions also can be revisited after initial consideration of quantification, if necessary.

As illustrated by the summaries of event analyses in Section 5 and Appendix A, past operational experience has shown that serious events typically involve contextual elements falling into more than one of the following major categories of deviations in plant conditions: physics, information, hardware, and plant configuration. Physics deviations were identified in Step 6. Consequently, analysts should consider the following types of additional plant conditions:

- additional hardware failures, configuration problems, or unavailabilities
- indication failures
- plant conditions that can confuse operators
- factors not normally considered in PRAs

Each of these is discussed briefly below. As in the physics search described in Section 9.6.3, the analysts should investigate if there are any unrecoverable slips or lapses (both operator interactions with equipment and misreading or misinterpretation of indicators by operators) that could cause the plant conditions associated with the additional factors identified in this search.

Table 9.17 provides example causes of hardware failures, configuration problems, or unmodeled unavailability issues. Analysts should focus first on those conditions that are supported by or are extensions of the context already defined in Step 6. For example, if certain hardware failures already are part of the deviation scenario in Step 6, these failures could be explained by common-cause or other dependent failures. Also, if this is a plausible explanation for the failures defined in the deviation scenario, then additional failures may be plausible for the same reason. Knowledge of plant-specific systems design and operations is crucial in identifying such plausible extensions or links to the previously defined context. By identifying additional conditions that are related to (even dependent upon) the initially defined EFC, the initial EFC is strengthened with minimal reduction in the HFE probability.

For indicator failures, analysts can refer to Table 9.18 for prompts of different types of indicator failures and their causes.

The accident record has shown that certain kinds of plant conditions can confuse operators. The analysts should refer to Tables 9.19 through 9.21 for examples of such conditions. As for the other tables provided in this section, the examples given in these tables should be viewed as prompts for analysts' thinking and discussion, rather than as an exhaustive list of possibilities.

The accident record also shows that there are some factors that may be important to operator performance that are not normally considered in PRAs. In Section 5, Table 5.7 provided examples of such factors that analysts could consider in deciding what additional plant conditions should be added to the error-forcing context initially defined in Step 6.

9.7.3 Reintegration of the Deviation Scenario Description

If elements are added to the deviation scenario description (or EFC) in this step, then the analysts should reintegrate the scenario description in a way similar to that described in Section 9.6.7 for Step 6. In particular, new plant conditions or performance-shaping factors should be integrated into the scenario description. Also, these new plant conditions or PSFs might activate different or additional error mechanisms.

Table 9.17 Examples of Hardware Failures, Configuration Problems, or Unavailabilities

Plant Condition Type	Examples
Hardware response	Random failures (including multiple failures, spurious actuations)
	Initiator-induced failures
	Mode-induced failures (e.g., equipment inoperable or unavailable during shutdown conditions)

Table 9.17 Examples of Hardware Failures, Configuration Problems, or Unavailabilities (Cont.)

Plant Condition Type	Examples
	Common-cause failures
	Other dependent failures (e.g., support system failures, other cascading effects, human-induced, etc.)
	Preexisting operational problems
	Degraded operation
	Beyond design limits
	Human-induced (both latent and active failures)
Plant configuration	Concurrent activities (as they affect operator actions required for accident response)
	Latent failures (as they affect operator actions required for accident response; see also Hardware response, human-induced above)
Unavailabilities	Realistic unavailabilities (e.g., two trains out for maintenance simultaneously)

9.7.4 Products of Step 7

The completion of Step 7 results in the explicit addition of PSFs and other physical conditions to the descriptions of the deviation scenarios so that the EFC is now considered sufficiently strong to make the likelihood of the HFEs or UAs worth concern.

9.8 Step 8: Evaluate the Potential for Recovery

In this step, the definitions of HFEs and the associated EFCs are completed by considering the opportunities for recovering from the initial error(s) (or more precisely not recovering from initial errors). Performance of this step, perhaps even more so than previous search steps, is linked to issues considered in quantification (see Section 10.2). Consequently, some iteration between this step and the quantification step is possible. Also, since the consideration of the opportunities for recovery will involve extending the context defined in previous deviation search steps, recovery analysis also is iterative with Steps 6 and 7. If an HFE can be ensured to be recovered, the analysis stops and proceeds to issue resolution. If recovery cannot be ensured, then the analysis proceeds according to the discussion below.

9.8.1 Guidance for Step 8

The definition of the HFE or UA and the associated context (represented by the description of the deviation scenario) corresponds to an initial error(s). Given this initial error in responding to a specific deviation scenario, it is possible that later in the accident sequence the operators will recognize their error and be able to correct their initial actions before core damage or functional failure(s) occurs. Since the definition of HFEs modeled in the PRA includes both the initial unsafe action and the failure to correct this action, the analysts should investigate what opportunities for successful correction do exist, given the definition of the unsafe action and its explanation developed through the last step.

In evaluating the potential for recovery, the analysts should consider the following five main elements in analyzing the potential for recovery actions:

(1) definition of the possible recovery action(s) if the HFE/UA has been performed

(2) time available to perform the recovery actions so as to prevent a serious outcome (e.g., core damage)

(3) the existence and timing of additional cues that would alert the operators to the need to recover and provide sufficient information to identify the applicable recovery action(s)

(4) the existence and timing of additional resources (e.g., personnel) that could assist in recovery

(5) an assessment as to the strength of the recovery cues with respect to the initial EFC (i.e., plant conditions, PSFs, associated error mechanisms) and hence the likelihood of successful recovery (Section 10 provides some discussion on how to make such assessments)

To consider the above, the analysts should first decide on the necessary recovery action(s). This is based largely on the underlying understanding of what safety function(s) and equipment are failed or otherwise jeopardized as a result of the plant conditions and the HFE and UAs making up the deviation scenario. In addition, the time by which the recovery action(s) needs to be performed should also be identified based on the deviation scenario and an understanding of its related thermal hydraulics.

With the above knowledge, the analysts then develop the deviation scenario progression beyond the initial loss or degradation of the safety function or equipment [i.e., after the initial unsafe action(s) in the defined HFE]. One way to identify additional cues for recovery and understand plant behavior following the initial unsafe action(s) is to continue the mapping of trends in key plant parameters that was begun in Steps 5 and 6. Then development of a scenario progression log, similar to the diagnosis log created for the event analyses documented in Appendix A, can help analysts in structuring and assessing this new information. Appendices B through E provide illustrative examples of such scenario progression logs, using the headings of timing, plant symptoms, and

operator actions. The scenario progression log should highlight expected changes in key plant conditions and parameters, as well as any new relevant cues (indications, alarms, plant personnel observations) that are likely to occur as a result of the scenario progression. The new cues and resources that are identified will form the basis for defining additional contextual elements that are associated with nonrecovery.

Analyst judgment is the basis for the assessment of the importance of new cues and resources. However, the amount of time available for correction is an overriding factor. In other words, if little or no time is available to recover from the initial error, then the chance for recovery will be small. After time available, the analysts look for potential dependencies between the deviation scenario description (i.e., EFC) for the initial unsafe action and the failure to correct the initial action. Also, the analysts should recognize that initial mindsets (i.e., situation models) can be very difficult to break. (See the Oconee 3 example, especially the scenario progression log, given in Section 5 as well as the more detailed analysis given in Appendix A.) Also, operators can be distracted (or be too busy) with other activities, thereby missing cues and opportunities for action. Finally, operators often can justify the delay of actions beyond their criteria for performance, especially if plant hardware is almost fixed or returned to service (or initially failed by operator slips or lapses) and the consequences of the action are considered extreme. (See, for example, the Davis Besse loss of feedwater event in 1985 in Appendix A.) When considering these possible reasons for not performing the recovery action, the analysts should note the number, timing, and nature of the new cues (e.g., alarm, indicator change) and decide on how compelling the new cues are relative to these possible reasons for failing to recover. Any resulting new EFC elements that are associated with the recovery action should be added to the EFC identified for the initial unsafe action in order to complete the EFC for the HFE that will be modeled in the PRA.

Finally, the ATHEANA analysts should compare the EFC context developed with the characteristics of serious accidents listed in Table 5.6 and the complicating factors not usually modeled in PRAs given in Table 5.7. Both of these tables can be considered templates for error-forcing contexts.

9.8.2 Reintegration of the Deviation Scenario after Recovery

Because recovery analysis may add elements to the deviation scenario description (or error-forcing context), just as in Step 7, the analysts should reintegrate the scenario description after recovery analysis also. This reintegration should follow the general guidance given in Section 9.6.7 for Step 6. As in Step 7, elements of the error-forcing context that are added through recovery analysis might activate different or additional error mechanisms.

9.8.3 Product of Step 8

The product of Step 8 is the finalization of the EFC for the HFE and UAs of concern as part of the overall deviation scenario description. However, as stated at the beginning of Section 9.8, iteration between this step and quantification (Step 9) may be required.

Table 9.18 Examples of Information (i.e., Transmit) Problems

Hardware/Software Failures (i.e., information wrong, including instrument, sensor, switch, computer, and calculated parameter failures) (failures may be known, undiscovered, or masked by other activities) Hardware/software may be: Randomly failed (including spurious indications, failures to respond, intermediate indications) Unavailable due to testing or maintenance Disabled by personnel Failed due to operator actions Outside operating range due to plant conditions Provide conflicting indications Failed due to design flaws (e.g., redundant parameters not independent)
Display Failures (i.e., information misleading) Display may: Be failed (e.g., a broken meter or alarm) - either known or undiscovered Lack global cues Lack reference context Have hidden indications (e.g, on back panels) Have distributed locations for displays or controls Have noisy interfaces Have design flaws (e.g., indicated valve position not connected with stem position) Have delayed indication (e.g., trends not noticeable due to recorder scale and event timing) Have only temporary indication (e.g., parameter or trend not noticeable because only temporarily displayed due to event timing or other factors)
Other Human Factor Problems (i.e., information wrong and/or misleading) Information may be wrong or misleading because of: Communication failures (wrong, misleading, ambiguous) (field operators, personnel in containment, I&C or maintenance technicians) Design flaws Lack of redundant instruments or other information sources Requirements for interpretations or hand calculations of parameters (e.g., due to operations outside normal conditions in Prairie Island 2 shutdown event)

Table 9.19 Physics Algorithms in Instruments that Can Confuse Operators

Indicator/Algorithm or Actual	Example
Valve position indicator	Drive vs. stem position Stem disk separation Switch on solenoid Motor operated valve drive screw
Level indicator	Flashing in reference leg P_{pzr} uncompensated for temperature Sensor leaks Sensor isolation
Pressure indicator	Indicated parameter can be time history algorithm Improper sensor location
Temperature indicator	RTDs: linearity limits, ambient temperature compensation T/C: linearity limits, reference temperature drift
Any indicator	Indicated parameter can be calculated from others rather than measured directly Plant behaves in a way to make algorithm generate wrong information or story

Table 9.20 Examples of Plant Conditions in Which the Plant Physics or Behavior Can Confuse Operators

Plant Conditions or Physics	Examples
Reaching saturation, then repressurizing	Steam bubbles will have formed in hot spots, possibly interfering with flow or reflooding)
Positive temperature coefficient	Can result in unanticipated overpower
Operation of electrical equipment	Effects of grounds Speed control and power in 3-phase induction (and synchronous) machines Breaker and controller lockout circuits Selective tripping
Transient effects beyond those analyzed and addressed in training	LOCAs other than 2-inch and double-ended guillotine)
Multiple evolutions (which confound expected physics)	Ramping up or down in power while equipment is being tested or bought back on-line after maintenance
Net positive suction head	Draining down to midloop while other tests, washdown activities, etc. are being performed during shutdown

Table 9.21 Other Plant Conditions that Can Confuse Operators

Plant Conditions	Details
Plant radios	Results in garbled communications
Multiple equipment failures	Common causes failure Combinations of degraded functions, unavailability, human-induced failures, and/or "random" failures
Partial degraded, rather than failed instrument or control air pressure Failures in selective tripping of electrical breakers	Can result in increasing combinations of failed equipment
Ambient temperature-induced failures of electrical or electronic equipment	Can result in increasing combinations of failed equipment
Multiple problems	Combinations of any of the above or conditions indicated on other tables

9.9 References

9.1 Magee, R.S., E.M. Drake, D.C. Bley, G.H. Dyer, V.E. Falter, J.R. Gibson, M.R. Greenberg, C.E. Kolb, D.S. Kosson, W.G. May, A.H. Mushkatel, P.J. Niemiec, G.W. Parshall, W. Tumas, and J. Wu, *Risk Assessment and Management at Deseret Chemical Depot and the Tooele Chemical Agent Disposal Facility*, Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, National Research Council, National Academy Press, Washington, DC, 1997.

9.2 Isselbacher, K.J., A.C. Upton, J.C. Bailar, K.B. Bischoff, K.T. Bogen, J.I. Brauman, D.D. Doniger, J. Doull, A.M. Finkel, C.C. Harris, P.K. Hopke, S.S. Jasanoff, R.O. McClellan, L.E. Moses, D.W. North, C.N. Oren, R.T. Parkin, E.D. Pellizzari, J.V. Fodricks, A.G. Russell, J.N. Seiber, S.N. Spaw, J.D. Spengler, B. Walker, and H. Witschi, *Science and Judgment in Risk Assessment*, Committee on Risk Assessment of Hazardous Air Pollutants, National Research Council, National Academy Press, Washington, DC 1994.

9.3 J.P. Poloski, D.G. Marksberry, C.L. Atwood, and W.J. Galyean, *Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995*, NUREG/CR-5750, Idaho National Engineering and Environmental Laboratory, February 1999.

9.4 J. Reason, *Human Error*. New York, Cambridge University Press, 1990.

9.5 J. Julius, E. Jorgenson, G.W. Parry, and A.M. Mosleh, "A procedure for the analysis of error of commission in a Probabilistic Safety Assessment of a nuclear power plant at full power," *Reliability Engineering and System Safety* **50**: 189-201, 1995.

9.6 D.J. Wakefield, "Application of the human cognitive reliability model and confusion matrix approach in a probabilistic risk assessment," *Reliability Engineering and System Safety*, **22**: 295-312,1988.

9.7 R. Ellis Knowlton, *An Introduction to Hazard and Operability Studies: The Guide Word Approach*, Chemetics International, October 1992.

Table 9.9a Possible EOCs for Systems or Equipment that Automatically Start or Stop

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to initiate or actuate automatically	1 and 2	Inappropriately removed from automatic control	Operators take equipment out of armed or standby status (e.g., pumps put in pull-to-lock) Operators change equipment configuration/lineup from armed, standby, or normal status
		Inappropriately removed from armed or standby status	Operators bypass or suppress automatic signals Operators disable automatic signals/sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators reset signal setpoints Operators disable or fail equipment
Equipment fails to stop automatically	7	Inappropriately removed from automatic control	Operators bypass or suppress automatic signals Operators disable automatic signals or sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators reset signal setpoints Operators disable or fail equipment

Table 9.9b Possible EOCs for Continuation of Operation or No Operation of Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to continue to operate for duration of mission time	3	Inappropriately terminated	Operators stop equipment (e.g., pumps stopped) Operators both stop and disable equipment for future service (e.g., pumps put in pull-to-lock) Operators disable or fail equipment (e.g., due to operation outside of design parameters) Operators stop and realign equipment out of required armed or standby configuration or lineup Operators stop equipment and bypass or suppress automatic signals Operators stop equipment and disable automatic signals/sensors Operators stop equipment and take automatic signals out of armed status Operators stop equipment and reset signal setpoints
		Inappropriately isolated or aligned	Operators realign equipment (e.g., valves repositioned) Operators actuate equipment automatic isolation signals Operators actuate equipment automatic reconfiguration signals
		Output and/or resources inappropriately diverted	Operators realign equipment (e.g., valves repositioned) Operators operate equipment outside design parameters (e.g., over RHR design pressure, resulting in flow diversion through lifted relief valves, ISLOCAs, etc.)
		Output and/or resources inappropriately depleted	Operators do not adequately control equipment that competes for resources before or during operation of required equipment Operators do not control equipment early in accident (Also considerations with ...resources diverted above)
Equipment status inappropriately changed	10	Inappropriately operated	Operators manually actuate or start equipment Operators manually realign equipment Operators manually override equipment automatic isolation signals Operators manually actuate equipment automatic control
Equipment fails to remain stopped for required duration	8	Inappropriately restarted (and continues to operate)	

Table 9.9c Possible EOCs or EOOs for Manual Actuation and Control of Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to be manually intiated or actuated when required	4	Fails to be actuated when required (EOO)	Operators never actuate equipment Operators actuate equipment too late Operators release or unsuppress equipment automatic initiation signals too late
		Inappropriately initiated or actuated (EOC)	Operators actuate equipment prematurely (i.e., too soon) Operators release or unsuppress equipment automatic initiation signals prematurely
Equipment fails to be stopped manually	9	Fails to be stopped when required (EOO)	Operators never stop equipment Operators stop equipment too late Operators release or unsuppress equipment automatic initiation signals for stop too late
Equipment fails to be controlled or operated as required	5	Fails to be operated or controlled (EOO) Inappropriately operated or controlled (EOC)	Operator control of equipment operation results in: Underfeeding or filling — Overfeeding or filling Undercooling — Overcooling Underpressure — Overpressure Reactivity decrease — Reactivity increase Integrity breach

Table 9.9d Possible EOOs for Backup (i.e., Recovery) of Failed Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to initiate or actuate automatically	2	Fails to perform backup, manual startup (after automatic actuation fails)	Operator fails to manually start/stop Operator fails to manually isolation/alignment Operator fails to manually open/close Operator fails to manually lockout/trip Operator fails to manually insert/withdraw Operator fails to manually transfer
Equipment fails to stop automatically	7	Fails to perform backup, manual stop (after automatic stop fails)	
Equipment fails to remain stopped for required duration	8	Fails to perform backup, manual stop (after spurious re-start)	
Equipment status changes spuriously and inappropriately	11	Fails to perform backup, manual stop (after spurious actuation) Fails to perform backup, manual re-alignment (after spurious re-configuration)	

Table 9.9e Possible EOCs or EOOs for Failures of Passive Systems and Components

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment status inappropriately changed	6	Fails to maintain integrity (EOO) Inappropriately breached integrity (EOC)	Operator actions (e.g., operator fails to operate/control, operator inappropriately operates/controls) from other categories that have these consequential effects

Table 9.15a
Scenario Characteristics and Description

1. **Situation Assessment** - If a scenario can be described by any of the characteristics below, go to the corresponding scenario characteristics for *failures in situation assessment* presented in Table 9.15b to identify Potential error mechanisms, possible unsafe actions (UAs), and relevant performance-shaping factors (PSFs).

Scenario Characteristics	Description
Garden path problems	Conditions start out with the scenario appearing to be a simple problem (based on strong but incorrect evidence) and operators react accordingly. However, later correct symptoms appear, which the operators may not notice until it is too late.
Situations that change, requiring revised situation assessments	Once operators have developed a situation assessment and have started acting on it, it is often very difficult for them to recognize that there is new information or new conditions that requires them to change their situation assessment
Missing information	Key indicators may be missing due to failed sensors, lack of sensors, or lack of informants in the plant.
Misleading information	Misleading information may be provided due to inherent limitations of reports (e.g., stale information, inherent limitations of predictions, distortions resulting from indirect reports, secondary sources, translations) or explicit intent to deceive through misinformation.
Masking activities	Activities of other agents, or other automated systems may cover up or explain away key evidence.
Multiple lines of reasoning	Situations can occur where it is possible to think of significantly different explanations or response strategies, all of which seem valid at the time, but which may be in conflict (or a source of debate and disagreement by the operating crew).
Side effects	Situations can arise where the effects of human or automated system actions, or effects of the initial failure, have side effects that are not expected or understood.

Table 9.15a
Scenario Characteristics and Description (Cont.)

2. **Response Planning** - If a scenario can be described by any of the characteristics below, go to the corresponding scenario characteristics for *failures in response planning* presented in Table 9.15b to identify potential error mechanisms, possible UAs, and relevant PSFs.

Scenario Characteristics	Description
Impasses	The scenario contains features where, at some point, it is very difficult for the operators to move forward, such as when procedures or the operators' situation model no longer matches the conditions, or assumed personnel or resources are not available.
Late changes in the plan	The scenario is being managed according to a prepared plan, and then for some reason changes are required late in the scenario. Operators can become confused as to next steps; the plan is no longer well tested and can contain flaws, or the whole "big picture" gets lost by those managing the event.
Dilemmas	Ambiguity in the plan or in the situation (the event looks somewhat like two or more different accidents) can raise significant doubt in the operators' minds about the appropriate next steps.
Trade-offs	Operators must make impromptu judgments about choices between alternatives, such as when to wait to see if a problem develops (and may get out of control) versus jumping in early before it is clear what has caused the problem (just one of many examples).
Double binds	Conditions exist where operators are faced with two (or more) choices, all of which have undesirable elements.
High tempo, multiple tasks (Sub- or related categories are escalating events, cascading problems, and interacting problems)	The operators simply run out of resources (mental or physical) to keep up with the task demands. In escalating events, the problem keeps getting harder and harder or more complex. Cascading problems are those where the effects of one problem (or an attempt to solve it by the operators) create new problems. In interacting problems two or more faults interact to create complex symptoms that may have never been foreseen.
Need to shift focus of attention	As the scenario unfolds, the operators may need to move attention from one particular aspect of the problem to another, yet they remain focused on the initial problem area, which may be minor.

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors

1. **Failures in Situation Assessment** - When particular characteristics in Table 9.15a are identified as relevant descriptors of a scenario, this table is used to identify potential human error mechanisms that may facilitate *failures in situation assessment.* Possible generic unsafe actions (UAs) and potential performance-shaping factors (PSFs) that could contribute to the occurrence of a UA are also presented. *(Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.)*

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Garden path problems Situations that change, requiring revised situation assessments	1. Simplifying 2. Recency 3. Frequency 4. Familiarity 5. Fixation 6. Tunnel vision 7. Confirmation bias 8. Complacency	1. Initial application of incorrect procedure step 1 - 8. Operators defer action on the changes indicated by other parameters 5 - 8. Fail to recognize a serious situation in time 1 - 8. Take an inappropriate action, take a correct action too soon, fail to take a needed action 5 - 8. Miss a decision point	1 - 4. Training/practice - Initial event is used repeatedly in training or was addressed in training, or is one about which a lot of attention is given in training All. Human-machine interface (HMI) - Later-occurring correct or complete indicators are located where they can be easily seen by one or more crew members. All. HMI Are the later - occurring indications compelling? All. Workload - Would the operators have to work hard to identify and understand the later occurring information? Could the workload become excessive? Could the situation not seem important enough to induce them to search for verification? 5 - 8. Procedures - Are there any warnings or items in the procedures that might alert operators to the importance of the later-occurring information?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Situation Assessment) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Missing information	1. Displayed parameters lead to entry into wrong procedure step or may not lead to entry into procedure 2. Displayed parameters match incorrect mental template (similarity matching) 3. Existing pattern of information directs operators' attention away from redundant sources 4. Complacency 5. Overly eager to respond 6. Simplifying	1,2,&3. Application of incorrect procedure step or no response. 1 - 6. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1, 2 & 3 HMI - Are there indicators that might help the crew discover the existence of the missing information? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 3. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 1 - 3. Training/practice - Lack of discipline or trained practice in searching for other relevant parameters 2. Training/practice - Similar event is used repeatedly in training or was addressed in training, or is given a lot of attention in training 1 - 6. Workload - Would the operators have to work hard to identify other sources of information that could help them detect the absence of the missing indications? Could the workload become excessive or could the situation not seem important enough to induce them to search for verification?
Misleading information	Same as above	Same as above	Same as above

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Situation Assessment) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Masking activities	1. General pattern of existing information seems normal enough that operators do not detect or understand important changes in some parameters 2. Simplifying 3. Apathy - Lack of urgent consideration of parametric behavior as displayed 4. Overeagerness (inclination to respond too soon)	1,2&4. Selection of wrong or less relevant procedure 1,2,3&4. Incorrect situation assessment due to hidden information 1,2,&3. Operators defer action on the basis of the parameters as displayed 1,2,&3. Fail to recognize a serious situation in time 1,2,3,&4. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1,2,&3. Miss a decision point 4. Anticipate an incorrect situation and take an action too soon.	1- 4. Training/practice - Lack of discipline or trained practice in monitoring all parameters and cross-checking against other information I- 4. HMI - Are there other indicators that might help the crew detect the existence of the hidden information? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 4. Training/practice - Operators have learned to focus on restricted set of available information sources 1,2 & 4. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately considering other relevant indications?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Situation Assessment) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Multiple lines of reasoning	1. Simplifying 2. Satisfying 3. Polarization of thinking 4. Expectation biases (familiarity, recency, primacy, frequency, confirmation bias) 5. Delays (due to crew disagreements) 6. Reluctance, cautiousness 7. Anxiety, stress 8. Lack of deep technical knowledge	1 - 8. Lack of, or reduced, attention paid to other parameters and their changes 1 - 8. Competing or inconsistent responses taken 1 - 8. Application of incorrect procedure step or no response 1 -8. Take an inappropriate action, take a correct action too soon, fail to take a needed action in time	1 - 8. Training - Lack of training or practice for off-normal accident conditions 1 - 8. Procedures - Inadequate information for correct discrimination between lines of reasoning 1 - 8. HMI - Are there other indicators that might help the crew verify or determine the correct line of reasoning ? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters make the conflicting interpretations harder to resolve?
Side effects	1. Lack of deep technical knowledge 2. Reduced vigilance given expected success (overconfidence) 3. Tunnel vision 4. Fixation on initial diagnosis and directly relevant results	1. Take an action that induces both desired and undesired consequences 1 - 4. Fail to take a needed action in time 1 - 4. Take an inappropriate action given the presence of the undesired side effects	1 - 3. Training - Lack of training or practice for off-normal accident conditions 1 - 3. HMI - Are there other indicators that might help the crew detect the undesired side effects ? Are they located where they can be easily seen by one or more crew members most of the time? Are they compelling? 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring make the undesired effects harder to detect?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Cont.)

2. **Failures in Response Planning** - When particular characteristics in Table 9.15a are identified as relevant descriptors of a scenario, this table is used to identify human error mechanisms that may facilitate *failures in response planning.* Possible generic UAs and potential PSFs that could contribute to the occurrence of a UA are also presented . *(Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.)*

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Impasses	1. Lack of deep technical knowledge 2. Operators' expectations or current situation model begins to conflict with the indications and/or what the procedures dictate 3. Anxiety about taking a wrong action	1 - 2. Fail to take a needed action in time	1 - 2. Training - Lack of training or practice for off-normal accident conditions 1 - 2. Procedures - Inadequate information for how to proceed 1 - 2. HMI - Are there other indicators that might help the crew verify or determine the correct response ? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 2. Workload - Could the operators' workload make the impasse about how to proceed more difficult to resolve? 2 - 3. Organizational factors Could fear of retribution or other aspects of the organizational climate at the plant contribute to making it more difficult to solve the impasse? 2 - 3. Organizational factors Does the plant have strict guidelines regarding adherence to procedures?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Response Planning) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Late changes in the plan	1. Lack of deep technical knowledge 2. Fixation on initial diagnosis and initial response plan 3. Anxiety about taking a wrong action	1 - 3. Fail to take a needed action in time 1 - 3. Take an inappropriate action	1 - 3. Training - Lack of training or practice for off-normal accident conditions I - 3. Procedures - Is there adequate information for how to proceed if the new indicators are accepted? 1 - 3. HMI - Are there other indicators that might help the crew tease out the correct response plan ? Are they located where they can be easily seen by one or more crew members most of the time? Are they compelling? 1 - 3. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring make it difficult to derive the correct response plan? 2 - 3. Organizational factors Could fear of retribution or other aspects of the organizational climate at the plant contribute to making it more difficult to change the plan late in the scenario? 2 - 3. Organizational factors Does the plant have strict guidelines regarding adherence to procedures?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Response Planning) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Dilemmas Trade-offs Double binds	1. Lack of deep technical knowledge 2. Anxiety about taking a wrong action	1 - 2. Fail to take a needed action in time 1 - 2. Take an inappropriate action	1. Training - Lack of training or practice for off-normal accident conditions 1. Procedures - Inadequate information or guidance for how to proceed 1. HMI - Are there other indicators that might help the crew verify or determine the the correct response ? Are they located where they can be easily seen by one or more crew members most of the time? 1. Workload - Could the operators' workload make the dilemma, trade-off, or double bind more difficult to resolve? 2 . Organizational factors Could fear of retribution or other aspects of the organizational climate at the plant contribute to making it more difficult to solve the dilemma, trade-off, or double bind? 2 . Organizational factors Does the plant have strict guidelines regarding adherence to procedures?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Response Planning) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
High tempo, multiple tasks (sub- or related categories are escalating events, cascading problems and interacting problems)	1. Lack of deep technical knowledge 2. Inadequate cognitive resources	1 - 2. Fail to take a needed action in time 1 - 2. Take an inappropriate action 1 - 2. Take an action that simply complicates the problem	1. Training - Lack of training or practice for off-normal accident conditions. 1. Procedures - Inadequate information or guidance for how to proceed 1. HMI - Are there other indicators that might help the crew verify or determine the correct response ? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 2. Workload - Could the operators' workload make the situation more difficult to resolve?
Need to shift focus of attention	1. Simplifying 2. Satisfying 3. Polarization of thinking 4. Expectation biases (familiarity, recency, primacy, frequency, confirmation bias) 5. Delays (due to crew disagreements) 6. Reluctance, cautiousness 7. Anxiety, stress 8. Lack of deep technical knowledge	1 - 8. Lack of, or reduced, attention paid to other parameters and their changes 1 - 8. Competing or inconsistent responses taken 1 - 8. Application of incorrect procedure step or no response 1 -8. Take an inappropriate action, take a correct action too soon, fail to take a needed action in time	1 - 8. Training - Lack of training or practice for off-normal accident conditions 1 - 8. Procedures - Inadequate information for correct discrimination regarding where to focus attention 1 - 8. HMI - Are there other indicators that might help the crew verify or determine where to focus attention? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 5. Workload - Could the operators' workload make it more difficult to determine where to focus attention or realize that they need to shift attention?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics
(Table to be used with Table 9.16b)

1. **Failures in Detection -** If answers to any of the questions are yes, go to the corresponding parameter characteristics for *failures in detection* presented in Table 9.16b to identify potential error mechanisms, possible UAs, and relevant PSFs)

Parameter Characteristics	Question
No indication	Does this scenario involve failed indicators? Does this scenario involve indications calculated from other failed instruments (e.g., subcooling based on RCS pressure)?
Small change in parameter	Within this scenario and with the existing human-machine interface design, is there a relevant parameter change small enough that it might be overlooked (i.e., not detected)?
Large change in parameter	Within this scenario and with the existing human-machine interface design, is there a relevant parameter change so large or out of range that it might be overlooked (e.g, indicator pegged at the top or bottom of a meter and not noticed).
Lower or higher than expected value of parameter	Does this scenario involve indications that are lower or higher than would be expected? Does this deviation correspond with expected values for nonaccident conditions, so that the deviation might not be detected as anomalous?
Low rate of change in parameter	Does this scenario involve significantly slower than expected changes in any indication? Within this scenario and with the existing human–machine interface design, is it likely that the slow rate of change might be overlooked?
High rate of change in parameter	Does this scenario involve rapid changes in any parameter that, with the existing human-machine interface design, may be overlooked (e.g., fleeting changes, briefly appearing alarms or indications, or an indicator pegged at the top or bottom of a meter and not noticed)?
Changes in two or more parameters in a short time	Does this scenario involve changes in two or more indications that are significantly different from expected? Do they involve rapid changes in any parameters that, with this interface design, may be overlooked (such as fleeting changes or briefly appearing alarms or indications)?
Delays in changes in two or more parameters	Does this scenario involve changes in two or more indications that are significantly delayed from what is expected? Do they involve late changes in parameters that, with this interface design, may be overlooked?
One or more false indications	Does this scenario involve false indications that, together with the genuine indications, resemble a situation that is expected (i.e., consistent with other on-going activities that could lead operators to ignore or not attend carefully to the indications)?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Cont.)

2. **Situation Assessment** - If answers to any of the questions are yes, go to the corresponding parameter characteristics for *failures in situation assessment* presented in Table 9.16b to identify potential error mechanisms, possible UAs, and relevant PSFs)

Parameter Characteristics	Question
No indication	Does this scenario involve failed indicators? Does this scenario involve indications calculated from other failed instruments (e.g., subcooling based on RCS pressure)?
Small change in parameter	Does this scenario involve small or significantly smaller-than-expected changes in any indication? Can the operators be led to a state of complacency by this small change? Within this scenario and with the existing human-machine interface design, is it likely that the operators will be misled by a small change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
Large change in parameter	Does this scenario involve a large or significantly larger-than-expected changes in any indication? Can the operators be led to a state of anxiety by this large change? Within this scenario and with this interface design, is it likely that the operators will be misled by a large change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
Lower or higher than expected value of parameter	Does this scenario involve indications that are lower or higher than expected? Does this deviation correspond with expected values for other (different) accident conditions?
Low rate of change in parameter	Does this scenario involve slow or significantly slower-than-expected changes in any indication? Can the operators be led to a state of complacency by this slow change? Within this scenario and with this interface design, is it likely that the operators will be misled by a slow change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
High rate of change in parameter	Does this scenario involve rapid or significantly more rapid-than-expected changes in any indication? Can the operators be led to a state of anxiety by this rapid change? Does this scenario involve rapid changes in any parameter that, with this interface design, may be discounted or assumed to be anomalous (such as fleeting changes or briefly appearing alarms or indications)? If overlooked or ignored, is the absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Situation Assessment)(Cont.)

Parameter Characteristics	Question
Changes in two or more parameters in a short time	Does this scenario involve changes in two or more indications that are significantly different from expected or inconsistent? If observed, will these indications cause operators to be significantly uncertain or confused as to the situation in the plant? Does this scenario involve rapid changes in any parameters that, with this interface design, may be overlooked (such as fleeting changes or briefly appearing alarms or indications)? If overlooked, is their absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
Delays in changes in two or more parameters	Does this scenario involve two or more indications that are significantly delayed from what is expected? If observed, will these delayed indications cause operators to be significantly uncertain or confused as to the situation in the plant? Does this scenario involve changes in two or more indications that are significantly delayed from what is expected? Do they involve late changes in parameters that, with this interface design, may be overlooked? If overlooked, is their absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)? Delayed information can be ignored or reinterpreted to match earlier (premature) assessments of the plant situation (such as being dismissed as "instrument error").
One or more false indications	Does this scenario involve false indications that, together with the genuine indications, resemble a situation that is "expected" (i.e., consistent with other on-going plant activities that could "explain" their presence)? Will these false indications cause operators to be significantly uncertain or confused as to the situation in the plant?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Situation Assessment)(Cont.)

Parameter Characteristics	Question
Direction of change in parameter(s) over time is not what would be expected (if the base case scenario was operative vs. the deviant) Direction of change in parameters over time, relative to each other, is not what would be expected (if the base case scenario was operative vs. the deviant) Relative rate of change in two or more parameters is not what would be expected (if the base case scenario was operative vs. the deviant)	Does this scenario involve changes in one or more parameters over time that are significantly different than what would be expected if the base case scenario was operative as opposed to the existing deviant scenario. If observed, will these changes cause operators to be significantly uncertain or confused as to the situation in the plant?
Behavior of apparently relevant parameters is actually irrelevant and misleading	Does this scenario involve the occurrence of one or more parameters that are actually irrelevant and misleading given the deviant scenario being examined. If observed, could these parameters cause operators to be significantly mislead. Would they be similar to patterns that would occur in base case scenario.

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics(Cont.)

3. **Response Planning** - If answers to any of the questions are yes, go to the corresponding parameter characteristics for *failures in response planning* presented in Table 9.16b to identify potential error mechanisms, possible UAs, and relevant PSFs)

Parameter Characteristics	Question
No indication	N/A
Small change in parameter	Does this scenario involve smaller-than-expected changes in an important parameter used as a cue or caution in the procedures, or used in training as a basis for actions? What is the likely effect of the operators misapplying this cue or caution? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of complacency or forgetfulness by this small change?
Large change in parameter	Does this scenario involve larger-than-expected changes in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of stress or anxiety by this large change?
Lower or higher than expected value of parameter	Does this scenario involve lower or higher-than-expected values in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of complacency or forgetfulness by the lower change or a state of anxiety by the higher change?
Low rate of change in parameter	Does this scenario involve slower-than-expected changes in an important parameter used as a cue or caution in the procedures? What is the likely effect of the operators mis-applying this cue or caution? Can the operators be led to apply informal rules by this slower deviation? Can the operators be led to a state of complacency or forgetfulness by this slower change?
High rate of change in parameter	Does this scenario involve faster-than-expected changes in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of stress or anxiety by this faster change?
Changes in two or more parameters in a short time	Does this scenario involve changes in two or more indications that are significantly different from the procedural expectations? If observed, will these indications cause operators to be significantly uncertain or confused as to how the procedures should be applied to the plant?
Delays in changes in two or more parameters	Does this scenario involve significant delays in two or more indications compared with the procedural expectations? Will these delays cause operators to be significantly uncertain or confused as to how the procedures should be applied to the plant?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Response Planning)(Cont.)

Parameter Characteristics	Question
One or more false indications	Does this scenario involve false indications that mislead the operators into believing that the required actions are no longer necessary or are not possible (e.g., false indication of a caution or prohibition)? Does this scenario involve false indications that require inconsistent actions by operators (e.g., both depressurize and repressurize the primary system)?
Parameters indicate response for which insufficient resources are available or indicate more than one response option	Does this scenario involve a situation where the unavailability of resources make the response difficult to execute? Are there competing options or options with trade-offs?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Table to be used following Table 9.16a)

1. **Failures in Detection** - When particular parameter characteristics in Table 9.16a are identified as relevant descriptors of critical parameters in a scenario, this table is used to identify human error mechanisms that may facilitate *failures in detection.* Possible generic error types and potential performance-shaping factors (PSFs) that could contribute to the occurrence of an unsafe action (UA) are also presented. *[Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.]*

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
No indication	1. Displayed parameters lead to entry into wrong procedure step or may not lead to entry into procedure 2. Other indications or parameters alone are benign, leading to complacency 3. Existing pattern of information directs operators' attention away from redundant sources	1,2,&3. Application of incorrect procedure step or no response	1. HMI - Are there other indicators that might help the crew detect the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 1. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 1. Training/practice -Are monitoring strategies such that operators would be unlikely to detect the absence of the indication on the basis of other indicators? 3. Training/practice - Operators have learned to focus on a restricted set of available information sources.

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Small change in parameter	1. Limited discrimination - Imperceptible change in display or functionally imperceptible given competing demands 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias	1 - 5. Lack of awareness that the parameter is changing; operators assume that the value is static. 1- 5. Application of incorrect procedure step or no response	1. HMI- Lack of trending displays (e.g., use of analog meter display only) 1. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 1. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1. HMI -Other indicators whereby operators could be led to monitor or detect the small change in the parameter 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting the small change? 1 - 4. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Large change in parameter	1. Limited discrimination (display design inadequate for detecting large change) 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias	1 - 5. Failure to take account of changes in parameter in creating situation model 1 - 5. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting a large or "out-of-normal range" change in this parameter? 1 - 5. HMI - Are the indicators located where they can be easily seen by one or more crew members most of the time? 1 - 5. HMI. Is the instrument designed so that large changes might be more difficult to detect than more normal changes, e.g., indicator pegged at the top or bottom of a meter and not noticed? 1 - 5. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Lower or higher than expected value of parameter	1. Tunnel vision 2. Confirmation bias 3. Expectation bias 4. Recency bias	1 - 4. Failure to take account of changes in parameter in creating situation model. 1 - 4. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 - 4. Training/practice - Is the operators' training such that they might make assumptions about what the value of this parameter would be in this context and therefore not carefully monitor it? 1 - 4. Procedures - Are there any aspects of the procedures called for by the other parameters that could lead operators to ignore this parameter?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Low rate of change in parameter	1. Insufficient attention to processes in time? 2. Limited discrimination - Imperceptible change in display or functionally imperceptible given competing demands 3. Tunnel vision 4. Confirmation bias 5. Expectation bias 6. Recency bias	1 - 6. Failure to take account of changes in parameter in creating situation model. 1 - 6. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 -2. HMI- Lack of trending displays (e.g., use of analog meter display only) 1 - 2. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 1 - 2. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1 -2. HMI - Other indicators whereby operators could be led to monitor or detect the small change in the parameter. 1 - 2. HMI - Instrument designed so that gradual changes are not easily detectable 1 - 6. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting the small rate of change? 1 - 6. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
High rate of change in parameter	1. Insufficient attention to processes in time? 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias	1 - 5. Failure to take account of changes in parameter in creating situation model 1 - 5. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1 - 5. HMI - Are there other indications whereby operators could be led to monitor/detect the high rate of change in the parameter 1. HMI - Instruments designed so that a high rate of change might not be noticed (e.g., digital display) or they are located where they cannot be easily seen by most of the crew 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting the small rate of change? 2 - 5. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training
Delays in changes in two or more parameters	1. Insufficient attention to processes in time? 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias 6. Satisfied with limited set	Same as above	Same as above

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Changes in two or more parameters in a short time	1. Saliency 2. Primacy 3. Recency 4. Availability (The above EMs may relate to detecting one indication over another or to failing to detect either because of earlier occurring indications) 5. Tunnel vision 6. Confirmation bias 7. Expectation bias	Same as above	Same as above and: 1 - 4. HMI - Indicators located close together so that detection of changes in one might facilitate (or in some cases interfere with) detection of changes in the other. 1 - 4. Training/Procedures - Are there any aspects of the procedures called for by one of the parameters that could lead operators to ignore the other?
One or more false indications	1. General pattern of false and genuine indications seems normal enough that operators do not detect important changes in some parameters 2. General pattern of false and genuine indications are benign enough that operators become complacent and fail to detect important changes 3. Indications misleading to the extent that operators do not monitor other important parameters	1 - 3. Failure to take account of changes in parameter in creating situation model 1 - 3. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 -3 . HMI - Are there other indicators that might help the crew detect the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 3. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 1 - 3. Training/practice -Are monitoring strategies such that operators would be unlikely to detect the failed indicator on the basis of other indicators? 1 - 3. Training/practice - Operators have learned to focus on a restricted set of available information sources

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics

2. **Failures in Situation Assessment** - When particular parameter characteristics in Table 9.16a are identified as relevant descriptors of critical parameters in a scenario, this table is used to identify possible human error mechanisms that may facilitate *failures in situation assessment.* Possible generic UAs and potential PSFs that could contribute to the occurrence of a UA are also presented. *[Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.]*

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
No indication (or no change in the indication) for an important parameter	1. Displayed parameters lead to entry into wrong procedure step 2. Displayed parameters match incorrect mental template (similarity matching) 3. Complacency 4. Overly eager to respond 5. Simplifying 6. Recency bias	1. Application of incorrect procedure step 2, 5, 6. Incorrect SA due to missing information 3. Operators defer action on the changes indicated by other parameters 3. Fail to recognize a serious situation in time 2,4,5,&6. Take an inappropriate action, take a correct action too soon, fail to take a needed action. 1,2,3,5,&6. Miss a decision point	1& 2 HMI - Are there other indicators that might help the crew discover the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 1.& 2 - Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 3. Training/practice - Lack of discipline or trained practice in responding to all parameters 6. Training/practice - Similar event is used repeatedly in training or was addressed in training, or is given a lot of attention in training? 1,2,3,5&6. Workload - Would the operators have to work hard to identify other sources of information that could help them detect the presence of the faulty indications? Could the workload become excessive or could the situation not seem important enough to induce them to search for verification?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Small change in parameter	1. Limited discrimination - Imperceptible change in display 2. Apathy - Lack of urgent consideration of parametric change 3. Overeagerness (inclination to respond too soon)	1. Lack of awareness that the parameter is changing; operators assume that the value is static 2. Operators defer action on the changes in the parameter until other parametric needs are addressed 2. Operators disbelieve or discount a small change in this context 1 & 2 . Fail to recognize a serious situation in time 1 & 2. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1 & 2. Miss a decision point 3. Anticipate a situation and take an action too soon.	1. HMI- Lack of trending displays (e.g., use of analog meter display only) 1. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 1. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1 & 2. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately considering the small change? 2. Training/practice - Lack of discipline or trained practices in responding to all parameters 2 & 3 HMI - Other indicators whereby operators could determine the significance of the small change in the parameter 2 & 3. Training/practice - Trained to cross-check this parameter?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Large change in parameter	1. Fixation - Preoccupation with parameter 2. Incredulity - Disbelief in displayed changes (sensor or instrument error) 3. Overeagerness 4. Displayed parameters match incorrect mental template (similarity matching) 5. Simplifying 6. Recency bias	1. Lack of, or reduced, attention paid to other parameters and their changes 1. Stress from concern that parameter is approaching a critical value much earlier than expected (may not match procedure). Stress may result in an inappropriate action, the taking of a correct action too soon, failure to take a needed action) 2. Failure to take account of changes in parameter in creating situation model 3,4,5,&6 . Take an inappropriate action, take a correct action too soon, fail to take a needed action	1. Training/practice - Lack of discipline or trained practice in responding to all parameters 1. Training - Lack of training or practice for off-normal accident conditions (use of FRG procedures) 1. Procedures - Omission of guidelines for unexpected plant conditions 2. Training - Lack of training in responding to "failed" parameters 2. HMI - Experience of unreliable performance of the relevant parameters 2,4,5,&6. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 2,3,4,.5,&6. HMI - Are there other indicators that might help the crew verify the accuracy of the large change in the parameter? Are they located where they can be easily seen by one or more crew members most of the time? 2,4,5,&6. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately considering a large or "out-of-normal range" change in this parameter?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Lower or higher than expected value of parameter	1. Tunnel vision 2. Confirmation bias 3. Expectation bias 4. Recency bias + all in row immediately above	1 - 4. Failure to take account of changes in parameter in creating situation model. 1 - 4. Take an inappropriate action, take a correct action too soon, fail to take a needed action + all in row immediately above	1 - 4. Training/practice - Is the operators' training such that they might make assumptions about what the value of this parameter would be in this context and therefore not carefully consider it? 1 - 4. Procedures - Are there any aspects of the procedures called for by the other parameters, that could lead operators to ignore this parameter? + all in row immediately above
Low rate of change in parameter	1. Limited discrimination - Imperceptible change in display or functionally imperceptible given competing demands? 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias 6. Apathy - Lack of urgent consideration of parametric change	1 - 5. Lack of awareness that the parameter is changing; operators assume that the value is static 6. Operators defer action on the changes in the parameter until other parametric needs are addressed	1. HMI- Lack of trending displays (eg., use of analog meter display only) 1. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 6. Training/practice - Lack of discipline or trained practice in responding to all parameters

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
High rate of change in parameter	1. Fixation - Preoccupation with parameter 2. Incredulity - Disbelief in displayed changes (sensor or instrument error)	1. Lack of, or reduced, attention paid to other parameters and their changes 1. Stress from concern that the parameter is approaching a critical value much earlier than expected (may mismatch procedure). Stress may contribute to an inappropriate action, the taking of a correct action too soon, failure to take a needed action) 2. Failure to take account of changes in parameter in creating situation model	1. 1 Training/practice - Lack of discipline or trained practices in responding to all parameters 1.2 Training - Lack of training or practice for off-normal accident conditions (use of FRG procedures) 1.2 Procedures - Omission of guidelines for unexpected plant conditions 2. Training - Lack of training in responding to failed parameters 2. HMI - Experience with unreliable performance of the relevant parameters
Changes in two or more parameters in a short time	1. Need to search for a single common explanation for multiple changes	1. Delay in response while search is made for common explanation 1. Generation of false theories to explain coincidental changes in parameters	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Delays in changes in two or more parameters	1. Need to search for a single common explanation for existing changes. 2. Displayed parameters lead to entry into wrong procedure step 3. Displayed parameters match incorrect mental template (similarity matching) 4. Anticipation or confusion, overly eager to respond	1. Delay in response while search is made for common explanation 1. Generation of false theories to explain existing changes in parameters 2 & 3. Application of incorrect procedure step 3. Incorrect SA due to missing information 1 - 4. Take an inappropriate action, take a correct action too soon, fail to take a needed action.	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of delayed changes 2&3. HMI - Are there other indicators that might help the crew discover the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 2 &3 - Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters.

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
One or more false indications	1. Displayed parameters lead to entry into wrong procedure step. 2. Displayed parameters match incorrect mental template (similarity matching). 3. Complacency 4. Overly eager to respond 5. Simplifying 6. Indications misleading to the extent that operators do not consider other important parameters.	1. Application of incorrect procedure step 2, 5, 6. Incorrect SA due to missing information. 3. Operators defer action on the changes indicated by other parameters. 3. Fail to recognize a serious situation in time 2,4,5,&6. Take an inappropriate action, take a correct action too soon, fail to take a needed action.. 1,2,3,5,&6. Miss a decision point	1& 2 HMI - Are there other indicators that might help the crew discover the existence of the false indications? Are they located where they can be easily seen by one or more crew members most of the time? 1.& 2 - Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 3. Training/practice - Lack of discipline or trained practices in responding to all parameters 6. Training/practice - Similar event is used repeatedly in training or was addressed in training, or is given a lot of attention in training 1,2,3,5&6. Workload - Would the operators have to work hard to identify other sources of information that could help them detect the presence of the faulty indications? Could the workload become excessive or could the situation not seem important enough to induce them to search for verification?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Direction of change in parameter(s) over time is not what would be expected (if the base case scenario was operative vs. the deviation scenario) Direction of change in parameters over time, relative to each other, is not what would be expected. (if the base case scenario was operative vs. the deviation scenario) Relative rate of change in two or more parameters is not what would be expected (if the base case scenario was operative vs. the deviation scenario).	1. Expectancy bias or fixation (has been setup). 2. Operators are mislead by initial information (the information may or may not be incorrect) and fail to notice or appropriately consider later information (e.g., garden path problems, situations that change, red herrings) 3. Incredulity - Disbelief in displayed changes 4. Multiple lines of reasoning are created (conflicting choices, double binds, red herrings, dilemmas). 5. Reluctance to accept implication of later changes influences situation assessment (double binds)	1, 2,3,&4. Failure to take account of changes in parameters or fail to attend to more relevant parameters in creating situation model 13,4,&5. Generation of false theories to explain coincidental changes in parameters 1, 2,3,&5. Fail to recognize a serious situation in time 1, 2,3,4,&5. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1, 2,3,4,&5. Miss a decision point	1, 2,3,4,&5. Training - lack of training or practice for off-normal accident conditions. 1,2,3,4,&5 HM1 - Are there other indicators that might help the crew discover the existence or importance of the more recent information? Are they located where they can be easily seen by one or more crew members most of the time? 1,2, & 3. Training/practice - The event indicated by the initial parameters is used repeatedly in training or was addressed in training, or is given a lot of attention in training? 1,2,&3. Training - lack of training for unexpected conditions and problem-solving

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Behavior of apparently relevant parameters is actually irrelevant and misleading	1. Expectancy bias or fixation (has been set up). 2. Operators are mislead by initial information (the information may or may not be incorrect) and fail to notice or appropriately consider later information (e.g., garden path problems, situations that change, red herrings) 3. Incredulity - Disbelief in displayed changes 4. Multiple lines of reasoning are created (conflicting choices, double binds, red herrings, dilemmas) 5. Reluctance to accept implication of later changes influences situation assessment (double binds)	1, 2,3,&4. Failure to take account of changes in parameters or to attend to more relevant parameters in creating situation model 13,4,&5. Generation of false theories to explain coincidental changes in parameters 1, 2,3,&5. Fail to recognize a serious situation in time 1, 2,3,4,&5. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1, 2,3,4,&5. Miss a decision point	1, 2,3,4,&5. Training - Lack of training or practice for off-normal accident conditions. 1,2,3,4,&5 HMI - Are there other indicators that might help the crew discover the existence or importance of more relevant recent information? Are they located where they can be easily seen by one or more crew members most of the time? 1,2, & 3. Training/ practice - The event indicated by the initial parameters is used repeatedly in training or was addressed in training, or is given a lot of attention in training 1,2,&3. Training - Lack of training for unexpected conditions and problem-solving

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Cont.)

3. **Failures in Response Planning** - When particular parameter characteristics in Table 9.16a are identified as relevant descriptors of critical parameters in a scenario, this table is used to identify human error mechanisms that may facilitate *failures in response planning.* Possible generic UAs and potential PSFs that could contribute to the occurrence of a UA are also presented. *[Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.]*

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
No indication (or no change in the indication) for an important parameter	N/A		
Small change in parameter	1. Apathy - Lack of urgency in considering response to parametric change 2. Reluctance 3. Over eagerness 4. Forget about small change when developing response plan	1 & 2. Operators defer action on the changes in the parameter until other parametric needs are addressed. 1. Take an inappropriate action or fail to take a needed action due to discounting of small change 1 & 2. Fail to develop a response to a serious situation in time or develop a faulty response plan 1 & 2. Miss a decision point 3. Anticipate a situation and take an action too soon 3. Develop a faulty response plan	1. Training/practice - Lack of discipline or trained practice in appropriately responding to all changes in parameters 1 & 2. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately responding to the small change? 1 & 2. HMI - Are there other indicators whereby operators could determine the significance of the small change in the parameter 1. Training/practice - Trained to cross-check this parameter? 2. Training/practice - Operators are aware of negative consequences associated with the indicated response. 3. Training/practice - Changes in this parameter usually indicate a serious problem and a needed response

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Response Planning) (Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Large change in parameter	1. Fixation - Preoccupation with parameter 2. Incredulity - Disbelief in displayed changes (sensor or instrument error) 3. Over eagerness, over-rapid response 4. Displayed parameters match incorrect mental template (similarity matching). 5. Simplifying 6. Recency bias	1. Lack of, or reduced, attention paid to other parameters and their changes 1. Stress from concern that parameter is approaching a critical value much earlier than expected (may mismatch procedure). Stress may result in an inappropriate action, the taking of a correct action too soon, failure to take a needed action) 1,3. Rush to response overlook cautions, missteps in planning, con't question applicability, don't question conflicting information, don't wait for feedback 2. Failure to take account of changes in parameter in creating situation model 3,4,5&6. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1. Training/practice - Lack of discipline or trained practices in responding to all parameters 1. Training - Lack of training or practice for responding to off-normal accident conditions (use of FRG procedures) 1. Procedures - Omission of clear response guidelines for unexpected plant conditions 2. Training - Lack of training in responding to failed parameters 2. HMI - Experience with unreliable performance of the relevant parameters 2,4,5&6. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 2,3,4,5,&6. HMI - Are there other indicators that might help the crew verify the accuracy of the large change in the parameter? Are they located where they can be easily seen by one or more crew members most of the time? 2,4,5&6. Workload - Could the operators' workload, pre-occupation with other parameters, or exceptions about what is occurring on the basis of the other parameters keep them from appropriately considering a large or out-of-normal range change in this parameters?
Lower or higher than expected value of parameter	Same as in two entries immediately above	Same as in two entries above + delayed action	Same as in two entries immediately above
Low rate of change in parameter	Same as small change in parameter	Same as small change in parameter	Same as small change in parameter
High rate of change in parameter	Same as large change in parameter	Same as large change in parameter	Same as large change in parameter

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Response Planning) (Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Changes in two or more parameters in a short time	1. Need to search for a single common explanation for multiple changes 2.Simplifying 3. Saliency 4. Primacy 5. Availability	1. Delay in response while search is made for common explanation 1 - 5. Generation of incorrect response plans	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes
Delays in changes in two or more parameters	1. Need to search for a single common explanation for multiple changes 2.Simplifying 3. Saliency 4. Primacy 5. Availability	1. Delay in response while search is made for common explanation 1 - 5. Generation of incorrect response plans	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes
One or more false indications (one fits the other doesn't)	1. Need to search for a single common explanation for multiple changes 2.Simplifying 3. Saliency 4. Primacy 5. Availability	1. Delay in response while search is made for common explanation 1 - 5. Generation of incorrect response plans	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes
Parameters indicate response for which insufficient resources are available or indicate more than one response option.	1. Impasse in how to proceed 2. Response dilemma introduced 3. Trade-offs	1 - 3. Generation of incorrect response plans 1 - 3. Failure to a needed response	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Displayed information insufficient for guiding fine tuning of response planning

10 ISSUE RESOLUTION

ATHEANA has been developed with the intention of providing a way to evaluate issues associated with human performance. Given the increasing emphasis of the NRC on risk-informed regulatory activities, this will frequently require the use of quantitative PRA-based models. The following sections describe the use of quantification methods and incorporation of their results into PRA models. It is not inevitable that the method will always be used in this way. In many cases, it may be practical to use more qualitative assessments to resolve an issue. However, the qualitative resolution of the issues will require many of the same kinds of assessments that are required in the quantification process described below. The quantification process is demonstrated in the example analyses in Appendices B - E.

10.1 Process for Issue Resolution

As discussed in Section 1 of this report, ATHEANA has been developed to provide a tool to help in resolving issues that involve human performance in high-technology environments. Section 1.4 provided examples of issues that might be addressed and Section 9.1 discussed what types of ATHEANA applications might be used. Issues may be addressed in several ways:

- qualitative analysis
- simplified quantitative analysis, typically using relative ranking of alternatives and simplified PRA models
- extensive quantitative analysis, typically using more formal quantitative methods and standard PRA models

For historical reasons, together with the recognition that many applications will involve quantitative analyses with standard PRA models, the development of ATHEANA has included appropriate detailed guidelines to perform quantification and PRA incorporation steps; these are provided in Sections 10.2 and 10.3. The following discussion concerns the process when these steps are not used.

The selection of the appropriate type of analysis is strongly influenced by the issue being evaluated (Step 1) and any restrictions on its scope imposed in Step 2 of the process. For example, if the issue is in the form: "Is there a way in which operators may be misled into turning off safety injection prematurely during a medium-break loss-of-coolant accident ?" then the analysis does not need to be quantitative. The process steps described in Section 9 present a qualitative basis for making such a judgement, since the question makes no reference to how frequently such an event (or others like it) may occur. The issue is resolved by the answer: "We found under the following conditions ... that operators can be misled into terminating safety injection prematurely during a medium loss-of-coolant accident."

Under more typical applications of ATHEANA, it is likely that the issue will be phrased in a way that requires some statement about the relative or absolute contribution to risk. In terms of the relative risk contribution, the analyst may be required to consider how likely a particular unsafe action is, given the existence of a particular error mechanism. When a quantified probability is not required, these judgments can be simplified to a relative rating of "high," "medium," or "low." Such final judgments may allow the issue to be resolved if it involves choices between alternatives (for example, is design A better than design B?) In such cases, a PRA framework allows the analyst to set out the parameters that underlie the relative likelihood(s) of the HFE(s) of interest, such as the likelihoods of the initiating event, the EFC, and the conditional probability of the unsafe actions. It is recommended that analysts performing qualitative assessments become familiar with the process for quantification described below, but recognize that in many cases the judgments described can be performed in a ranking process, rather than by assigning specific probabilities.

It is also recognized that some analyses may use simplified PRA models, or that no model exists, but a risk-based framework is needed to resolve the issue. In many cases, PRAs exist that represent to some level of accuracy the plant and the systems being analyzed; for example, IPE PRAs exist for all U.S. nuclear plants. Therefore, in very few cases will the analyst need to create a new PRA model, rather than adapt an existing model. However, some IPEs do not contain sufficient detail for all kinds of issues to be addressed. For example, simplifying assumptions may have been made about the types of dependence between the so-called frontline and support systems. In other cases, bounding assumptions may have been made for success criteria that are very pessimistic. Therefore, the analyst must consider what changes may need to be made to the PRA model to make it adequate for addressing the issue of concern. Establishing the connection between the issue of concern and the PRA model may have been started in Step 2 of the process. However, before incorporating the results of the ATHEANA analysis into an existing PRA model, the analyst must be sure that the model is appropriately sensitive to the changes.

10.2 Guidance for Quantification

ATHEANA requires a somewhat different approach for quantification from those used in earlier HRA methods. Where most existing methods have assessed the chance of human error occurring under nominal accident conditions (or under the plant conditions specified in the PRA's event trees and fault trees), quantification in ATHEANA becomes principally a question of evaluating the probabilities of specific classes of error-forcing contexts (EFCs) within the wide range of alternative conditions that could exist in the definition of the scenario, and then evaluating the conditional likelihood of the unsafe action occurring, given the occurrence of the EFC.

10.2.1 Formulation of Quantification

The foundation for quantifying human failure events is to consider three separate but interconnected stages in the process:

- the probability of the EFC in a particular accident scenario

- the conditional likelihood of the UAs that can cause the human failure event
- the conditional likelihood that the UA is not recovered prior to the catastrophic failure of concern (typically the onset of core damage as modeled in the PRA)

While this three-step quantification process is not conceptually different from the approach in other HRA methods, there are two aspects that set this method apart. First, both the UA and the failure to take a recovery action can be extremely dependent on the context; therefore consideration of these parts separate from the context and from each other is not valid. For example, when the operators, based on their assessment of the situation, believe a system is not needed and turn it off, it is very unlikely that they would revise their assessment if there was little change in the context that led to the initial termination. Even in the face of subsequent cues, the initial context often controls operator performance, as discussed later in this section and as illustrated in several of the events described in Appendix A.

Second, the relationship between the UA and the recovery opportunity is strongly dependent. For example, during the accident at TMI-2, the operators persisted in their belief that high-pressure injection should remain throttled for several hours despite contradictory indications (see the discussion of the TMI-2 event in Appendix A). In other words, once an erroneous action has taken place, the operators can persist in that belief even when the context changes; people are often very persistent in maintaining an erroneous belief (see the discussion on the psychological bases of ATHEANA in Section 4).

10.2.2 Quantification Process

The three basic elements considered in the quantification process are:
- the probability of the EFC
- the probability of the UA
- the probability of not recovering from the initial UA

Each element is discussed in turn.

10.2.2.1 Quantification of EFCs

The EFC represents the combination of plant conditions and performance-shaping factors that are judged likely to give rise to the UA. For applications of ATHEANA that are extending analyses of existing PRAs, parts of the EFC are often determined by the accident sequence path on an existing event tree. These subsets include the initiating event frequency, a partial loss of equipment, and subcategories of events in the event tree.

For example, suppose the analysis being performed is of human actions that terminate coolant injection during a medium loss-of-coolant accident (LOCA). The PRA will have an event tree showing core damage resulting from failure to achieve adequate coolant injection. The conditions

under which operators can terminate injection will be defined by one or more paths in the tree. Therefore, once the identification of an appropriate initiating event has occurred and the corresponding event tree is selected, the purpose of this step is to calculate the probability of the context arising, given an initiating event. In some cases, the EFC may occur within the definition of an accident sequence within the event tree. In that case, it may be appropriate to model the EFC as a subset of the accident sequence. In this case, the calculation of the probability of the EFC would be conditional and dependent on the occurrence of the accident sequence.

There are two separate though strongly related elements to the EFC as described earlier: the plant conditions and the performance-shaping factors. Each of these is described below.

Plant Conditions

Plant conditions encompass the physical state of the plant, the operability of equipment, and operations and evolutions that are under way. For example, plant conditions would include the initiating event and its influence on the plant. For many EFCs, the initiating event would only partially define the plant conditions. For example, in the case of a medium LOCA, the plant conditions might only apply to a narrower range of leak rates than those defined by the specification of the medium LOCA. In addition, they may include unusual failure modes or abnormal behavior of equipment modeled in the PRA and equipment not generally modeled in the PRA, such as the displays and related parts of the instrumentation and control systems.

In order to quantify the probabilities of these conditions, the ATHEANA team must gather plant-specific information. The information to be gathered depends on the EFC defined using the guidelines in Section 9. Information that might be required may include the following examples:

- frequencies of initiators (especially those defined in more detail than provided in the PRA)
- frequencies of certain plant conditions (e.g., plant parameters, plant behavior) within a specific initiator type
- frequencies of certain plant configurations, evolutions, etc.
- failure probabilities for equipment, instrumentation, indications, etc.
- dependent failure probabilities for multiple pieces of equipment, instrumentation, indicators, etc.
- unavailabilities of (especially, multiple) equipment, instrumentation, indicators, etc. due to maintenance or testing
- frequencies of restoration, calibration, and other latent human failures that result in failed (especially, multiple) equipment, instrumentation, indicators

- the probability of specific performance-shaping factors (PSFs) being present as defined in Steps 6 and 7; evaluation of additional complexity

The information needed to quantify the likelihood of the EFC using ATHEANA will depend upon the specific EFC elements identified in the search process. Since specific EFC elements and plant-specific information sources are not predictable, this section describes the collection of information in a general sense only. The ATHEANA team also must consider the plant-specific information resources that are available to them for quantification purposes.

There are several ways in which the ATHEANA team may derive information on plant condition and hardware (listed in order of preferred use):

(1) statistical analyses of operating experience
(2) engineering calculations (using assumptions, estimates, etc.)
(3) quantitative judgments from experts
(4) qualitative judgments from experts

Plant-specific operational experience (e.g., plant trip history, equipment failure histories, maintenance logs) is the principal source of statistically derived information. The ATHEANA team may have already derived some information (e.g., initiating event frequencies) for the purposes of the PRA. The team may use industry information (e.g., generic operational experience, vendor data) if plant-specific information is not available or is too sparse.

The ATHEANA team may use engineering calculations to derive EFC element probabilities or frequencies if operational experience is not available, either because the contextual factor rarely occurs or because data are not directly collected for a specific parameter or factor. Examples of such engineering are:

- the likelihood of equipment being demanded in certain situations (e.g., likelihood of a power operated relief valve (PORV) demand given a loss of offsite power transient)

- the probability of a fire spreading, once it has begun

- the time between loss of heating, ventilation, and air-conditioning (HVAC) systems and the occurrence of a room high-temperature alarm or actual temperature-related failures of equipment

In some cases, the ATHEANA team may use existing calculations (e.g., those performed to support the PRA, those used to support other engineering analyses or licensing submittals). In other cases,

new calculations may be performed or judgments made that are based on estimates using available information and simplifying assumptions.[1]

If data are not available to derive the necessary frequencies or probabilities, then the ATHEANA team should interview plant personnel in order to derive the inputs necessary for quantification. In order to elicit these expert judgments, the team should seek out the plant personnel with the appropriate topic-specific knowledge and experience. Often plant experts are unable to provide quantitative inputs directly in the form needed for quantification. The team should construct interview questions that allow the experts to use their knowledge bases. The team then will need to interpret the information provided and transform it into the form required for ATHEANA quantification. In some cases, plant-specific experts may be able to provide rough quantitative estimates based upon their past experience and knowledge that require little manipulation to transform them into inputs. In other cases, they may be able to provide only qualitative estimates that will require greater interpretation and manipulation (and probably some judgment on the part of the ATHEANA team) before producing the appropriate inputs for quantification.

Performance-Shaping Factors

Section 9.7.1 discusses two types of PSFs:

- PSFs that are triggered or activated by the plant conditions for the specific deviation scenario defined in Steps 6 and 7

- other PSFs that are not specific to the context in the defined deviation scenario

In many cases, activated PSFs will have a probability of occurrence equal to or nearly 1.0. It is critical that such activated PSFs be assessed only with respect to the context of the defined deviation scenario, and not the expected one or some other situation. For those situations in which the activated PSF is a given for the context, the probability of occurrence is 1.0. Appendices B through E contain examples of activated PSFs (such as no procedural guidance, training, or indications available for the specific context). Operator trainers or other knowledgeable plant staff should be consulted in estimating the probability of occurrence if the activated PSF is not a given. So far, there are several possibilities for the dominant factors to be considered in such an assessment. For example, within the range of conditions defined by the deviation scenario, the PSF may be a given for only a certain range of conditions. In such a case, if the frequency or probability of these conditions can be determined, then the activated PSF can be assessed. Another example would be the assessment of operator trainers that a negative PSF influences a certain fraction of the operating crews. Other possibilities for such PSF assessment will be highly dependent upon the specific deviation scenario and plant.

[1] As in any PRA analysis, assumptions should be documented. Also, if the associated HFE probability results in either a very high or very low value, the assumptions ought to be reexamined for overconservatism or oversimplification.

PSFs that are not specific (i.e., generic) with respect to context will still be plant specific.[2] First, analysts should verify that there are no plant conditions that would make the PSF more likely. If such is the case, then the analysts should consider adding these conditions to the EFC, following the guidance given in Steps 6 and 7.[3] For these cases, the analysts should follow the guidance given in the paragraph above.

If the PSFs are truly not tied to specific plant conditions, then operator trainers and other plant-knowledgeable staff should be consulted in assessing the likelihood for these PSFs. For those PSFs that are not triggered by the plant conditions, the focus of the identification of additional PSFs should be on those whose influence will be to increase the likelihood of the combination of the EFC and the UA. The addition of any non-triggered PSFs will inevitably reduce the probability of the EFC but will increase the probability of the UA, given the occurrence of the EFC. The net effect of these changes in probabilities can, in principle, either increase or decrease this combination. The analysis should focus on these PSFs where the combined probability increases. Clearly, some initial investigation is required to determine whether such a change is likely for candidate PSFs. The probability of some PSFs (e.g., suboptimal performance due to time of day or abnormal crew makeup) can be estimated from historical records (e.g., percentage of hours operated in early morning shifts, frequency of changes in the normal crew assignments). Other PSFs may be linked to a variety of factors, including informal rules (i.e., "the way we do things around here"), on-the-job training, operating and simulator experience, control room and plant design, etc. Like the assessments made for activated PSFs, these generic PSFs may or may not have a probability of occurrence equal to or nearly 1.0. In either case, the judgment of plant experts, coupled with that of the analysts applying ATHEANA, forms the basis for assessing the likelihood of these PSFs occurring.

10.2.2.2 Quantification of Unsafe Actions

There are three types of conditions that can determine how the probability of an unsafe action is estimated:

(1) The EFC is so compelling that the occurrence of the UA is virtually certain.

(2) The EFC is so noncompelling that there is no increased likelihood of the UA compared with the routine PRA context.

(3) The extent to which the EFC is compelling lies somewhere between these extremes.

---

[2] As noted in Section 9.7.1, analysts should be prudent in including such generic PSFs in the EFC. If such PSFs are judged to significantly affect the likelihood of the unsafe action occurring (i.e., the point of the next section, Section 10.2.2.2), then they should be included.

[3] This iteration in the ATHEANA process is normal and expected.

At this stage of development in ATHEANA, it is recommended that the analysis initially estimate the likelihood of an unsafe action occurring without demanding a high level of precision. In other words, for condition 1 above, the likelihood of the unsafe action occurring would be estimated at 0.5. Such a probability would be appropriate in those cases where the context faced by the operators seems entirely consistent with the operators' belief that the UA is the right thing to do in the circumstance. An example would be an event where plant information is failed or misleading, but meets procedural criteria for which there is limited or negligible redundancy, and the action is normal and expected for what the operators believe is happening. In other words, the context is overwhelmingly compelling.

For condition 2, the EFC may be considered exceptionally weak. In such cases it is recommended that the analysts use the HRA method that was used, for example, in the PRA that is being extended. In those cases where no PRA exists, the analyst is directed to the types of more traditional HRA methods, such as those discussed in Reference 10.1, which are not intended to be so focused on EFC-driven errors. (In practice, it may be that conditions that are not significantly error forcing would be identified and eliminated in the evaluations in Steps 6 and 7 of the process, which ask in effect, "Is this scenario worth considering further?")

In practice, many if not most of the contexts will fall between these extremes. In these cases, there are two possibilities for estimating the likelihood of the unsafe action given the context. These are:

(1) *Situations where experienced operator training staff have observed similar plant conditions in training and have observed a consistent fraction of crews taking the UAs being modeled.* In this case, the probability of the UA, given the plant condition, is estimated on the basis of the trainers' experience. Similarly, it is possible to poll or evaluate different crews in those cases where the action and the context are specific, but the factors that different crews may weigh are somewhat uncertain. Also, simulator trials for the UA and the associated deviation scenario can be developed and performed to inform the judgments of operator trainers if there is no relevant past experience.

(2) *Situations requiring estimation of the likelihood of a UA using modeling methods.* In this case, the analyst must employ one or more tools to provide a basis for quantification. Inevitably this will require some judgments to be made by the ATHEANA analysis team, as discussed below.

The preferred situation is one in which operator trainers can provide expert judgment as an input to the quantification of unsafe actions. However, if they are unable to provide this input (because there is no past experience or the operators, trainers, and simulator are unavailable), then modeling methods are the next best choice. Both of these approaches are discussed below.

Expert Judgment of Operator Training Staff

In those cases where the training staff have a body of experience to make judgments about the likelihood of unsafe actions because they have seen similarly challenging contexts, it is appropriate

to use this experience as a basis for quantification since it is plant and training specific. Also, simulator trials or talk-throughs of the specific EFCs may inform trainers sufficiently to make the necessary judgments.

Operator trainers are most able to provide quantitative or qualitative assessments because:

- They have the broadest knowledge base of plant-specific operating experience (i.e., their own and that of all shift and staff crews licensed at their plant).
- Because of their observations of simulator exercises and knowledge of actual operating experience, they know best how the operators at their plant perform.
- They have observed and collected statistics regarding failures in simulator exercises and, therefore, are likely to have some understanding of likelihoods for failures.
- They know how to create scenarios on the simulator that will cause operating crews to fail.

As discussed in Section 7, it is expected that training staff will be a part of the group of analysts performing ATHEANA. Also, it is expected that simulator exercises would be useful in the development of EFCs. Consequently, if the analysts have not yet used both of these resources in the ATHEANA process, they should do so now, if possible. Not only can simulator exercises support the trainers' judgments for quantification, but they can also be used to validate that the EFC is indeed challenging to operators and is likely to result in the predicted UA(s). Experience in applying ATHEANA documented in an earlier draft of this report (Ref. 10.2) showed that the training staff were invaluable in helping to define the EFC through development of the simulator trial and because of their knowledge and experience. In addition, actual performance of the simulator trial was valuable, informative, and even a little surprising to all analysts involved, including the trainers.[4]

In general, no new guidelines are proposed for performing this activity since several existing techniques are available for structuring the estimation of such probabilities [e.g., as those discussed by Seaver and Stillwell in NUREG/CR-2743 (Ref. 10.3), Budnitz et al. (Ref. 10.4), and Otway and von Winterfeldt (Ref. 10.5)]. In addition, the analyses provided in Appendices B through E and the early demonstration given in Ref. 10.2 can be used as illustrative examples of this approach to UA quantification.

Modeling Methods

In the second situation, where the analysts rather than the operator training staff must make some judgment of the likelihood of a UA, there are several approaches that can be followed. The following discussion provides two separate bases for estimating the probability. In both cases, what

[4] Based upon the results of the simulator trial performed in this early demonstration, the plant trainers decided to include this scenario in next year's training.

is required is a judgment about how relatively forcing or compelling the context is. That is, the end points of the range of possible probability values are known–they are a probability of 1.0 at one extreme and the human error probability estimated by a traditional HRA method that takes, at most, some minimal account of a "bad" context (e.g., time available or layout of a panel) at the other. Quantification of the UA in ATHEANA, therefore, must estimate where, relatively speaking, the influence exerted by the context lies. Figure 10.1 shows this concept as a graphic representation.

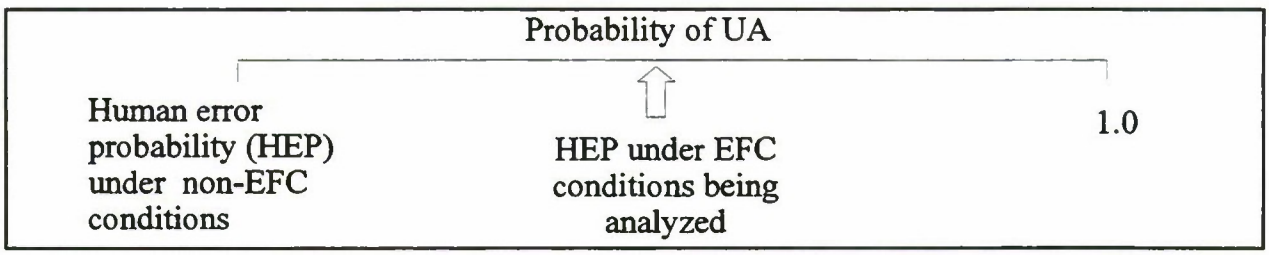


Figure 10.1 Representation of Estimation of UA Probability

In order to decide where the conditions being analyzed lie, the following guidelines are provided. It is recognized, however, that there are no absolute methods for making this judgment. The most important part of this process is for the analyst to explain the basis for the assessment, what factors are considered important, and why.

First, one HRA method, HEART (Ref. 10.6), does provide a basis for assessing the degree to which a context influences the likelihood of failure. The HEART method consists of two steps to quantify the likelihood of a UA. First, the analyst identifies a generic task description that most closely corresponds with the context of the action being analyzed. Generic task descriptions, together with their associated failure probabilities (both point value and uncertainty range), are shown in Table 10.1.

Following selection of the generic task description, there are a series of performance-shaping factors to use in adjusting the failure probabilities. (See Table 10.2.) Users wishing to use the HEART method should see Ref. 10.6 for details of applying the method in practice. In particular, use of HEART requires attention to the combinations of generic task descriptions and PSFs in Tables 10.1 and 10.2 to ensure that they do not "double-count" factors. For example, if the generic task description includes the condition that the task is "totally unfamiliar," then one does not also apply a factor for "unfamiliarity with the situation" since the effect of the EFC is already contained in the generic task probability. In addition, the application of the PSFs should be limited to the most significant two or three at the judgement of the analyst. Finally, and most obviously, the addition of PSFs to the generic task probability should be undertaken with care as the final probability of failure approaches 1.0. It is suggested that when the calculated probability exceeds 0.5 to 0.6, the analyst should carefully consider and limit the need for any additional factors. In addition, events with probabilities estimated in the range 0.1 and higher should be subject to a review process to ensure that the estimates are not overly pessimistic.

Table 10.1 HEART Generic Task Failure Probabilities

Generic Task Description	Failure Probability
Totally unfamiliar, performed at speed with no real idea of likely consequence	0.55 (0.35 – 0.97)
Complex task requiring high level of comprehension or skill	0.16 (0.12 – 0.28)
Fairly simple task performed rapidly, or given scant attention	0.09 (0.06 – 0.13)
Routine, highly practiced, rapid task involving relatively low levels of skill	0.02 (0.007 – 0.045)
Shift or restore system to a new or original state following procedures, with some checking	0.003 (0.0008 – 0.007)
Completely familiar, well-designed, highly practiced routine task occurring several times per hour, performed by highly motivated, highly trained and experienced person who is totally aware of the implications of failure, with time to correct potential errors, but without the benefit of significant job aids	$4x10^{-3}$ ($8\times10^{-4} – 9x10^{-3}$)
Respond correctly to system commands even when there is an augmented or automated supervisory system providing accurate interpretation of the system state	$2x10^{-5}$ ($6x10^{-6} – 9x10^{-4}$)

Table 10.2 HEART Performance-Shaping Factors

Error-Forcing Context	Maximum Increase in Failure Probability
Unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel	17
Insufficient time available for error detection and correction	11
A low signal/noise ratio	10
A means of suppressing or overriding information or control features that is readily accessible	9
No means of conveying spatial and functional information to operators in a form they can readily assimilate	8
A mismatch between the operators' model and that imagined by the designer	6
No obvious means for reversing an unintended action	5
A channel capacity overload, particularly one caused by the simultaneous presentation of nonredundant information	6
A need to unlearn a technique and apply another that requires the application of an opposing philosophy	6
The need to transfer specific knowledge from task to task without loss	5.5
Ambiguity in the required performance standards	5
A mismatch between the perceived and the real risk	4
Poor, ambiguous, or ill-matched system feedback	4
No clear, direct and timely confirmation of an intended action	4

Table 10.2 HEART Performance-Shaping Factors (Cont.)

Error-Forcing Context	Maximum Increase in Failure Probability
Inexperienced operator	3
Impoverished quality of information conveyed by procedures and person to person interaction	3
Little or no independent checking or testing of outputs	3

The failure probabilities calculated using HEART are typically higher than the more traditional HRA values. For example, human error probabilities in those situations where the EFC is noncompelling very often lie in a range with a lower limit of 10^{-3} to 10^{-4}, as shown by the evaluations of IPEs in NUREG-1560 (Ref. 10.7), though events for which (for example) there is a limited time for actions may have significantly higher probabilities.

In the second approach, the following approach can be used to estimate where, in the range of EFC conditions portrayed in Figure 10.1, the conditions being analyzed lie, and an interval- or scale-based tool such as the success likelihood index method (SLIM) (Ref. 10.8) can be used to estimate the failure probability.

In applying this approach, there are several questions that must be answered. These are:

- Given the context, what is the likelihood of the error mechanism being triggered?
- Given the error mechanism being triggered, what is the likelihood of the unsafe actions occurring?
- Given the occurrence of unsafe actions, what is the likelihood that they will lead to the human failure event and consequential plant damage?

SLIM can be used for each of these steps, or the assessment can be performed as an integrated assessment. The example studies in Appendices B-E principally illustrate assessment in an integrated manner.

In reviewing the characteristics of challenging conditions in Tables 9.15b and 9.16b while developing the scenario deviations, the analysts will note that specific PSFs and plant conditions are associated with specific error mechanisms and conditions. In almost all the searches used in Section 9.6, the search focuses on error mechanisms through the use of Tables 9.15 and 16. (The exception is the search for error types in Section 9.6.6 and is discussed separately below.) The more such negative PSFs and plant conditions are present in the scenario, the more likely is the occurrence of the error mechanism and, potentially, the unsafe action. Therefore the first step in assessing the

likelihood is to judge which of the plant conditions and PSFs associated with the particular error mechanisms are most important, and second the degree to which these PSFs exist in the scenario being analyzed. Analysts experienced with SLIM will recognize that these kinds of judgments are commonly performed in such cases. Since in most cases there are only a few PSFs and plant conditions identified for a particular error mechanism, the SLIM rankings and weightings can be performed efficiently on these factors.

The second stage of the assessment, the likelihood of the unsafe action given the occurrence of the error mechanism, can be assessed, again using a ranking scale. As an initial input to the analysts' judgment, the following error mechanisms are considered potentially very likely to result in an unsafe action should they occur:

- tunnel vision
- fixation
- confirmation bias
- complacency
- satisfying
- incredulity
- simple explanation for complex problems
- garden-path events
- misleading information
- masking events
- high-tempo multitasking events

This ranking is based in the number and relative severity of events that have occurred that have involved the mechanisms.[5] Events in which these error mechanisms are present can be considered to have a high likelihood of the unsafe action occurring. (The extent to which the mechanism is likely to be present was assessed in the previous step, based on the plant conditions and PSFs.)

In addition, a few error mechanisms were considered to have a low likelihood of leading to an unsafe action in a nuclear power plant setting:

- limited discrimination
- reluctance
- impasse
- late changes in plans

The remainder are assessed as having a moderate likelihood of leading to an unsafe action in a nuclear power plant setting.

---

[5] Event analyses that have been performed to support ATHEANA, as well as independent analyses of nuclear and non-nuclear events by others (e.g., Refs. 10.9 through 10.12), are the basis for this statement.

In general, the suggested strategy for judging the likelihood of an unsafe action implies that if any of the more global mechanisms (such as those listed in Table 9.15a, Section 9) appear to be operative in a scenario, then the unsafe action can be judged to be likely.

10.2.2.3 Quantification of Recovery

The final stage of the assessment process is to assess the likelihood that the unsafe action will persist into the failure event and therefore cause the undesired outcome–usually core damage conditions in typical power-plant PRA contexts. This third stage focuses on several recovery issues that may prevent the unsafe action from continuing to the point of core damage. These issues are:

- the occurrence of alarms and other indications following the unsafe action that may raise questions as to the correctness of the actions taken or not taken
- opportunities for new crew members (i.e., those not involved in the unsafe action) to question the on-going response
- the potential for consequential changes in the plant state to lead to new alarms and indications

Analyzing the opportunities for each of these to lead to an effective recovery of the unsafe action and termination of the accident sequence requires a somewhat detailed assessment of what the time scale is for the remainder of the accident sequence, what cues will occur, and how these cues will be assessed in light of the initial error mechanisms and the resulting unsafe action. The example analyses presented in Appendices B - E show the level of detail that can be required to assess the opportunity for recovery. For example, the sequence of cues over time must be compared with the time available for recovery in the context of the initial and developing sequences. Then the analyst must evaluate the total probability of nonrecovery for the chain of cues that will develop during the available time. (Note that the length of this chain may be uncertain. If so, then quantifying nonrecovery for the various possible cue chains, weighted by each chain's likelihood of being the correct length, will be a strong measure of the overall uncertainty in quantification of the HFE.)

Quantification of the probability of nonrecovery for the chain of cues is conditional on the original EFC, the UA, and the revised context that arises out of the UA and consequent chain of cues. There is no formula for this process. The process relies heavily on judgment based on the knowledge used in the previous steps in the quantification.

An example from an earlier ATHEANA publication (Ref. 10.13) assists the analyst in assessing the significance of context in creating a strong dependent effect. The example is based on an event at Oconee 3 that occurred during shutdown conditions in 1991 (Ref. 10.14). Before stroke testing the decay heat removal (DHR) suction valve from the recirculation sump, an operator attached a blind flange to the drop line and verified it in place. This is the large line that is used for open-loop recirculation cooling following a LOCA. Immediately after the valve was opened, a reactor building

emergency sump high-level alarm was activated. The operator took no action because this is a small sump to collect minor leakage and it fills and is pumped down routinely. The operator did not suspect a connection with the valve manipulation on the RCS boundary. So the first cue came and went without being recognized as evidence of a problem.

A short while later the second cue occurred. The operator observed that the reactor vessel level had dropped to 20 inches and was decreasing. The following table lists the full chain of cues that were generated by this event. For purposes of discussion, assume that this is the list of cues developed by the analysts to support their recovery analysis:

Table 10.3 Potential Recovery Opportunities, Oconee, 1991

Accident Symptom or Cues
E_1. Reactor building emergency sump high-level alarm
E_2. Reactor vessel level reading at 20 inches and decreasing
E_3. Reactor building normal sump high level alarm
E_4 Reactor vessel ultrasonic low level alarm (i.e., no water in hot leg pipe nozzle)
E_5. High pressure in reactor building verifies reduction in reactor vessel level and increasing radiation
E_6. Low-pressure injection (LPI) pump A current fluctuating downward
E_7. Evidence that reactor coolant system is not refilling

Now the recovery analysis would ask, "What is the probability of nonrecovery (within the available time) given the original EFC, the UAs (which have not yet been completely described), and the changes in context as a result of the UA and the string of cues." Without a consideration of the EFC and changes in context, traditional approaches that assume that the associated nonrecovery probabilities are independent would generate a probability of nonrecovery that is very low indeed. In fact, the individual non-recovery probabilities $\overline{R_1}$, $\overline{R_2}$, ,... would be expected to be quite low. The argument might proceed as follows:

> *The operators have stroked a valve on the RCS boundary that is protected by a temporary blind flange, potentially opening a path to containment. It is possible that they could consider E_1 as the normal result of leakage in containment, but it is a potentially significant cue and would be investigated. Let us assign a typical conservative non-recovery probability of 0.1.*
>
> *Now, when observation shows the reactor vessel level to be decreasing, it is nearly certain that the operators will close the sump valve. They have clear evidence of a loss of RCS inventory and will certainly respond to the loss of coolant. From*

THERP (Ref. 10.15) Table 15-3 for errors of omission in carrying out written produces, we estimate the probability of $\overline{R_2}$ as 3×10^{-3}. Thus the nonrecovery probability after E_2 is $\overline{R_1} \times \overline{R_2} = 3 \times 10^{-4}$.

As the analysis continues, it is probable that the most conservative value assigned to the individual nonrecovery factors is 0.1. Let us assume that our analysts' thermal-hydraulic analysis found that by the time cue E_6 arrived, damage would already be present. In that case, the total nonrecovery probability (through E_5) would be 3×10^{-7}. But this event actually continued through E_7 over a period of about 23 minutes before the operators decided to check the line that *they had opened* to the sump, as shown in Table 10.4. Previous circumstances set them up so that they were unable to view the sequence of events as evidence of what really occurred.

Table 10.4 Recovery Opportunities vs. Actions Taken

Accident Cues	Recovery Opportunity (Table 10.3)	Actual Recovery Response
Reactor building emergency sump high-level alarm	E_1	None
Reactor vessel level reading at 20 inches and decreasing	E_2	Erroneous operation of reactor vessel wide-range level transmitter suspected
Reactor building normal sump high-level alarm	E_3	Washdown operations suspected
Reactor vessel ultrasonic low level alarm (i.e., no water in hot leg pipe nozzle)	E_4	Investigation of cause begun Entered procedure AP/3/A/1700/07, loss of LPI in DHR mode
High-pressure in reactor building verifies reduction in reactor vessel level and increasing radiation	E_5	None
Low-pressure injection (LPI) pump A current fluctuating downward	E_6	Stopped pump Opened borated water storage tank (BWST) suction isolation valves
Evidence that reactor coolant system is not refilling	E_7	Reclosed BWST isolation valves NLO sent to close 3LP-19 or -20
Event stabilized		

10.2.3 Representation of Uncertainties

Uncertainties exist in the estimates of the probabilities of the EFC, the UAs, and the recovery. The probabilities of the plant conditions are largely derived from plant experience or other operating data in the same way that many other parameters are derived in the traditional quantification tasks of a PRA. The approaches used in those traditional approaches are similarly appropriate here. For those PSFs that are independent of the context, an approach to estimating the uncertainties in the plant experience or judgment can be used that is similar to that used for uncertainties in the probabilities of the plant conditions. For those PSFs that are inherently associated with the plant conditions (such as procedures that are not applicable in the plant conditions), in most cases these PSFs have a probability of 1.0, given the plant conditions, and do not have an associated uncertainty separate from that of the likelihood of the plant conditions themselves.

In the case of the UAs, as discussed earlier, there are three different ways in which to estimate the probabilities. Different strategies provide estimates in the uncertainties in each case. First, in those cases where the probability of the UA occurring is judged to be virtually certain, the recommendation is to use an uncertainty range of 0.5 to 1.0.

Second is the case where staff have a body of experience in training for similar scenarios in which a consistent fraction of crews commit the UA of concern. If the numbers of crews being evaluated and the number of times they commit the UA are recorded, these data can be used to develop an uncertainty distribution. If experienced individuals provide the estimates and there are no recorded data, then processes exist to generate an uncertainty distribution on the basis of their collective estimates.

With regard to the use of the HEART method, uncertainty ranges are provided for the probabilities of failure for the generic task descriptions. These should be used consistent with the guidelines of the HEART method itself.

10.3 Guidance for PRA Incorporation of HFEs

Defining the HFEs, particularly in relation to the PRA, has been previously covered in Step 4 of the ATHEANA search process documented in Section 9. This guidance regarding the incorporation of the HFEs into the PRA model addresses only post-initiator HFEs. Since it is assumed that all U.S. plants already have completed human reliability analyses (HRAs) as part of their IPE submittal, the focus of this guidance is the addition of ATHEANA-generated post-initiator HFEs to PRA models, and not the modification of currently modeled HFEs. Specifically, the focus is on new errors of commission that would be identified as a result of applying the ATHEANA search scheme.

Before providing guidance on the incorporation of such events into the PRA model, it is valuable to first provide an overview of a typical PRA model as a basis for understanding how that model may need to be modified.

10.3.1 Overview of the Typical PRA Model

There is considerable variety in the details of how different PRA analysts construct a PRA model for depicting nuclear power plant severe accidents. However, nearly all recent PRAs, including those performed in response to Generic Letter 88-20 and the IPE program, use inductive logic models called "event trees" in combination with deductive models called "fault trees."

An event tree is a pictorial representation of the possible sequences of events that can occur following some initial challenge to plant operation, called an "initiating event." These sequences are usually depicted by the success or failure of functions or systems that are significant in mitigating the effects of the initiating event. Necessary and sufficient combinations of functional and system successes lead to a successful plant response to an initiating event; while sufficient failures are predicted to lead to damage to the reactor core, fission product release, and possible containment failure and release to the environment.

Fault trees are mostly used to model plant responses at a lower, more detailed component level. Fault trees are deductive models that depict the combinations of failed equipment that must occur in order to fail the functions and systems of interest in the event trees. The basic events in the fault tree models represent the unavailability or failure states of plant equipment, with the models constructed at a level commensurate with available failure data.

"Quantifying" the PRA means calculating the predicted frequencies of the sequences of events that lead to core damage. This is accomplished conceptually by first determining the probabilities of failure of the functions or systems in the model. The combination of these probabilities with the expected frequencies of the initiating events determines the expected frequencies of the undesirable core damage sequences. The resulting solution process provides a series of expressions, each made up of the product of the initiating event and various basic event failures that together lead to damage to the reactor core. Each expression is called a cut set with each cut set having an associated frequency. Combining the frequencies of each cut set related to a single sequence yields an overall frequency for that sequence. Combining the sequence frequencies yields the overall expected rate of occurrence (usually expressed as a probability per year) of core damage.

Figure 10.2 is a simplified depiction of how the above modeling and data interrelate to form the PRA model. The extent to which the different modeling techniques are used and combined depends on such things as PRA scope and plant mode being analyzed (e.g., full power, refueling), analyst preference, and whether a detailed or only a screening analysis is required, among other factors. However, the above description, at least conceptually, encompasses the typical PRA modeling approach used by today's analysts.

10.3.2 Treatment of Human Failure Events in Existing PRAs

In order to address how to include the ATHEANA human failure events in the PRA model, it is first necessary to understand how PRA models typically incorporate human failure events. There are four

places where human failure events are typically incorporated into the PRA model. These are shown in Figure 10.3 by highlighting the human modeling interfaces with the basic PRA model depiction shown in Figure 10.2. Each interface is discussed below.

10.3.2.1 Human-Induced Initiating Events

The first place in the PRA model structure where human failure events are included (albeit implicitly) is in the identification of the initiating events and their expected frequencies. For a typical at-power PRA, initiating events include such challenges to the plant as turbine trips, loss of feedwater, steam generator tube rupture, loss of offsite power, loss-of-coolant accidents, inadvertent flow diversions during shutdown, earthquakes, etc. Many of these initiators can be induced by human failures, such as inadvertently causing a reactor scram during a half-scram test of the reactor protection circuitry. Since the frequencies of such initiating events induced by human failure are accounted for in the frequency for each class of possible initiators, oftentimes these events are not specifically modeled in the PRA. This is done for three reasons: first, it is assumed (even if implicitly) that there is little or no dependence between the cause of the initiating event and how plant staff will respond to subsequent events. Second, depending on the scope and objectives of the analysis, usually the PRA analyst only requires the initiating event frequency for the analysis and it is not necessary to understand why or how the event is initiated. Third, in at-power PRAs, the human contribution to initiators is often considered to be small compared with that of hardware failures.

10.3.2.2 Human Failure Events in Event Trees

Oftentimes the event trees in the PRA model explicitly depict human failure events in the logic. Figure 10.4 provides an illustration. There is no industry-wide accepted rule or standard as to when to include such events in the event tree structure. However, this is usually done when the human action of interest is a key part of numerous sequences in the event tree and the action is not particularly associated with a specific system or equipment item, but instead has functional repercussions regarding whether there is a successful recovery or whether core damage occurs. Sometimes, such events must be included in event trees to highlight the human failure event as a potentially important part of the entire sequence of events that might occur. In current PRAs, these human failure events nearly always involve errors of omission, such as failure to depressurize the primary system when a steam generator tube is ruptured, failure to initiate feed and bleed, or failure to provide coolant level control in a boiling-water reactor (BWR) anticipated transient without scram (ATWS).

10.3.2.3 Human Failure Events in Fault Trees

Such human failure events may be modeled in the appropriate fault trees if the action of interest is more easily associated with a specific system or equipment item in the plant, and failure of that action can contribute to the failure of that system or equipment to perform its desired function. Figure 10.5 provides an illustration. Here the analyst attempts to define all the ways that human

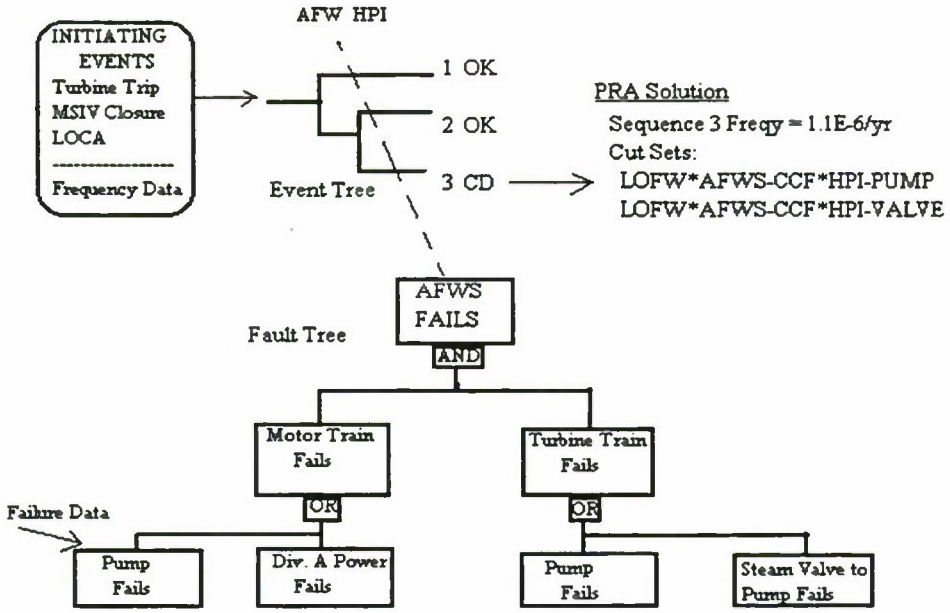


Figure 10.2 Overview of PRA Modeling.

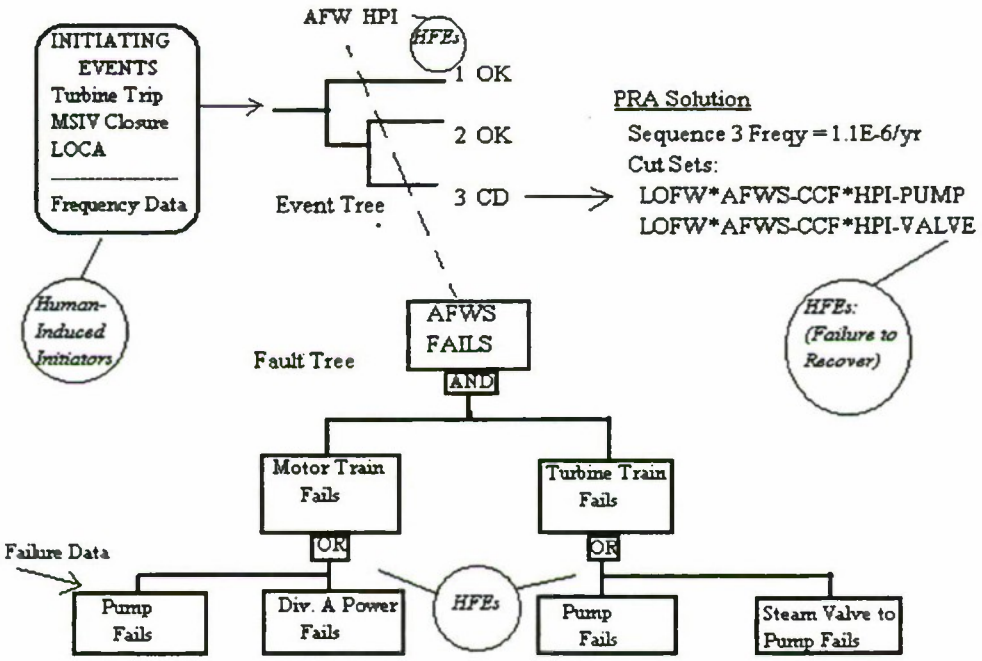


Figure 10.3 Overview of PRA Modeling with HFE Interfaces Shown.

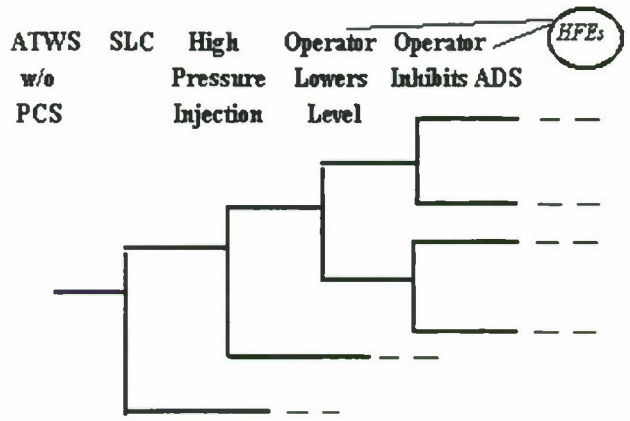


Figure 10.4 Illustration of HFEs in Event Trees

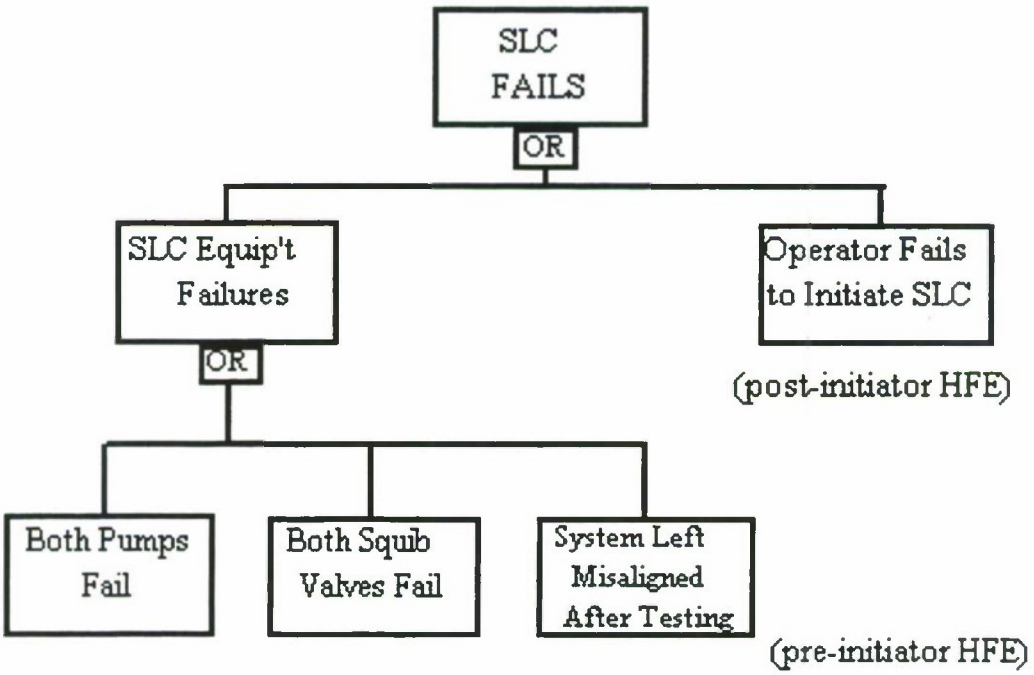


Figure 10.5 Illustration of HFEs in Fault Trees.

failures can credibly contribute to failure of the system or equipment of interest and estimates the probability of that failure, eventually in the context of each sequence in which the failure of that system or equipment plays a role. The human failure events in the fault trees tend to include the following:

- so-called pre-initiator errors involving omissions in maintenance, testing, or calibration activities that leave the equipment in a nondetected failed state so that the equipment cannot respond properly when an initiating event occurs

- post-initiator events such as that shown in Figure 10.5 involving omissions in responding to sequences of events following an initiating event

10.3.2.4 Failures to Perform Specific Recovery Actions

Not every combination of equipment failure that leads to core damage can be predetermined before the model is solved, and for other calculation and modeling efficiency reasons, a variety of failure-to-recover events are added to the PRA model during the last stages of quantification. This involves analyst examination of the sequence cut sets derived from solution of the PRA model, and on the basis of the combinations of failures in each cut set leading to core damage, the analyst postulates reasonable recovery actions that can be taken by the plant staff to change the outcome from core damage to successful mitigation of the accident. Failure to take the desired recovery actions is included in the PRA model. This is done by adding events representing such failures to the sequence cut sets, thereby accounting for the probability that the plant staff will not be able to find a way to avert the core damage outcome by performing an action not explicitly included in the original model. Examples of such failure-to-recover events and how they are implemented in the model cut sets are shown in Figure 10.6.

10.3.3 Incorporating ATHEANA Human Failure Events in the PRA Model

The following sections offer recommendations on how to incorporate the ATHEANA-defined human failure events in an existing typical PRA model.

10.3.3.1 Human-Induced Initiating Events

Since plant and industry experience data are used to identify and quantify the frequencies of most initiating events, no general requirement exists regarding the decomposition of initiators into those that are human induced and those that are not. Nor is it necessary to model how such human-induced initiators might occur. Examination of actual experience can provide these insights and hence, by using a modeling and quantification approach like ATHEANA, it is oftentimes not necessary to build or quantify the PRA model.

Sequence Cut Sets Before Recovery:

TMFW * AFWS-CCF * HPI-CCF
TMFW * AFWS-CCF * SWS-CCF
TMFW * AFWS-HVAC * HPI-CCF

Sequence Cut Sets after Recovery:

TMFW * AFWS-CCF * HPI-CCF * OPER-DEP-COND
TMFW * AFWS-CCF * SWS-CCF (no recovery action)
TMFW * AFWS-HVAC * HPI-CCF * OPER-DOOR

where: TMFW = initiator; loss of main feedwater
AFWS-CCF = common-cause failure of AFWS
HPI-CCF = common-cause failure of HPI for feed and bleed
SWS-CCF = common-cause failure of service water
OPER-DEP-COND = operator failure to depressurize and use condensate for steam generator feed
OPER-DOOR = operator failure to open doors of AFWS rooms for ventilation

Figure 10.6 Illustration of Failure-to-Recover Events in Cut Sets.

However, this applies only when there is little or no dependence between the cause of the initiating event and how the plant staff will respond as the sequence of events unfolds. If there may be a relationship between the initiating event and subsequent staff response, the ATHEANA process will help uncover such relationships through identification and definition of error-forcing contexts. In such cases, it may be desirable to develop or modify existing PRA models to add specific initiator-causing HFEs found to be of potential interest using ATHEANA (i.e., some HFEs may be analyzed as separate initiating events).

10.3.3.2 Human Failure Events in Event Trees

This is the portion of the model where incorporation of the ATHEANA process will often take place. Because the highest priority HFEs defined by ATHEANA tend to lead directly to the undesired outcome (i.e., core damage for nuclear plants), the event tree structure is the ideal portion of the PRA model to incorporate such HFEs. These events should be identified considering the initiating event being addressed, the related successes and failures associated with the undesired sequences containing the HFEs, and the possible error-forcing contexts accounted for using the ATHEANA process. The HFEs should be defined so as to capture errors of commission (of highest priority) and errors of omission that are missing from the present PRA model and that would cause the undesired overall effect. For example, core cooling in the form of feed-and-bleed may not be successful because the operator fails to initiate it (a form of omission that is usually found in current PRAs) or

because the operator prematurely stops feed-and-bleed, thinking that it is no longer required (an error of commission to be added using ATHEANA).

The specific location of the ATHEANA HFEs in the event tree is largely a matter of analyst preference. However, as is done currently in placing events in event trees, the expectation is that the placing of an additional ATHEANA HFE in an event tree will depend on how it relates chronologically to the demand of functions and systems involved in responding to the initiating event, where its inclusion will provide the most efficient analysis of all the possible sequences depicted by the event tree and the logical dependencies of other events to the HFE in the sequence.

In addition, it may be desirable or even required that if subsequent successes or failures in a sequence would significantly alter treatment of the incorporated HFE (e.g., by providing new cues for action), the event tree may need to include multiple HFEs that are similar. However, definition and/or quantification would be different because of possible differences in timing, the plant status, etc.

Figure 10.7 illustrates one possible way to incorporate ATHEANA HFEs into a PRA event tree. In this illustration, the incorporation accounts for human failure to initiate or otherwise maintain the required function (in this case-core cooling) until a successful outcome is achieved. In this case, the HFE is included by adding a separate event tree branch that leads directly to core damage. The HFE must obviously be defined in such a way that the undesired outcome will be a direct result.

10.3.3.3 Human Failure Events in Fault Trees

At least conceptually, incorporation of the ATHEANA method into the event trees may allow elimination of some of the high-level, functional, or system-related HFEs currently modeled in the fault trees as post-initiator errors. This is because the anticipated ATHEANA HFEs will include within their scope and definition those events (typically only errors of omission) currently in the PRA fault trees. For example, "failure to align the enhanced flow mode of control rod drive (CRD) injection" in a BWR PRA may be an existing human failure event in the fault tree for the CRD system. An ATHEANA-defined HFE involving the "failure to ensure adequate injection (regardless of the system)" added to the event tree would eliminate the individual CRD human failure event in the CRD fault tree since such a failure would be encompassed by the broader ATHEANA HFE definition. However, the pre-initiator HFEs and some equipment-specific post-initiator HFEs will remain in the fault trees.

While the ATHEANA development to date has not been aimed at addressing events such as pre-initiator HFEs, the scope, definition, and quantification of these events already in the PRA could be different. Not only would the current errors of omission be considered, but these HFEs could also include errors of commission taking into account error-forcing contexts that may cause the undesired pre-initiator or equipment-specific HFE. Note that the development of ATHEANA has not focused on these types of events, but instead is on the broader events directly leading to core damage, as discussed in the event tree subsection.

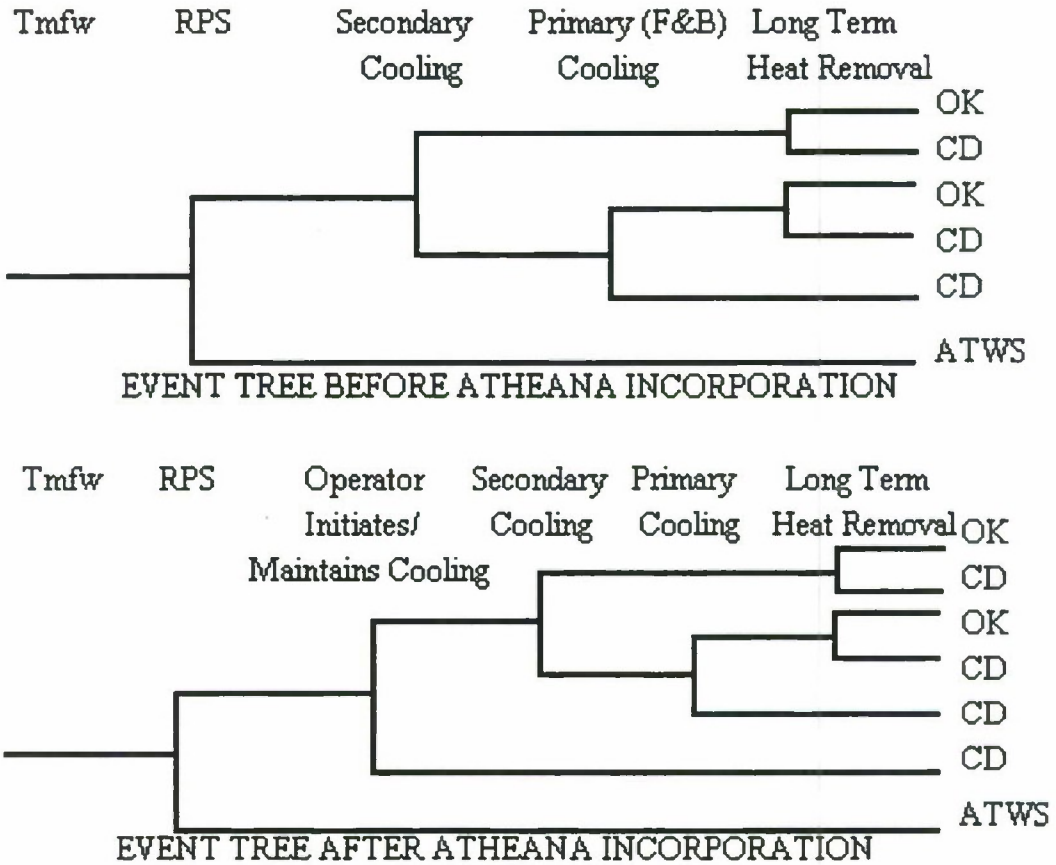


Figure 10.7 Illustration of Incorporating an ATHEANA HFE in an Event Tree.

10.3.3.4 Failures to Perform Specific Recovery Actions

As with the fault trees, some of the recovery events normally added to the cut sets after initial solution and quantification of the PRA model may be eliminated, but only when the ATHEANA HFEs are broadly defined to include failure to recover from the original error, as is intended with the ATHEANA process. For example, "failure to switch over to an alternative water source" could be an existing recovery event added to cut sets involving loss of a primary water source. However, if an ATHEANA-defined HFE has been added to the model which involves the "failure of ensuring an adequate water supply (including consideration of switching to an alternative source when necessary)", then the existing recovery event is no longer needed, since the broader-defined ATHEANA event already encompasses the recovery failure.

Until the initial solution of the PRA model is obtained, all possible recovery considerations may not become evident. Some recovery events may therefore still need to be applied as is currently done.

10.3.3.5 Overall Sequence Quantification Considerations

As with the current PRA practices, the analyst should exercise care in the final quantification of the accident sequences. The ATHEANA incorporation process may reduce the overall number of different HFEs in the model and the number of times multiple HFEs appear in the same cut set (because of the broadly defined HFEs often identified using ATHEANA). However, entire elimination of multiple HFEs in the same cut set may not be possible. When this condition does occur, the analyst must still address the same issues of dependencies among the HFEs in a cut set during final sequence quantification using existing HRA/PRA technology.

10. 4 References

10.1 ASME, A Proposed National Standard: Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, Draft Released for public review and comment, ASME RA-S-1999, draft edition #10, February 1, 1999.

10.2 U.S. Nuclear Regulatory Commission, Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), Draft report for comment, NUREG-1624, U.S. Nuclear Regulatory Commission, May 1998.

10.3 D. Seaver and W.G. Stillwell, *Procedures for Using Expert Judgment to Estimate HEPs in Nuclear Power Plant Operations,* NUREG/CR-2743, Idaho National Engineering Laboratory, Idaho Falls, ID 1983.

10.4 R.J. Budnitz, G. Apostolakis, D.M. Boore, K.J. Coppersmith, C.A. Cornell, and P.A. Morris,, *Recommendation for Probabilistic Seismic Hazard Analysis Guidance on Uncertainty and Use of Experts*, NUREG/CR-6372, Lawrence Livermore National Laboratory, Livermore, CA, April 1997.

10.5 H. Otway, and O. von Winterfeldt, "Expert judgement in risk analysis and management: Process, context and pitfalls." *Risk Analysis* pp. 12(1): 1992.

10.6 J. C. Williams, A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance, Paper presented at 1988 IEEE Fourth Conference on Human Factors and Power Plants, IEEE, 1988.

10.7 U. S. Nuclear Regulatory Commission, *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance,* NUREG-1560, U.S. Nuclear Regulatory Commission, Washington, DC, December 1997.

10.8 D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea, SLIM-MAUD: *An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment,* Brookhaven National Laboratory: NUREG/CR-3518, Upton, NY, 1984.

10.9 D.D. Woods, L.J. Johannesen, R.I. Cook, and N.B. Sarter, *Behind Human Error: Cognitive Systems, Computers, and Hindsight*, Crew System Ergonomics Information Analysis Center (CSERIAC), Ohio State University, Wright-Patterson Air Force Base, Columbus, OH, December 1994.

10.10 E.M. Roth, R.J. Mumaw, and P.M. Lewis, *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, NUREG/CR-6208, Westinghouse Science and Technology Center, Pittsburgh, PA, July 1994.

10.11 R. J. Mumaw and E. M. Roth, How to be more devious with a training simulator: Redefining scenarios to emphasize cognitively difficult situations. *In 1992 Simulation MultiConference: Nuclear Power Plant Simulation and Simulators*, 1992.

10.12 J. W. Perotti and D.D. Woods, *A Cognitive Analysis of Anomaly Response in Space Shuttle Mission Control,* Cognitive Systems Engineering Laboratory (CSEL), CSEL 97-TR-02, Ohio State University, Columbus OH, March1997. Prepared for NASA Johnson Space Center.

10.13 M. T. Barriere, W. J. Luckas, J. Wreathall, S. E. Cooper, D. C. Bley, and A. M. Ramey-Smith, *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis*, NUREG/CR-6265, Brookhaven National Laboratory, Upton, NY, August 1995.

10.14 U.S. Nuclear Regulatory Commission, *Oconee Unit 3, March 8, 1991, Loss of Residual Heat Removal*, Regional Augmented Inspection Team Report No. 50-287/91-008, U.S. Nuclear Regulatory Commission, Washington, DC, April 10, 1991.

10.15 A.D. Swain and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque, NM, August 1983.

11 PERSPECTIVE ON ATHEANA

The techniques for performing risk and reliability assessments have significantly improved over the past few decades. These assessments have become effective tools for identifying and understanding the nature of risks associated with modern technologies such as nuclear, chemical, air and surface transportation. However, in spite of the valuable information gained from such analyses and the improvements made to these modern technologies, few people, including most analysts, genuinely believe that these analyses provide a comprehensive understanding of the related risks and serve as accurate indicators of future accidents.

The reason for this criticism is in part due to the general belief that human reliability analysis techniques are still relatively immature, and our experiences demonstrate that the risks of severe accidents in these technologies are likely to involve a key human contribution as evidenced by Three Mile Island, Chernobyl, the Air Florida crash, etc. Hence, if the risks of severe accidents are going to be successfully managed or reduced, the human element of the risk must be better understood and estimated, and ways must be found to (a) maintain or improve the chances for correct operator intervention and (b) avoid introducing conditions that will enhance the chances of operator error.

This report has described a human reliability analysis method called "a technique for human event analysis" (ATHEANA). ATHEANA is the result of efforts sponsored by the Probabilistic Risk Analysis (PRA) Branch in the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research (RES). ATHEANA was developed to increase the degree to which HRA studies can represent the kinds of human behaviors seen in accidents and near-miss events at nuclear power plants and in other technologies that involve broadly similar kinds of human–system interactions. In particular, ATHEANA provides this improved capability by:

- more realistically searching for the kinds of human–system interactions that have played important roles in accident responses, including the identification and modeling of errors of commission and dependencies

- taking advantage of, and integrating, advances in psychology, engineering, human factors, and PRA disciplines in its approach

ATHEANA provides a structured way to investigate how conditions of the technology and influences on operator performance may coexist in ways that could set up operators to carry out critical unsafe acts that may lead to undesired consequences. Methods have been developed for performing both retrospective analyses of past events and prospective analyses of potential future events. While structured, these methods allow for flexibility in their implementation and take advantage of the knowledgeable brainstorming creativity of the analysts.

ATHEANA provides an approach for more effectively combining the possible conditions of the technology with considerations that govern human performance so as to identify circumstances that could be more error forcing (i.e., make operators more likely to fail). It does this by building on the

principles and techniques of human behavioral science and HRA methods that have come before it. It has also benefitted from a prior peer review which is summarized in Appendix F.

The examples of prospective analyses and retrospective analyses provided here demonstrate the use of ATHEANA and illustrate the kinds of observations and findings that are possible when this approach is used. These types of results can provide users of ATHEANA with a better understanding of why humans may perform unsafe acts in certain situations.

It is the authors' hope that application of ATHEANA will provide users with new insights into the human contribution to risk, and therefore be useful in identifying ways to lessen the chances or consequences of severe accidents in the future.

APPENDIX A
REPRESENTATIONS OF SELECTED OPERATIONAL EVENTS FROM AN ATHEANA PERSPECTIVE

A.1.1 EVENT IDENTIFIER - Three Mile Island 2

Plant Name:	Three Mile Island 2
Plant Type/Vendor:	PWR/B&W
Event Date/Time:	03/28/79, 04:00
Event Type:	Small-break LOCA with loss of primary cooling
Secondary Event:	Reactor trip with failure of all EFWS
Unit Status:	Full-power
Data Sources:	Three Mile Island Report of NRC's Special Inquiry Group (Rogovin, et al.), January 1980; Analysis of Three Mile Island - Unit 2 Accident, NSAC-1, Nuclear Safety Analysis Center, July 1979 and Supplement 1, October 1979.
Data Input By:	John Wreathall, Contractor (TWWG), 614-791 9264

A.1.2 EVENT SUMMARY

Event Description: Three Mile Island, Unit 2 (TMI-2) experienced a turbine trip and consequential reactor trip because of loss of feedwater. Loss of feedwater occurred because of ingress of moisture to the instrument air system used to control the condensate polishing valves. The moisture ingress came from use of an air lance by plant operators to try to unblock a blocked resin bed transfer line; the air lance was inappropriately connected to the instrument air supply because of its proximity to the resin bed. Following the reactor trip, the emergency feedwater (EFW) system failed to provide cooling to the once-through steam generators because the EFW inlet block valves were closed (probably as a result of a failure in earlier maintenance). The operators were unaware initially that the EFW valves were closed because tags on the control room panel hid the indicators. The primary system pressure rose and caused the pressurizer relief valves to cycle to relieve the high pressure. Shortly thereafter, the pressurizer emergency relief valve (ERV) stuck open. However, the operators were unaware of the valve being stuck open because the position indicator showed the "demanded" position of the valve (whether the control solenoid was energized or not), not its actual position. A second indication of the valve being open (high line temperature) was discounted by the operators since the valve was known to leak.

Because of concerns that the indicated pressurizer water level was indicating high and increasing, the operators became convinced that the reactor primary system was "going solid." That is, the steam bubble in the pressurizer was shrinking to zero, which potentially would mean loss of pressure control of the primary system and the possibility of a loss-of-coolant accident (LOCA) being caused. The operators were from the Navy nuclear program, in which "going solid" is a major area of concern. Because of this concern, the operators throttled high-pressure injection (HPI) virtually to zero injection within 5 minutes of the initiating event. HPI flow was effectively zero for the next 4 hours. Three minutes later, at 04:08, the operators discover the EFW valves closed and opened them, restoring flow to the steam generators. At 04:20 and 04:38, the operators do not recognize the existence of the LOCA when the rupture disk on the reactor coolant drain tank (RCDT) fails and when the containment sump alarms indicate high. At 06:18, the operators close the block valve for the ERV but make no attempt to restore HPI until 08:17. Because of the lack of HPI flow, two-phase flow in the primary system was taking place. By 05:14, the two-phase flow led to serious vibrations in the "B" reactor coolant pumps so the operators stopped the pumps. About 30 minutes later, at 05:41, the operators stopped the "A" reactor coolant pumps because of significant vibration. These pumps remained off until 19:50, when the operators restarted them; thereby, restoring forced cooling within the primary system.

Over the next days, operators and NRC analyzed and responded to concerns of hydrogen build-up in the primary system.

Three Mile Island 2
Small-break LOCA with loss of primary cooling
March 28, 1979

Event Surprises: The operators overlooked the possibility of a two-phase coolant in the reactor coolant system (RCS) for a prolonged period of time despite numerous symptoms of the LOCA, its consequences to the reactor coolant pumps, and core damage shown by the indications of the in-core thermocouples.

Licensee Corrective Actions: The industry and NRC implemented significant changes in the practices associated with the human-factors design of control rooms, the basis for and design of emergency operating procedures, and the industry approach to training.

ATHEANA Summary:

Deviation From the "Expected" Scenario:

- The discharge path via the pressurizer power-operated relief valve (PORV) for the LOCA was unexpected. The consequence of this deviation was that the operators were misled by the indicated increasing pressurizer level to believe that the RCS was going solid.
- In relation to the discharge path, the fact that the indications associated with the PORV were not directly measuring its position, but rather its demanded position, misled the operators into not realizing the valve was open. This discrepancy in information was a significant deviation from expected.
- Complete failure of the emergency feedwater system to start (due to its non-restoration after previous maintenance) on loss of main feed was a deviation from the expected scenario for loss of all feedwater.
- Behavior of the RCS after the saturation point had been reached was a significant deviation from the expected for the operators and the NRC.

Key Mismatch(es):

- The behavior of the RCS indications (particularly of the pressurizer level) compared with the operators' training and procedural guidance for small LOCAs was a mismatch.
- The indicated position of the pressurizer PORV compared with its actual position (both the valve position indicator and the downstream line temperature indications) created a mismatch.
- The relative importance of the risks of the RCS going solid versus the risks from two-phase conditions.
- The belief that the core exit thermocouples were faulty based on the very high readings.

Most Negative Influences

- The operators' **prior experience (PSF)**, particularly their navy training, had created a belief that "going solid" was just about the worst condition that the plant could be in. The TMI **training (PSF)** had not overcome that experience, and the **procedures (PSF)** were not particularly helpful for the situation.
- Many of the indications that might have helped the operators recognize the plant conditions were located such that they were not visible in the normal working areas of the control room (**man-machine interface - PSF**).
- The operators were not trained to recognize the potential for a LOCA via the steam-generator relief valves where the normal symptom of a small LOCA (falling pressurizer level) are reversed (**training - PSF**).
- The problem underlying many of these deficiencies was the failure within the industry to recognize the significance of small-break LOCAs, both in terms of their significance to risk and their differences from design-basis (large) LOCAs in terms of what symptoms might exist and the responses required of the operator (**unexpected plant dynamics - plant condition**).

Most Positive Influences (that could have prevented or otherwise mitigated the event)

- The most positive influence was the involvement of outsiders who eventually identified the appropriate response to the event (**plant condition**).
- In many (though not all) cases, instrumentation existed that could, if seen, have revealed the existence of the LOCA such as the containment sump drains and the pressure in the RCDT. Even the reactor system pressure, if attended to, would have revealed that the reactor coolant was in a two-phase state (**instrumentation - PSF**).

Significance of Event:
This event represents the only accident involving substantial core damage at a U. S. commercial power plant.

Extreme or unusual conditions: None initially. Subsequently, RCS level fell to the point of uncovering the core with resultant fuel damage.
Contributing pre-existing conditions: EFW system isolated probably exacerbated the RCS pressure transient; leaking PORV masked some of the stuck-open valve symptoms.
Misleading or wrong information: PORV position indicated the valve was shut.
Information rejected or ignored: Core exit thermocouple readings were ignored as being faulty.
Multiple hardware failures: Loss of main feedwater system; EFW system isolated; PORV stuck open.
Transitions in progress: Unblocking the resin beds in the feedwater polishing system.
Similar to other events: Symptoms of pressurizer LOCA resembled the RCS going "solid", an event of great concern to the crew from their Navy nuclear experience.

KEY PARAMETER STATUS	
INITIAL CONDITIONS	**ACCIDENT CONDITIONS**
Power level: 97% **RCS temperature (°F)**: Nominal **RCS pressure**: Nominal (about 2255 psig) **RCS level**: Nominal **Other**: Nominal	**Power level**: Tripped **RCS Temperature (°F)**: 590 - 780 **RCS pressure**: 400 - 2365 psi **RCS level**: Minimum ~3 feet above bottom of active core **Other**: Fuel temperatures in excess of 2500°F

FACILITY/PROCESS STATUS	
Initial Plant Conditions & Configurations	**Accident Conditions & Consequences**
Configuration: (1) Nominal at-power conditions (2) Crew was responding to problems in the condensate polishing plant (3) Unit 1 was in hot shutdown **Noteworthy Pre-existing Conditions:** (1) Emergency feedwater block valves closed (2) Pressurizer ERV had a history of leaking, with high line temperature indicated (3) Pressurizer spray valve and heaters were in manual control **Initiator** (1) Turbine trip on loss of feedwater led to reactor trip on high RCS pressure	**Automatic Responses:** (1) EFW system auto-initiated (2) Pressurizer ERV cycled to relieve high RCS pressure (3) High pressure injection pumps 1A and 1C started on low RCS pressure (ESF actuation signal) **Failures:** (1) EFW block valves were closed (assumed a latent failure following earlier maintenance) thereby preventing secondary cooling for initial 8 minutes (2) ERV stuck open

A.1.3 ACTION SUMMARY

Event Timeline:

Pre-Initiator / Initiator / Post-Accident

(-42hr)	up to 04:00	04:00	04:05	05:14	06:22	07:20	19:33
	^^^	^	^	^	^	^	^
U1	U2	E1	U3	H1	R1	R2	R3

Unsafe Actions and Other Events:
Key: U = unsafe actions
E = equipment failures (significant to the event)
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
U1	EFW block valves left shut (probably from maintenance work 42 hrs before initiating event)
U2	Operators use instrument air to try freeing blocked resin bed transfer line - leads to initiating event
E1	Pressurizer ERV sticks open
U3	Operators throttle HPI "to prevent pressurizer going solid"
H1	Operators shut down RCPs on indication of high vibration
R1	Operators close ERV block valve
R2	Operators manually initiate additional HPI flow
R3	Operators restart RCPs

HUMAN DEPENDENCIES		
ID	**Dependency Mechanism**	**Description**
	None	

Unsafe Actions Analysis		Three Mile Island 2
U1: Unknown, but probably EOO, slip: Valves not restored after maintenance.		
Error Forcing Context		
Plant Conditions	**PSFs**	**Failures in Information Processing**
Evolution and activities: 1) It is assumed that the valves were left closed following earlier maintenance work though the personnel involved in that work reported the valves as repositioned correctly. *Configuration:* 2) Unknown. *Plant Impact*: 1) Prevented initial secondary cooling, which exacerbated pressure transient following loss of feedwater.	Unknown.	Unknown.
U2: EOC: Operators use instrument air (IA) to try to free clogged resin transfer line - moisture entered instrument air supply (could be mistake or circumvention concerning use of IA for non-control purposes but no information provided)		
Error Forcing Context		
Plant Conditions	**PSFs**	**Failures in Information Processing**
Evolution and activities: 1) Operators had been experiencing difficulties in transferring resins from an isolated condensate polisher to a receiving tank. Attempts to free the plugged transfer line had been in progress for about 11 hours.	Unknown.	Unknown.
U3: EOC: Mistake: Operators substantially terminated HPI "to prevent the pressurizer from going solid"		
Error Forcing Context		
Plant Conditions	**PSFs**	**Failures in Information Processing**
Evolution and activities: 1) Operators were responding to the operation of automatic controls in the immediate post-initiator phase. *Configuration:* 1) Plant had tripped on high RCS pressure following loss of feedwater; emergency feedwater injection flow was blocked by the valves left shut (consequence of U1). HPI started injecting automatically. ERV LOCA discharged via pressurizer. *Plant Impact:* 1) Substantially causes core damage.	*Man-machine interface:* 1) ERV position indication was on the basis of "demand" signal, not actual position. Many indications that might have prevented the misunderstanding were located on back panels. *Training:* 1) Operators were untrained in LOCAs via the pressurizer relief lines. 2) Operators persisted in believing that "going solid" was a major hazard at TMI. *Procedures:* 1) LOCA procedures did not provide direct guidance for the ERV LOCA.	*Situation Assessment:* 1) Operators created a mistaken situation model because of the following factors: • pressurizer level indicated high and rising • ERV position indicated the valve was closed when it was open • ERV discharge line had a history of indicating high

A.1.4 ACCIDENT DIAGNOSIS LOG

Time*	Accident Progression & Symptoms †	Response ‡
Just before 04:00	Unit at 97% and nominal conditions. Plant operators were unblocking a condensate polishing bed resin transfer line using instrument air to supply air lance **(U2)**	
04:00:37	Condensate polishing valves closed because of moisture in instrument air supply. Turbine tripped on resulting loss of feed water	
04:00:45	Reactor tripped on high RCS pressure following turbine trip and loss of main feed water	
04:00:49	Pressurizer emergency relief valve (ERV) cycled and then stuck open **(E1)**	None. Control-room indication shows valve shut--signal is "demand" not "actual" position
04:05:15	Pressurizer level was 363" and increasing	Operator throttles HPI flow "to prevent system going solid" - procedures state pressurizer level must not exceed 400" **(U3)**
04:08:55		Operators discover emergency feedwater (EFW) block valves are shut and open them, allowing EFW flow to the steam generators
04:14 - 04:20	Reactor coolant drain tank (RCDT) rupture disk failed	Operators note pressure drop in RCDT but fail to diagnose ERV LOCA
04:25 - 07:??	ERV discharge line temperature high	Operators twice consider this to be the residual heating effect of the initial valve opening
04:38	Containment sump pumps reported running	Operators turn off pumps
04:40+	Low boron measurement plus increasing neutron count in core	Significance not understood (indication of core drying out)
05:00	Containment building temperature is 170°F, pressure is 2.5 psi	Not apparently observed
05:14	Both loop B reactor coolant pumps (RCPs) indicate significant vibration	Operators shut down loop B RCPs (H1)
05:41	Loop A RCPs indicate significant vibration	Operators shut down loop A RCPs **(H1)**

Time*	Accident Progression & Symptoms †	Response ‡
06:18	ERV discharge line temperature high	Operators requested ERV line temperature reading, and closed ERV block valve 4 min later (R1)
06:45 - 06:54		Operators try starting RCPs - pump 2B runs for a few seconds and trips; other pumps do not start
06:55		Site emergency declared
07:13		Operators reopen ERV block valve; ERV line temperature increased
07:17		Operators reclose ERV block valve
07:20		Operators manually initiate safety injection signal, reactor coolant make-up pump 1C starts **(R2)**
07:20	8R/hr radiation reading in reactor building	General emergency declared
08:17 - 08:27	Make-up pumps 1A, 1C tripped	Pump 1B started manually, pump 1C restarted manually
19:33 - 19:50		RCP 1A started manually, stopped, and restarted **(R3)**

* Times are based on NSAC 1 analysis
† A large number of alarms and indications occurred throughout the event, many of which were indicative of the event
‡ Operators performed many actions beyond those listed here which played key roles in the event

A.2.1 EVENT IDENTIFIER - Crystal River Unit 3

Plant Name:	Crystal River Unit 3
Plant Type and Vendor:	PWR/B&W
Event Date, Time:	12/8/91, 2:49 am
Event Type:	Pressurizer spray valve failure
Secondary Initiator:	None
Unit Status:	Start-up
Data Sources:	AEOD/INEL Trip Report, "Onsite Analysis of the Human Factors of an Event at Crystal River Unit 3 December 8, 1991 (Pressurizer Spray Valve Failure)," EGG-HFRU-10085, January 1992
Data Input By:	Leslie Bowen, Contractor, Buttonwood Consulting, Inc., (703) 648-3104

A.2.2 EVENT SUMMARY

Event Description: On December 8, 1991, a reactor coolant system (RCS) pressure transient occurred during startup following a reactor power increase. During a normal power increase the pressurizer spray valve cycled opened to control a slight increase in pressure. The actuator for the spray valve failed which left the valve partly open but position indicating lights showed that the valve was closed. RCS pressure began to decrease and as a result of the erroneous indication, the operators failed to identify the cause. RCS pressure continued to decrease, reaching setpoints for arming the engineered safety features (ES). Circumventing procedural guidance, operators bypassed ESF for 6 minutes, in anticipation of terminating the transient. Control room supervisors directed operators to take ESF out of bypass and the high-pressure injection system automatically started. Injection was secured because of fears of over-filling the pressurizer but eventually the operators reinitiated injection to increase and stabilize RCS pressure. The pressure transient was terminated after the pressurizer spray line isolation valve was closed, on the suggestion from a supervisor that it might be helpful.

Event Surprises: ES Bypass by the operator without understanding the cause of the transient.

Licensee Corrective Actions: At the time of the report, plant management was considering the following types of actions to reduce the reliance on knowledge-based behavior during this type of event:
(1) providing a diagnostic procedure for response to a loss of control of RCS pressure
(2) providing a clearer statement in policies and procedures defining the restrictions on overriding ES actuation or other safety system actuation
(3) reviewing and supplementing existing training fore this type of event.

ATHEANA Summary
Deviation From the "Expected" Scenario:
- Continuing pressure decrease due to stuck open spray valve.
- Instrument failure in an unannounced mode: pressurizer spray valve indicated closed, when it was actually open.

Key Mismatch(es):
- Training (inexperienced crew) not well matched to this unusual plant condition; snap judgment of situation was incorrect, but adopted by entire crew without question. Strong confirmation bias (assumed cooldown confirmed by decreasing pressure, closed indications for PORV and spray valve, and field reports of steam flow to the de-aerators) led to failure to use procedures and failure to notice contradictory evidence.

- Supervision not well matched to the inexperience of crew and the unusual plant conditions, in that supervision did not provide guidance for diagnosis or for which procedures to turn to in the early stages of the event.
- Procedures were a weak match for this particular scenario, in that the scenario was not specifically addressed.

Most Negative Influences:

- Both procedures and training were unclear regarding diagnosis of decreasing system pressure. (PSF)
- There was no indication of spray line flow to use to verify the valve position. (PSF).
- STraining was not sufficient to prevent operators from taking action that was against procedure and policy (bypassing ES). (PSF)

Most Positive Influences:

- That experienced plant management was in the control room to advise in two key instances (1) to unbypass ES and (2) to close the spray isolation valve. (Plant Condition)

Significance of Event:

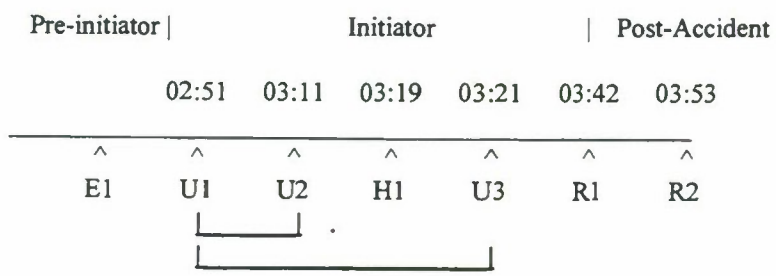
Extreme or unusual conditions: None.
Contributing pre-existing conditions: Shift turnover briefing included mention of spray valve position indicator trouble.
Misleading or wrong information: Pressurizer spray valve indicated closed, when it was really open.
Information rejected or ignored: Briefing on spray valve position indicator trouble.
Multiple hardware failures: None.
Transitions in progress: Power ascension following startup.
Similar to other events: Decreasing pressure believed to be because of pressure outsurge, as a consequence of reactor coolant shrink (as a result of cooldown), despite evidence to the contrary.

KEY PARAMETER STATUS	
Initial Conditions	**Accident Conditions**
Power level: 10% RCS temperature: normal operating temperature RCS pressure: normal operating pressure RCS level: normal level Other:	Power level: 0% RCS temperature: low of 544°F RCS pressure: low of around 1500 psig RCS level: increased to top of scale Other:

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configuration	**Accident Plant Conditions and Consequences**
Configuration: The plant is starting up from a short maintenance outage. The rods are in manual and the operators are preparing to roll the turbine by increasing reactor power to 15%. The plant lineup is normal configuration for start-up. **Preexisting operational problem:** Shift turnover briefing included mention of spray valve position indicator trouble. **Initiator:** Following a normal increase in reactor power, the pressure control system automatically opened the pressurizer spray valve to compensate for a small increase in pressure.	**Automatic Response:** 1) Reactor trip on RCS low pressure (1800 psig) 2) "ES A and B not bypassed" alarms (1640 psig) 3) ES initiation (1553, 1574 psig) **Failures:** Pressurizer spray valve indication is erroneous in that the pressurizer spray line control valve does not reseat because of a failed actuator but the control board indicator shows it as closed.

A.2.3 ACTION SUMMARY

Event Timeline:



Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS ANALYSIS	
ID	**Description**
E1	Spray valve actuator faulty
U1	Operators increase power to increase Tave and RCS pressure.
U2	Operators bypass ES
H1	Operators unbypass ES
U3	Operators secure HPI
R1	Operators take manual control of high-pressure injection to stabilize RCS pressure
R2	Operators close the spray line isolation valve.

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**
U1, U2	Training	Operator did not refer to procedures
U1, U3	Situation Assessment	Incorrect mental model influenced use of available information to reach the correct conclusion

Unsafe Actions Analysis		Crystal River 3
U1 EOC, Mistake Operators increase reactor power (several times) to increase RCS temperature and pressure.		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Evolution and activities: 1) The plant is starting up from short maintenance outages. The rods are in manual and the operators are preparing to roll the turbine by increasing reactor power to 15%. *Configuration:* 1) The plant lineup is normal configuration for start-up. *Preexisting operational problems:* 1) Shift turnover briefing included mention of spray valve position indicator trouble. *Plant Impact:* 1) RCS pressure decrease with resulting reactor trip and high-pressure safety injection	*Procedures:* 2) Procedures were not used. Had they been, they may not have helped the diagnosis. *Training:* 1) Operators relatively inexperienced in responding to unplanned transients. Operators did not turn to procedures. *Supervision:* 1) Supervision did not provide guidance in diagnosis or to turn to the procedures in the early stages of this event. *Stress:* 1) Plant dynamics provided limited time for investigation , analysis, and decision-making. *Environment:* 1) Significant actions during the event took place between 3:00 am and 4:00 am. (Effect of duty rhythm is expected to impact cognitive capabilities more than skill- or rule-based activities.	*Situation Assessment:* 1) Action on the basis of incorrect conjecture that an overcooling event was in progress. This conjecture seemed to be supported by reports from field operators that there was steam flow to the deaerators although securing the flow did not change the plant response. 2) Although operators were monitoring pressurizer parameters, the evidence that level remained fairly stable and T_{ave} was decreasing only slightly did not cause a reanalysis of the situation model the operators were holding. *Response Planning:* 1) Operators did not refer to procedures, in particular not to the annunciator response procedure which would have been appropriate. 2) In actuality, the annunciator response procedure did not provide guidance that would have assisted in stopping the pressure decrease.
U2 EOC, Mistake Operators bypass ES		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Safety equipment actuation: 1) Reactor trip on RCS low pressure (1800 psig) 2) AES A and B not bypassed@ alarms (1640 psig) *Indications:* 1) Pressurizer spray valve indication malfunction *Plant Impact:* 1) Pressure continues to decrease and threatens sub-cooling margin	*Procedures:* 1) Procedures were not used. Had they been, they may not have helped the diagnosis. *Training:* 1) Operators did not use procedures and violate procedures by bypassing ES without an understanding of what was causing the transient. Operators terminate HP flow because of concerns with taking the pressurizer solid without benefit of procedure. 2) Communications: *Supervision:* 1) Supervision did not provide guidance in diagnosis or to turn to the procedures in the early stages of this event. *Stress:* 1) Plant dynamics provided limited time for investigation , analysis, and decision-making. *Environment:* 1) Significant actions during the event took place between 3:00 am and 4:00 am. (Effect of duty rhythm is expected to impact cognitive capabilities more than skill- or rule-based activities.	*Response Planning:* 1) Operator does not refer to procedure when bypassing ES. Bypassing ES is in error. 2) Operator does not seek permission from nor inform supervision of ES bypass.
U3 EOC, Mistake Operators secure HPI		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Safety equipment actuation: 1) Reactor trip on RCS low pressure (1800 psig) 2) AES A and B not bypassed@ alarms (1640 psig) 3) ES initiation (1500 psig) *Indications:* 1) Pressurizer spray valve indication malfunction *Plant Impact:* 1) RCS pressure decreases and threatens sub-cooling margin	*Training:* 1) Procedure for securing ES is followed without understanding nature of the transient. *Supervision:* 1) Supervision did not provide guidance in diagnosis or to turn to the procedures in the early stages of this event. *Stress:* 1) Plant dynamics provided limited time for investigation , analysis, and decision-making. *Environment:* 1) Significant actions during the event took place between 3:00 am and 4:00 am. (Effect of duty rhythm is expected to impact cognitive capabilities more than skill- or rule-based activities.	*Situation Assessment:* 1) Operators shift concern from decreasing pressure to overfilling the pressurizer. *Response Planning:* 1) Operators do not continue with the ES actuation procedure once conditions for securing the HPI are met. Later instructions would have them isolate all sources of low RCS Pressure including closing the spray isolation valve.

A.2.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	Response
24:39	Reactor Startup	
1:03	Reactor Critical	
2:07	Entered Mode 1 operations; power above 1% Warmed steam lines, established main condenser vacuum, and dumping steam to the main condenser via turbine bypass valves (TBVs)	
2:47	Reactor power increased from 1% to 12%	NO2 pulled rods to increase reactor power; NO1 preparing to roll turbine
2:49	Reactor pressure increased slightly in response to small power increase which caused spray valve to actuate, but did not reclose.	NO2 reported that the RCS pressure was decreasing. NO1 suggested that NO2 bump up power to increase reactor temperature.
2:51	Reactor power increased to 14%. RCS pressure increased 2223 psig and then began to decrease. Tave was 567.3°F and pressurizer level was 176 in.	**U1**: Operator pulled rods to increase reactor power by 3%.
2:52	RCS Pressure was 2150 psig and decreasing; Tave was 568.5°F and pressurizer level was 190 in.	NO2 monitoring parameters on the strip chart recorders on the panels. NO1 was monitoring RCS pressure on the digital indication available on the safety parameter display systems (SPDS).
2>53	RCS low pressure alarm annunciated.	Operators began a concerted search for the cause of the decreasing RCS pressure transient. Secured steam flow to deaerating feed tank on the premise that an RCS cooldown was in progress. Checked for indications of LOCA. ANSS suspected (incorrectly) that the insurges to the pressurizer caused by reactor power bumps were cooling the water in the pressurizer and decreasing the pressurizer temperature and pressure. Operators manually closed pressurizer spray control valve to ensure that it was closed even though the indication was that it was already closed.
2:54	RCS pressure was 2050 and decreasing.	**U1**: NO2 bumped reactor power 3% to 15%.
3:00	RCS pressure was 1980 and decreasing.	**U1**: NO2 bumped reactor power from 13.5% to 15%.
3:09	Reactor auto trip on RCS low pressure (1800 psig); Low pressurizer level alarm annunciated.	Operators entered reactor trip procedure AP-850. Immediate actions were being executed.
3:11	ES A and B Not Bypassed alarms at 1640 psig	**U2**: NO1 bypassed both A and B HPIS and alarms cleared.
3:12		NO1 announced that ES A&B were bypassed.
3:09	ES initiation bistables tripped. RCS pressure at 1553 psig on Channel A and 1574 psig on Channel B.	AOS asked ANSS and the SS if they concurred with the ES bypass. ANSS directed that the bypass be lifted.
3:19:04	HPI initiated, EFW initiated. DG started.	**H1**: NO 1 removed the bypass. Operators entered ES actuation procedure AP-380.
3:27		NO1 bypassed ES as per procedure and secured EFW, as normal feed was available.
3:27	RCS pressure increased to 1600 psig.	**U3**: NO1 secured flow from the HPIS into the RCS and stopped pumps 3A and 3C leaving 3B running.
3:27	RCS pressure increase reset the 1500 psig bistables for auto ES initiation.	NO1 reset auto initiation circuit.
3:35	RCS pressure began to decrease again and decreased sufficiently to trip on 1500 psig ES bistable.	NO1 bypassed the automatic ES initiation
3:42	RCS pressure continues to decrease. RCS temperature has decreased to 544°F but has begun to increased once ES was secured.	Operators monitoring the subcooling margin indication. **R1**: ANSS decided to prevent RCS pressure form decreasing below 1500 psig by establishing a controlled HPI flow to the RCS to increase water level and compress the bubble, thereby increasing pressure. ANSS directed NO1 to slowly open makeup valve MUV-24. HPI pump 3B was still operating. NO1 does as directed.

Crystal River 3
Pressurizer Spray Valve Failure
December 8, 1991

Time	Accident Progression and Symptoms	Response
3:42	RCS pressure begins to increase slowly from 1503 psig.	
3:45	Pressurizer high level alarm annunciated. RCS pressure was 1550 psig.	
3:53	RCS pressure at 1675 psig and pressurizer level indication was at the top of the scale.	**R2**: AOS suggested that the pressurizer spray line isolation valve be closed.
3:54	RCS pressure began to increase rapidly.	Operators take manual control of the pressurizer heaters.
4:02	RCS pressure stabilized at approximately 1750 psig.	
4:55		SS made an emergency action level determination of an unusual event.
5:00		State notification
5:06		SS declared that the event had been exited.
5:32		NRC notification.

A.3.1 EVENT IDENTIFIER - North Anna 2

Plant Name:	North Anna 2
Plant Type and Vendor:	PWR/W
Event Date, Time:	4/16/93, 7:16 am
Event Type:	Degradation of heat removal capability by disabling AFWS (i.e., bypass of ESFAS)
Secondary Initiator:	None
Unit Status:	Full power
Data Sources:	LER #93-002-00 dated 5/14/93; Inspection Report 50-339/93-17 conducted 4/16-23/93; AEOD/INEL Trip Report, "Disabling of Auxiliary Feedwater System (AFWS) During Reactor Trip Recovery," 6/93
Data Input By:	Alan Kolaczkowski, Contractor, SAIC, (303) 273-1239

A.3.2 EVENT SUMMARY

Event Description: The unit experienced an automatic generator-turbine-reactor trip because of a failed voltage regulator. Safety systems responded as designed although there were other nuisance failures. Approximately 9 minutes into the event, an operator, without explicit knowledge of shift supervision, disabled the entire AFWS (which was running) and used main feedwater (which was recirculating at the time) as a means to feed the steam generators and control primary plant cooldown (operator was concerned about excessive cooldown with full AFWS flow). A valid AFWS start signal from low-low steam generator levels in all 3 steam generators was still present. This condition was not recognized until about 18 minutes after the AFWS was disabled during a procedural step for recovering all systems back to a "normal" state. The AFWS was then returned to "auto" standby per direction of shift supervision. Main feedwater had already recovered all 3 steam generator levels. Further shutdown of the unit proceeded normally.

Event Surprises: No one noticed the disabling of AFWS in spite of turbine AFWS steam valves closed alarms and other visual indications (motor AFWS pump controls in pull-to-lock, operator using main feedwater).

Licensee Corrective Actions: Subsequent actions included:
(1) Unit 2 Supervisor and Backboard operator relieved of license duties and coached on station's policy for defeating ESFs as well as later received remediation training on control room communication and control room command and control structure.
(2) Requirements put in place to discuss event in Licensed Operator Requalification program.
(3) "Nuisance" hardware problems repaired.
(4) Root cause and other actions - pending management review. (Do not know what else was done)

ATHEANA Summary
Deviation From the "Expected" Scenario:
- The fact that both AFWS and main feedwater were apparently available instead of the "expected" total loss of main feedwater, was a deviation in the scenario that contributed to the unsafe act of most concern.

Key Mismatch(es):
- How to handle the situation when both AFWS and main feedwater were apparently available, represents the most significant *mismatch* between the actual event and the procedural and training guidance for the operators, (i.e., the

guidance was not clear on how to respond to a rapid cooldown event with both AFWS and main feedwater available).

Most Negative Influences:

- Both procedures and training were unclear (PSFs) as to how to mitigate a rapid cooldown (Plant Condition), particularly when both AFWS and main feedwater are apparently available (Plant Condition).
- Inadequate command and control during the event including directions by multiple persons, closed-loop communications not used, and terminology misunderstanding ("secure" AFWS) (PSFs).
- Operator's pre-conceptions about (a) possible degradation of AFWS pumps when in recirculation, and (b) the best standby status for AFWS (thought it best to have pumps shutdown than valves throttled way down) (PSF).

Most Positive Influences:

- Station policy and licensed operator training address disabling ESFs (PSFs).
- Procedure for returning systems to "normal" caught the fact that AFWS had been inappropriately disabled (PSF).

Significance of Event:

Extreme or unusual conditions:

- Plant configuration ended up such that backup heat removal (AFWS) could not have automatically responded if main feedwater had not restored SG levels or if main feedwater had failed later (i.e., all secondary heat removal would have been lost without manual intervention to "re-enable" AFWS which may or may not have restarted).
- Main feedwater status and operability was not "completely clear" following the initial transient:
  (a) there was a feedwater heater relief valve stuck-open and so the feedwater heater was being isolated (could have disrupted main feedwater flow if subsequent problems occurred),
  (b) "B" main feedwater pump breaker was inoperable in the control room,
  (c) a condensate recirculation valve had failed, and
  (d) a severe weather alert had just been issued (possible jeopardy to offsite power and hence main feedwater operation).

Contributing pre-existing conditions: None

Misleading or wrong information: Control room command and control problems, particularly those related to misunderstanding about the actual status of the AFWS, could have been a more significant factor in more complex or challenging events.

Information rejected or ignored: None

Multiple hardware failures: None

Plant transition in progress: None.

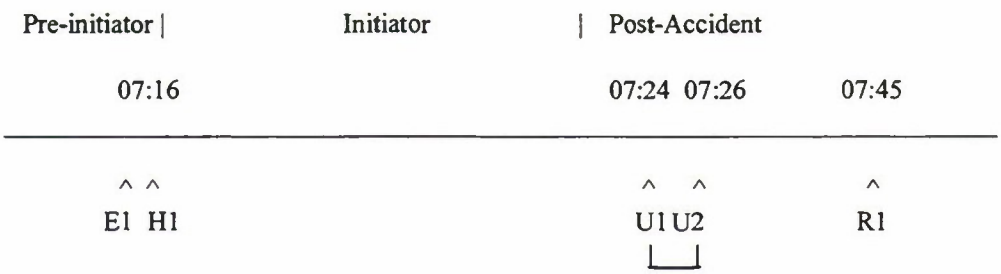
Similar to other events: None.

KEY PARAMETER STATUS	
INITIAL CONDITIONS	**ACCIDENT CONDITIONS**
Power level: 100%	Power level: tripped, headed toward shutdown
RCS temperature: normal operating temperature	RCS temperature: reached min Tavg = 540°F (below no-load control setpoint of 547 ° F)
RCS pressure: normal operating pressure (about 2235 psig)	RCS pressure: minimum reached was 1925 psig
RCS level: normal level	RCS level: minimum reached was 23%
Other: nominal	Other: cooldown rate was about 2F/5 minutes; at time of AFWS disabled, steam generator levels at 5%, 12%, and off-scale low - all below 18% setpoint for auto AFWS start - operator had opened 2 main feedwater bypass valves to supply flow.

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configuration	**Accident Plant Conditions and Consequences**
Configuration: (1) Nominal at-power conditions. (2) Crew consisted of 3 senior licensed operators and 3 operators; on day 2 (07:00-19:00 shift) following 6 days off; STA also on shift. Crew consisted of Shift Supervisor, Unit 1 Supervisor, Unit 2 Supervisor, Unit 1 reactor operator, Unit 2 reactor operator, and backboard operator. Unit 1 Supervisor came over to Unit 2 side of control room following Unit 2 trip, to assist. **Preexisting operational problem:** No specific equipment or indications noted as being out-of-service or problematic; nor mention of specific administrative controls or temporary equipment in use. **Initiator:** Following a VARS alarm because of a voltage regulator failure, in response to which the Unit 2 reactor operator attempted to take manual control and lower excitation, a differential lockout was received causing a generator-turbine-reactor trip; thereby, starting the event.	**Automatic Response:** (1) 2 condensate and 2 main feedwater pumps remained on-line, recirculating thru 1" line back to condenser (2) All 3 AFWS pumps (2 motor, 1 turbine) auto started with discharge valves full-open on steam generator levels reaching lo-lo setpoint of 18%; flow reached >1400 gpm (3) AMSAC initiated (SG levels <13% in 2/3 SGs); all SG levels continued to shrink (not unexpected) No safety injection ever occurred **Failures:** (1) Abnormal amount of steam in turbine building because of feedwater heat exchanger relief valves lifting and one would not reset - involved Shift Supervisor attention a few times while in the control room to dispatch others and communicate with other operators (2) One control rod bottom indication not reached - Unit 2 reactor operator agitated indicator which broke the cover but caused bottom indication to indicate on the panel. (3) Reactor coolant pump vibration alarm received - responded to by Shift Supervisor who reset alarm and alarm cleared (4) Others: air ejector hi rad spike alarm, "B" MFW breaker light out in control room, condensate recirc. valve failure, source range indication failure. **Consequences:** (1) No plant or offsite damage, or personnel injury occurred; nor was radiation released.

A.3.3 ACTION SUMMARY

Event Timeline:



Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
E1	Exciter field voltage regulator failure cause overexcitation
H1	Operator attempts to manually lower excitation; but plant trips
U1	Operator resets AMSAC although this was not yet directed by procedure (action allows U2)
U2	Operator disables AFWS while AFWS start signal still present (switched to main feedwater)
R1	Crew recognizes AFWS is disabled and restore AFWS to auto start configuration

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**
U1, U2	Common PSFs and same overall situation assessment.	Operator recognition that U1 was required to be performed in order for U2 to be performed. Taken together, they resulted in the desired (but unsafe) outcome (i.e., really 2 steps in the same single unsafe act of securing AFWS)

Unsafe Actions Analysis — **North Anna 2**

U1 & U2; EOCs; Mistakes (completely coupled)

Error Forcing Context

Plant Conditions

Evolution and activities:
1) The plant was at 100% power with nominal conditions when overexcitation caused plant trip followed by normal response of isolation of main feedwater on low T_{avg} and auto start of AFWS.
2) AMSAC logic tripped when SG levels dropped below 13% before AFWS could recover SG levels (not unexpected).
3) SG "B" level was at 12% and recovering and so had cleared 11% setpoint to allow AFWS flow to be throttled to 400 gpm.
4) SG "A" level at 5%; SG "C" level narrow range off-scale low
5) All AFWS pumps on with discharge valves full open and system supplying >1400 gpm. AFWS valid signal still present since all SGs still <18%.
6) Main feedwater recirculating.
7) RCS conditions indicative of cooldown concerns; though not an extreme cooldown.
8) Other "nuisance" failures were being dealt with

Configuration:
1) Nominal at 100% power and during initial response to trip.

Preexisting operational problems:
1) None indicated.

Plant Impact:
1) U1 allowed AFWS pumps to be stopped even though AFWS start signal was still present (pumps would not stop if AMSAC had not been reset). U2 action then disabled AFWS such that it could not have auto restarted if main feedwater had subsequently not worked or failed. Because main feedwater did successfully operate and restore SG levels, the heat sink was never actually lost.

Performance Shaping Factors

Procedures:
1) Procedure not clear as to how to mitigate a cooldown beyond step 1, which occurred in this case. No procedural direction on shutting down AFWS and placing main feedwater in service.

Training:
1) Topic of overriding or disabling ESFs is an integral part of licensed operator training.
2) Unclear as to design basis of AFWS with SG levels between 11% and 18%. Previous training had not prevented Backboard operator's rendering AFWS inoperable when permission received to use main feedwater. Previous training for all operators had not established consistent procedure usage for stopping a cooldown event and in fact usually dealt with events where the need to cooldown was req'd.

Communications:
1) "Secure" AFWS thought to mean to close AFWS valves to reduce flow by SS and Unit 2 Supervisor (terminology problem). Procedure reader (Unit 1 Supervisor) not included in command path to ensure procedure properly carried out. Multiple supervisors (SS, 2 Unit Sups) giving commands at various times. Closed-loop communications not used.

Supervision:
1) Station policy exists on bypassing ESFs.

Staffing:
1) Unit 2 reactor operator had been on the shift for only 2 months. Unit 2 Supervisor had just returned from several months on Unit 1 outage.

Human-System Interface:
1) Multiple indications available in CR of AFWS pump and valve status (two red annunciators, pull-to-lock handles, and valve indicators).
2) STA unaware of specific AFWS status since AFWS pump and valve status not on SPDS safety function pages he was monitoring.

Organizational Factors:
1) No apparent corporate factors involved but specific control room command organization broke down when multiple supervisors gave instructions and closed-loop communication not used effectively. See "Communications" above.

Stress:
1) Concern about cooldown, dealing with other nuisances, and an awareness of accumulation of people in back of CR after trip may have contributed to stress.

Environment:
1) (apparently not a factor)

Other:
1) Backboard operator concerned with use of 1" AFWS recirc line and just throttling back the pumps because of previous pump degradation problems in tests (per follow-up interview). Engineering had "okayed" use of 1" line for short emergency operation but apparently this had not been communicated to everyone. Backboard operator (per interview) apparently also thought that restart timing and reliability of AFWS pumps would be better than stroke-time and reliability of AFWS valves should system have to be restarted. Finally, apparently Backboard operator did not know (understand) that lo-lo SG levels are an ESF.

Failures of Information Processing

Situation Assessment:
1) Apparently failed to recognize that cooldown rate, while of concern, was not excessive which may have contributed to some urgency to fully stop AFWS on part of Backboard operator.
2) Backboard operator believed AFWS recirculation on 1" line may be detrimental to pumps despite Engineering "okay".
3) Backboard operator believed better to restart AFWS pumps than to reopen throttle valves, if necessary.
4) Miscommunication about "secure AFWS" left two different situation assessments in minds of crew concerning status of AFWS (pull-to-lock vs. throttled down).
5) Apparent lack of recognition by Backboard operator that lo-lo SG signals is an ESF that should not be bypassed.

Monitoring and Detection:
1) No one noticed alarms or other visible indications that AFWS had been disabled for 18 minutes.
2) Perhaps other nuisance problems contributed to this lack of detection.
3) No indication of AFWS pump and valve status on SPDS functional displays being used by STA.

Response Planning:
1) Lack of a well-trained plan for how to deal with further evidence of cooldown when past step 1 in procedure.
2) Lack of a well-trained plan for when and how to remove control from AFWS and go on main feedwater especially when heat sink had been re-established but AFWS start signals not yet completely cleared.

Response Implementation:
1) Lack of well-structured line of command during event; may have been contributed to by (a) dealing with other nuisances, and (b) some recent changes to crew.
2) Lack of "closed-loop" communication which may have otherwise "caught" error made by Backboard operator.
3) Apparent lack of knowledge by everyone as to correct time to reset AMSAC.

A.3.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	Response
07:16	Unit at 100% and nominal conditions. Crew being briefed in Tech Support Center adjacent to control room (had just come on shift starting at 07:00). Unit 2 Supervisor on phone with dispatcher about a severe weather alert that had just been issued.	
07:16:28	Exciter field forcing annunciator and a Volts/Hertz relay actuation annunciator received indicating a voltage regulator problem and overexcitation.	**H1:** Unit 2 reactor operator responds and attempts to manually lower excitation.
07:16:45	Differential lockout received causing a main generator trip concurrent with a turbine trip, followed immediately by a reactor trip. Main feedwater isolation subsequently occurs because of Tavg < 554 °F with reactor trip.	Unit 2 Supervisor immediately terminates phone call, locates Procedure "Reactor Trip and Safety Injection," and directs operators to perform immediate actions. Unit 1 Supervisor announces trip over page system and proceeds to Unit 2 side of control room to assist as "procedure reader." Backboard operator leaves Unit 1 side of control room and takes over secondary plant responsibilities for Unit 2. Shift Supervisor and rest of crew take positions and perform immediate actions. STA enters about 1 min. later.
07:16:51	All three AFWS pumps auto start on SG lo-lo levels (<18%). AFWS total flow rate reaches 1425 gpm. Two condensate and two main feedwater pumps running with recirculation thru one line back to condenser. Apparently another recirc line path is failed. Tavg is approaching 547°F no-load setpoint.	
07:17:19	AMSAC initiates (SG levels <13% in 2 of 3 SGs). All SG levels continue to shrink below narrow range indication	
07:17 - 07:24	Crew notes no safety injection has occurred nor required. Tavg continues to drop Unidentified person pages control room about abnormal steam in turbine bldg. (relief valves on feedwater heat exchangers were lifting and one had stuck-open). Nuisances: One control rod bottom position not indicating. Air ejector high rad alarm received. Reactor coolant pump vibration alarm received.	Crew exits "Reactor Trip and Safety Injection" procedure at step 4 and enters "Reactor Trip Response" procedure. STA checks SPDS and reports to SS and Unit 2 Supervisor that the only function that is not "green" is heat sink condition (SG levels <11% with feed flow >400 gpm) - a yellow condition. • SS dispatches an auxiliary operator (AO) to check on steam in turbine bldg. A few minutes later, AO returns about relief valve and SS dispatches others to isolate feedwater heaters and locally unisolate another main feedwater recirc path. SS, and Unit 2 reactor operator, deal with nuisances (appear to be momentary distractions) as time permits. Unit 2 reactor operator voices concerns several times about decreasing Tavg but gets little or no verbal feedback. He increases charging flow to maintain pressurizer level and watches pressure.
07:24 - 07:26	RCS parameters approaching min values reached during event. SG levels start to recover.	Backboard operator, hearing Unit 2 reactor operator concerns about Tavg, informs Unit 2 Supervisor that SG "B" narrow range level >11% and per step 6 of procedure, AFWS flow can be decreased below 400 gpm. **U1:** Back board operator requests permission from Unit 2 Supervisor to "secure AFWS" and go on main feedwater and that AMSAC be reset - Unit 2 Supervisor directs Unit 2 reactor operator to reset AMSAC which is done. Procedure reader (Unit 1 Supervisor) tries to go back to step 1 in procedure for instructions to control or throttle AFWS even though step 1 is not a continuous action step. Unit 2 Supervisor halts procedure reader. A conference is held among Unit 2 Supervisor, SS, and another SRO from previous shift noting cooldown not that severe. Unit 2 Supervisor then gives permission directly to Backboard operator to "secure AFWS".

Time	Accident Progression and Symptoms	Response
07:26 - 07:27	AMSAC has been isolated (which allows AFWS pumps to be stopped). SG levels: A: 5%; B: 12%; C: narrow range off-scale low (all less than 18% thereby indicating a sustained AFWS start signal). One source range indication not functioning.	**U2:** Backboard operator, without telling anyone and without interaction from procedure reader, opens 2 main feedwater bypass valves to establish flow to SGs and pulls-to-lock AFWS motor pumps and closes 2 steam supply valves to turbine AFW (system now disabled). [Red alarms are present for 2 steam supply valves but *apparently* no one notices or *perhaps* alarms are cleared too quickly]. At this time, Unit 2 Supervisor checks out problem with source range indication and tells Unit 2 reactor operator to enter "Malfunction of Source Range Instrumentation" procedure.
07: 30:38	SG "B" lo-lo level alarm clears (18%)	
07:40:45	SG "C" lo-lo level alarm clears (18%)	
07:43:55	SG "A" lo-lo level alarm clears (18%)	
07:45	All parameters recovering or stable. All SG levels now >20%. Step 12 of procedure is reached which directs shutdown of AFWS.	**R1:** At procedure step 12 which addresses returning AFWS to normal, procedure reader notes AFWS is already in pull-to-lock and immediately notifies SS who directs Backboard operator to return AFWS to auto. This is done (pumps put in auto and steam valves opened).
08:30	Nominal conditions.	Transition to unit shutdown procedure.
09:30	Shutting down.	Post-trip review initiated.
10:55	Shutting down.	NRC notified of reactor trip and the disabled AFWS during the trip recovery.

A.4.1 EVENT IDENTIFIER - Salem 1

Plant Name:	Salem 1
Plant Type and Vendor:	PWR/W
Event Date, Time:	04/07/94, 10:47 am
Event Type:	Loss of Circulating Water
Secondary Initiator:	Loss of Condenser Vacuum
Unit Status:	Full-power
Data Sources:	AIT. 50-272/94-80 and 50-311/94-80
Data Input By:	Susan Cooper, SAIC and Leslie Bowen, Buttonwood Consulting, Inc.

A.4.2 EVENT SUMMARY

Event Description: The plant was at reduced power because of reductions in condenser cooling efficiency resulting from river grass interference with the condenser's circulating water (CW) intake structure. Shortly after 10 am, a severe grass intrusion occurred and many CW pumps tripped. Operators reduced plant power (1%, 3%, 5%, finally a rapid 8%) through manual rod insertion and boration to take the turbine off line. Because of operator errors and pre-existing hardware problems, a reactor trip and safety injection (SI) occurred. As a result of operator errors, the pressurizer filled to solid or nearly solid conditions and PORVs opened numerous times (and normal pressure control was lost). Because of operator error and pre-existing hardware problems, the secondary pressure increased concurrently with pressurizer level, steam generator code safety valve(s) lifted and caused a rapid depressurization, a second SI, and more PORV openings.

Event Surprises:

(1) Control rods were being controlled manually (automatic control out of service because of corrective maintenance) during a period of at least twice daily demands for power reductions.
(2) Caused RT through series of actions: rapid power reduction (manual rod insertion and boration resulting in power reduction up to 8% per minute), over-cooling, then power increase to "reactor startup" 25% power trip setpoint. 3)
(3) Extensive efforts and plans to avoid plant trip (e.g., special procedures and personnel, atypical power reduction, SNSS leaving CR to attempt CW pump restart) but no parallel efforts or plans to address increased workload in control room and no criteria for when to trip reactor.
(4) Spurious SI because of recognized but uncorrected, pre-existing hardware design problem.
(5) RCS overcooling pre-trip, as a result of human actions.
(6) Solid PRZR conditions caused by human actions. Failed to terminate SI early enough to avoid solid PRZR conditions.
(7) Multiple (>300), successful operations of both PORVs.
(8) Failed to monitor and control secondary pressure, resulting in SG code safety valve(s) lifting, rapid depressurization, and second SI (on low PRZR pressure).
(9) Failure of automatic SG pressure control because of recognized but uncorrected, pre-existing hardware problem.
(10) Rapid depressurization and second SI as a result of human actions.
(11) Yellow path, functional recovery procedures not used to re-establish PRZR bubble; rather, plant cooldown achieved through assistance of Tech Support center and manual control of SG atmospheric RVs and letdown and charging.

Licensee Corrective Actions:
(1) Replaced both PORVs.
(2) Made a number of changes and replacements in the steam flow control systems and other steam flow control changes had been planned for upcoming feedwater system modification
(3) Replace summator module in high steam flow setpoint change circuitry with correct model, though did not solve problem the unneeded setpoint drop after reactor trip.
(4) Rod control system isolators replaced to eliminate noise which caused unexpected rod insertion and operators were trained not to use the Tavg recorder as an indicator of required rod speed during power changes.
(5) Procedure changes are referred to but not listed in the report.

ATHEANA Summary

Deviation From the "Expected" Scenario:
- Continuing grass intrusion event combined with unavailability of automatic rod control. Required manual control of reactor power in response to rising condenser back-pressure.
- Degradation of circulating water required 12 people at the intake structure, reducing manning level in control room. Circulating water pump failures forced rapid power reduction and consequential cooldown, to the point reactor trip setpoints dropped to startup settings.
- Spurious and partial safety injection (SI) caused unfamiliar plant response.

Key Mismatch(es):
- Mismatch between operator expectations of unfolding sequence of events and actual plant conditions. Anticipating circulating water recovery, operators focused there and lost control of overall event.
- Mismatch between workload, especially communications flow, and the ability of operators to track changing plant conditions and develop response plans.
- Mismatch between communications goals and practice. With some operators acting independently, there was a consequent loss of supervisory control.
- Complexity and speed of event evolution went beyond training and procedural support.
- Mismatch between operator mental model and the partial SI.

Most Negative Influences:
The operators inability to diagnose the condition of the plant at several junctures, because of training (PSF) in combination with the unavailability of systems and components to operate automatically as designed (Plant Condition).

Most Positive Influences:
In large measure, the plant responded to operator actions as designed, with the exception of the unavailable automatic functions of some systems and components (Plant Conditions). In addition, the operators used EOPs well (Procedures).

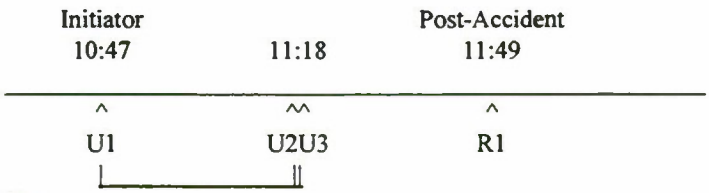
Significance of Event:
Extreme or unusual conditions: Severe grass intrusion.
Contributing pre-existing conditions: Operating at reduced power because of marsh grass accumulation on traveling screens. Automatic control rod system out-of-service.
Misleading or wrong information: None.
Information rejected or ignored: Unable to keep up with the flow of information on changing plant.
Multiple hardware failures: Failure of all CW pumps because of grass intrusion , SG atmospheric relief valve (RV) failure as a result of pre-existing problems, spurious SI because of pre-existing design problems, and failure of 12A DW pump to start (circuit breaker not fully racked in).
Transitions in progress: Power reduction in response to decreased circulating water flow.
Similar to other events: History of annual grass problems.

KEY PARAMETER STATUS	
INITIAL CONDITIONS	**ACCIDENT CONDITIONS**
Power level: 73% RCS temperature: Nominal 547°F RCS pressure: Nominal 2235 psig RCS level: Nominal Other:	Power level: 0% RCS temperature: 552°F (high), 531°F (low) RCS pressure: approximately 2300 psig, low of 1755 psig RCS level: Other: Pressurizer solid. The PRT rupture disk relieved to containment as designed during the event.

FACILITY/PROCESS STATUS	
Plant Conditions and Configurations	**Plant Conditions and Configurations**
Configuration: (1) Continuous monitoring of condenser back pressure (and corresponding decrease in power) because of river grass interference w/ circulating water (CW) traveling screens. (2) Rods in manual control (3) Special work control procedures to facilitate quick restoration of failed CW screen shear pins. **Preexisting operational problem:** (1) Operating at reduced power because of reductions of condenser cooling efficiency (result of river grass intrusions at the condenser's CW intake structure). (2) Grass intrusions @ CW intake structure, at least 2 per day (seasonal occurrence, severe attacks in spring and autumn - vulnerability documented for a number of years). (3) Spurious high steam flow signals because of a design which cause spurious SI (first identified in 1989). (4) Problems w/ SG atmospheric RV controllers (since controllers were modified in the late 1970's). (5) The SS and two off-duty SS, the maintenance supervisor, and ~12 people stationed at the CW intake structure w/ fire hoses and shovels during grass intrusions and to assist in pump priming operations. (6) Local SS provided direct continuous communications with both Salem control rooms. (7) Automatic control rod control system (because of CM - out of service for ~1 month before event, final surveillance test needed to return to service scheduled for the day of the event). (8) 12A CW pump out of service for water box cleaning. **Initiator:** (1) Unit 1 operating crew initiated a plant power reduction, at a rate up to 8% per minute, to respond to circulating water system failures.	**Automatic Response:** (1) PRZR heaters cutout on low PRZR level (level contracted to 17% because of overcooling pre-trip). (2) RT on low power high flux at 25% power ("startup"). (3) SI (twice) - "A" only 1st SI, spurious high steam flow + low T_{ave}; "B" only 2nd SI, low PRZR pressure; injection equipment starts in both cases. (4) PRZR level control system tries (but fails) to maintain level by limiting letdown and increasing charging. (5) 2 PORVs together actuated over 300 times. (6) SG atmospheric RVs (not successfully). (7) SG code safety valves. **Failures:** (1) Spurious SI (1st) as a result of pre-existing design problem. (2) Not all safety equipment actuates (e.g., 2/4 MS isolation valves) on 1st SI because of short duration of signal. Manual positioning of 10 valves required. (3) SG atmospheric RVs did not operate as designed to control SG pressure. (4) Controls for 1/4 SG atmospheric RVs did not operate as designed (pre-existing problem). (5) No "first out" light for 1st SI. (6) Degradation of condenser vacuum. (7) Loss of PRZR steam bubble (and normal pressure control). (8) 4/5 operating CW pumps (initiator). (9) 4/5 operating CW pumps (initiator) because of severe grass intrusion at CW intake structure. (10) SG atmospheric RV failures because of pre-existing problems. (11) Spurious SI because of pre-existing design problem. (12) Failure of 12A CW pump to start as a result of circuit breakers not being fully racked in.

A.4.3 ACTION SUMMARY

Event Timeline:



Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	Description
U1	Operators fail to control RX power (balance power and turbine) load and temperature, resulting in over-cooling then trip when power is increased to "reactor startup" trip setpoint (25%).
U2	Operators fail to terminate HPI soon enough, resulting in solid PRZR.
U3	Operators fail to control secondary pressure, resulting in SG safety valve opening, rapid cooldown, and 2nd SI.
R1	Operators manually open and close SG atmospheric dump valves to control RCS temperature and control RCS pressure through charging and letdown.

HUMAN DEPENDENCIES		
Actions	Dependence Mechanism	Description
U1, U2, U3	Training	Operators consistently fail to monitor plant condition
U1, U2, U3	Stress	Workload is very high in the control room, which leads to distraction from monitoring plant condition.

Unsafe Actions Analysis — **Salem Unit 1**

U1 EOC, Mistake Operators fail to control reactor power (balance power and turbine) load and temperature, resulting in over-cooling then trip when power is increased to reactor startup trip setpoint (25%).

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Evolution/activities: 1) Continuous monitoring of condenser back pressure (and corresponding decrease in power) because of river grass interference w/circulating water (CW) traveling screens. *Operational problems:* 1) Operating at reduced power because of reductions of condenser cooling efficiency (result of river grass intrusions at the condenser's CW intake structure). 2) Grass intrusions @ CW intake structure, at least 2 per day (seasonal occurrence, severe attacks in spring and autumn - vulnerability documented for a number of years). *Unavailable: system/component:* 1) Automatic control rod control system (because of CM). *Plant functions lost:* 1) Degradation of condenser vacuum (result of CW pump loss). 2) System/components lost: operating CW pumps (initiator).	*Procedures:* 1) Guidance for rapid down power maneuvers and loss of CW pumps was weak or did not exist. As a result, atypical rate of reduction (i.e., 8% per minute) and boration was used in attempt to maintain main condenser and turbine operation despite the fact that the number of operating CW screens and pumps was below the minimum for turbine operations. 2) Insufficient guidance regarding actions required for operation with the reactor temperature below the minimum temperature for critical operations (just required recovery within 15 minutes). 3) Alarm response procedures for low vacuum conditions did not provide specific turbine trip criteria. Abnormal procedure for low vacuum did not state turbine trip setpoint. *Training:* 1) Operators failed to recognize decreasing T_{ave} immediately. 2) Operators failed to identify that a RX trip on low power-high flux condition would occur as a result of 7%-25% power increase. 3) RO responsible for rod control relatively inexperienced. *Communications:* 1) NSS does not tell rod operator that NSS withdrew rods. 2) NSS does not provide clear direction to rod operator regarding size and speed of power increase. *Supervision:* 1) SNSS left control room during down power operations to attempt to restore circulators (not procedurally directed) when his duties were to provide direction to NSS on when a reactor or turbine trip should be initiated. 2) NSS directs rod operator to leave his station to shift electrical loads when reactivity is not stable. 3) NSS does not provide rod operator with sufficient direction regarding size and speed of power increase to restore T_{ave} above minimum for criticality. *Organizational Factors:* 1) Operators not provided with adequate guidance regarding management expectations for control room activities during grass intrusions. 2) No guidance as to when operators should cease the effort to maintain plant operations and, instead, stabilize plant conditions by either turbine or reactor trip. 3) Perceived management expectations that extraordinary effort would be used to overcome grass intrusions; attention inappropriately diverted from primary systems to balance of plant (i.e., inappropriate priorities). *Stress: workload:* 1) Numerous distractions in control room during load reduction - continuing communications with CW operators and numerous assessments of plant conditions and restarts or trips of circulators (i.e., 7 trips and 3 restarts in 10 minutes before to trip) plus Unit 2 activities. Also during this period, one boron addition and 150 steps into core with CRs. 2) Rod control operator directed to leave rod control panel to shift electrical loads while reactivity not stable. 3) No additional operators obtained in anticipation of transient to compensate for rod control in manual (only 3 staff in CR at time of event - SS and 2 ROs.). 4) SNSS outside control room during power reduction attempting to start 12A CW pump.	*Situation Assessment:* 1) Expected that CW could be returned to service, focused on keeping plant at power. 2) Failed to recognize that power was still decreasing because of delayed effects of boration, unstable reactivity. 3) Failed to recognize that reactor trip would occur when power was increased to 25% ("reactor startup" setpoint). *Response Planning:* 1) Lacked plan for when to stop trying to maintain operations versus turbine or reactor trip. 2) Lacked plan for reducing power in response to condenser back pressure increases because of the severe grass intrusion. *Response Implementation:* 1) Used an atypical rate of power reduction (8% per minute). 2) Did not control power increase in response to pre-trip overcooling (NSS pulled rods then did not tell RO; because of a lack of NSS direction, RO pulled rods too many and too fast).

Notes: Grass intrusions at the CW intake structure at Salem are a seasonal phenomenon, with more severe attacks in spring and autumn which occur following diurnal tide changes. During heavy grass intrusions, high differential pressure across the CW travelling screens rapidly develops and disables the traveling screens by sacrificial failure of the shear pins that connect the screen motor to the screen gear. Once a CW traveling screen fails because of a grass intrusion, the corresponding CW pump trips off line. Losses of CW pumps or screens affect condenser vacuum. Degradation of condenser vacuum can necessitate reducing reactor power or removing the turbine from service. Operator actions to cope with a grass intrusion are governed by procedures. However, in general, the actions taken by operators are a function of the extent and rapidity of the grass intrusion (and resultant loss of circulators and condenser vacuum) and the prospects for recovery of any lost circulators. No event before to 4/7/94 required as high a rate of power reduction to compensate for the loss of CW (and minimize the increasing back pressure in the condenser).

U2 EOO, Mistake Operators fail to terminate HPI soon enough, resulting in solid PRZR — **Salem Unit 1**

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Operational problems: 1) Spurious high steam flow signals because of the design which cause spurious SI. 2) Only "A" SI actuates, not "B." 3) Indications: No "first out" light for 1st SI. *Hardware failures:* 1) Not all safety equipment actuates (e.g., 2/4 MS isolation valves) on 1st SI because of a short duration of signal. Manual positioning of 10 valves required. 2) SG atmospheric RVs did not operate as designed.	*Procedures:* 1) RX trip or SI EOP used and useful in manually aligning components. 2) Correct transfer and use of SI Termination EOP. *Procedures: incomplete:* 1) No actions specified when SI train disagreement occurs. *Training:* 1) Operators did not properly monitor RCS heatup (as well as corresponding S/G pressure increase) because of decay heat and running RCPs. 2) Operators had not anticipated that the pre-trip overcooling and the post-trip heatup would fill the PRZR. No diagnosis that the post-SI sequence would result in solid PRZR. *Stress: workload:* 1) Manual alignments of components which did not automatically actuate w/ SI and concerns re: the operability of SI "B."	*Situation Assessment:* 1) Failed to monitor and recognize RCS heatup and increasing PRZR level after RT and SI. 2) Failed to understand and recognize the effect of the pre-trip cooldown, followed by heatup on the PRZR. *Response Planning:* 1) Procedures did not specify actions to be taken in response to an SI train disagreement. *Response Implementation:* 1) Took too long to terminate SI (i.e., 17 minutes to reset SI from RX trip, PRZR filled to solid or nearly solid conditions).

Notes:

1) Before reset of SI and alignment of charging and letdown, more than 30 minutes had passed, the pressurizer filled solid, and the PORVs had actuated repeatedly.

- ~ 5 minutes to realign valves which had not appropriately positioned because of SI.
- 4 minutes required to complete EOP steps, including control of AFW and isolation of MSIVs (2/4 had not closed).
- ~ 17 minutes to reset initial SI.
- ~ 17 minutes to establish pressure control with letdown and charging.

2) Salem operators took ~17 minutes to terminate SI during the 1st SI (and12 minutes for the 2nd SI) and the PRZR did become water solid. Salem's FSAR analyses include an allowance of 20 to reset SI for inadvertent actuation. However, Westinghouse recently provided information on this topic, stating that "Westinghouse has discovered that potentially non-conservative assumptions were used in the licensing analysis of [Inadvertent SI].... The PRZR shall not become water solid...within the minimum time required for the operator to identify the event and terminate the source of fluid increasing the RCS inventory. Typically, a 10 minute operator

action time has been assumed." The AIT concluded that the Westinghouse-recommended actions may need to be re-examined in light of the Salem experience.

U3 EOO, Mistake Operators fail to control secondary pressure, resulting in SG safety valve opening, rapid cooldown and second SI.

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Plant functions lost: 1) Loss of PRZR steam bubble. *Safety equipment actuation:* 1) PRZR level control system tried (but failed) to maintain level by limiting letdown and increasing charging. 2) PORVs together actuated over 300 times. 3) SG atmospheric RVs (not successfully). 4) SG code safety valves.	*Procedures:* 1) No clear guidance on solid plant pressure control provided in SI Termination EOP. *Training:* 1) Operators did not recognize RCS heatup and corresponding S/G pressure increase. 2) Training: No attempt was made to control secondary pressure prior to the rapid pressure decrease that led to auto and manual actuation of SI. 3) Operators did not anticipate the effect of the lifted S/G code safety valve on the solid plant pressure (i.e., rapid pressure reduction). No diagnosis of the effect of the open safety valve on the solid plant until pressure rapidly fell. *Stress: workload:* 1) Because of his involvement in manual valve alignments, the secondary operator did not adequately monitor and maintain a stable S/G pressure. Secondary operator did not establish adequate heat removal using the atmospheric steam dumps	*Situation Assessment:* 1) Failed to recognize rising pressure in S/G. 2) Failed to anticipate rapid depressurization following S/G safety valve lifting.

R1, Recovery Operators manually open and close SG atmospheric dump valves to control RCS temperature and control RCS pressure through letdown and charging.

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Plant functions lost: 1) Solid plant operation *Safety equipment actuation:* 1) PRT rupture disk fails	Notes: R1 included because of suboptimal performance. Positive operator performance: (U2) Recognized conditions requiring 2nd SI (manual as well as auto SI) and (R1) decay heat and pressure controlled by manually opening and closing S/G atmospheric dump valves and letdown and charging.	*Response Planning:* 1) No procedural guidance or plans for pressure control during solid PRZR conditions. 2) Failed to recognize or use yellow path functional recovery procedure to re-establish PRZR bubble.

A.4.4 ACCIDENT DIAGNOSIS LOG

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
07:30	~73% power (less than full power because of marsh grass interfering with traveling screens @ CW intake structure, resulting in increase in condenser back pressure). 12A circulator out of service for water-box cleaning.	
10:16	Massive river grass intrusion @ CW intake structure begins. 13B circulating water pump emergency trips on traveling screen differential pressure (between 10:15 and 10:40 am 13A, 13B and 12B traveling screens all clog and eventually go out of service, causing corresponding CW pumps to trip off line).	
10:27	13A pump trips on high screen differential pressure.	
10:30		Power had been decreased to ~60% because of condenser back pressure (from grass interfering w/ CW traveling screens)
10:32		UI: Unit 1 operators initiate power reduction from approximately 650 MWe @ 1% minute initially (power had already been decreased from 800 MWe at this point because of condenser back pressure). Subsequently, power reduction rate was increased to 3%, 5%, then (an atypical) 8% per minute by inserting control rods and borating. (As turbine operator reduced unit load, reactor operator correspondingly reduced RX power. Initially, operators reduced turbine power ahead of RX power, resulting in power mismatch and slightly higher than normal RCS temperatures.)
10:34		Operators try to start 12A circulating water pump, but pump immediately trips as a result of the pump circuit breakers not being fully racked in.
10:39	All CW pumps except 12B have tripped.	P-8 permissive reset (reactor trip on low coolant flow in a single loop) reset (blocked) @ 36% power. 13A and 13B pumps are restarted but by 10:46 they have tripped again, leaving 12B as the only circulator in service.
10:43	Reversal of power mismatch and decreasing T_{ave}.	P-10 permissive reset @ 10% RX power (power range low setpoint RT and intermediate range RX trip and rod stop). UI: NSS directs RO at rod control panel to go to electrical distribution control panel to perform group bus transfers (shifting loads to offsite power sources). (RO gone for 3-5 minutes.) (Operators believed plant was stable, failing to recognize that RX power was still decreasing because of delayed effects of the boron addition made.)
10:44	Turbine load @ 80 MWe, RCS temp - 531 °F (RCS cooled to below minimum temperature for critical operations). Low-low T_{ave} bistables trip (setpoint Tech Spec allowable value $ 541 °F).	

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
10:45	PRZR level < 17%, PRZR heaters auto-off to control level. Contraction of coolant because of low RCS temperature.	U1: NSS identifies over-cooling resulting from delayed effect of boration. NSS goes to reactor control panel and begins to withdraw control rods to raise RCS temperature - rods pulled 35 steps (from step 55 to step 90 on control rod bank D). NSS then turns control over to RO. NSS tells RO to raise power to restore plant temp. RO begins steady "pull" - 7% - 25% power. (NSS doesn't tell RO about NSS's actions, or how far or how fast to raise power.)
10:47	RX trip @ 25% - 25% power range low setpoint ("reactor startup" nuclear instrument (NI) trip). NI "intermediate range" 20% power rod stop and 25% power reactor trip did not actuate. Automatic SI on high steam flow (spurious signal resulting from pressure wave in MS lines caused by closing of turbine stop valves when turbine automatically tripped) coincident with low-low T_{ave}. All ECCS pumps start. ECCS flow paths functional, MFW regulating valves close. No "1st out" alarm for SI, SI signal received on SSPS logic channel "A" only. Not all alignments successful	
10:49		Operators enter EOP - Trip 1 procedure.
10:53		Operators manually isolate MFW. Secondary operator misses monitoring SG pressure, auto-control doesn't work because of the design. (As a result of the nature of initiating signal, SI did not successfully auto-position all necessary components, requiring operators to manually reposition affected components.)
10:58		Operators manually initiate MS isolation (only 2 of 4 MS isolation valves auto-closed at the time of auto-initiation of SI). Operators manually trip MFW pumps.
11:00		"Unusual Event" declared on the basis of "Manual or Auto ECCS actuation with discharge to vessel."
11:05		Following EOP step 36, operators reset and terminate SI. Operator notices SI logic channel "B" already reset (indicating that "B" channel had not auto-initiated) and SI logic disagreement light flashing (RP4 panel). Operators discuss whether train B should be considered inoperable. Operators begin trying to establish pressure control using letdown and charging.

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
11:18	PRZR PORVs (PR-1 and PR-2) periodically open on high pressure (indicating PRZR was fully to solid condition). (Primary heats up because of decay heat and running RCPs while operators perform EOP steps. PRZR fills because of heatup and volume of water added by SI. SG atmospheric RVs open several times to control secondary temperature and pressure. Because of pre-existing problems with these valves, SG pressure is not controlled properly. (Concurrent with PRZR filling, SG pressure increased because of primary heatup.) T_{ave} is 552 F. SG code safety valves (11 and/or 13) open, causing rapid RCS cooldown. Because of solid PRZR conditions, rapid SG pressure decrease also results in rapid decrease in primary pressure. (This indicated that SG atmospheric RVs were not properly controlling pressure.)	Transition to EOP - 3, SI Termination. U2: Operators fail to recognize and control increasing primary temperature and pressure and PRZR level. U3: Operators fail to recognize increasing secondary pressure. Operators do not anticipate the rapid pressure reduction resulting from SG safeties opening.
11:26	2nd Auto SI - initiated by low PRZR pressure (Auto "B" only, "A" had been reset). (Low PRZR pressure setpoint >1765 psig, allowable >1755 psig). Low PRZR pressure because of RCS cooldown resulting from SG safety valves opening. Numerous PORV openings because of SI	Operators manually SI (just after auto-SI) in response to rapidly decreasing RCS pressure (when RCS pressure reached SI setpoint).
11:41		Reset and terminate 2nd SI. Operator notices SI logic in agreement (RP4 panel). Tech Spec action statement (TSAS) 3.0.3 entered as a result of two blocked auto-SI trains.
11:49	PRT rupture disc fails (as expected). (PRZR solid or nearly solid after 1st SI @ 10:47, and the 2nd SI resulted in sufficient relief of RCS to the PRT to raise level and pressure until rupture disk blew.)	Operators have no clear guidance on solid plant pressure control. They do not consider yellow path. R1: Operators control RCS temp with manual control of 3 out of 4 MS10s (SG atmospheric RVs). (Operators had difficulty with the controls for a fourth MS10 earlier.) Operators control RCS pressure through a combination of charging and letdown using the CVCS.
12:54		Because of an SG safety valve opening, difficult to control SG atmospheric RVs.
13:16		Alert declared (in order to ensure proper technical staff available). Licensee staff recognized that TSAS 3.0.3 could not be met for inoperable SI logic channels. Operators also concerned about how to properly restore the PRZR to normal pressure and level from solid RCS conditions and wanted sufficient engineering support.
13:36		The NRC entered the monitoring phase of the Normal Response Mode of the NRC Incident Response Plan. NRC Region I activated and staffed their Incident Response Center, with support provided by NRC headquarters personnel.
14:10		Technical Support Center was staffed to assist control room operators with recovery of normal RCS pressure and level control.
15:11		Operators restore PRZR bubble.
16:30		PRZR level restored to 50% (normal band), level control returned to auto. EOPs exited, IOP-6 (Hot Standby to Cold Shutdown) procedure entered.

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
17:15		Plant cooldown initiated.
20:20		Alert terminated.
01:06		Mode 4 (Hot shutdown) entered.
11:24		Mode 5 (Cold shutdown) entered.

A.5.1 EVENT IDENTIFIER - Wolf Creek

Plant Name:	Wolf Creek
Plant Type and Vendor:	PWR/W
Event Date, Time:	09/17/94, 4:00 am
Secondary Initiator:	None
Unit Status:	Hot shutdown
Data Sources:	AEOD/S95-01 Special Report (3/95) & Wolf Creek Incident Investigation Team Report 94-04 Revision 2 (4/14/95)
Data Input By:	William J. Luckas, Brookhaven National Laboratory, (516) 344-7562 [Susan Cooper, SAIC, (302) 234-4423]

A.5.2 EVENT SUMMARY

Event Description: In September 1994, the WCNPC's Wolf Creek Generating Station had an inadvertent discharge of ≈9, 200 gals. of 350 psig reactor coolant (RC) at 235-300°F through the residual heat removal (RHR) system to the refueling water storage tank (RWST) rapidly in ≈66 seconds. Before the event, the reactor (RX) was shutdown, borated to ≈2000 ppm concentration and in the process of cooling down via one RHR train. The nonoperating RHR train was being lined up in the plant for boron recirculation because of an RHR check valve leakage from the reactor coolant system (RCS) at the same time an RHR valve was being stroked from the control room (CR). The RCS and the operating "A" RHR train loop were pressurized @ 350 psig with 2 [of 4 total] reactor coolant pumps (RCPs) operating. The pressurizer (PZR) was being filled by reducing RCS letdown as part of the cooldown. The idle "B" RHR train was being setup with an inter-system lineup to increase the train loop boron concentration from = 1200 ppm to within 50 ppm of the RCS ≈2000 ppm boron concentration by "recircing" through the 2000 ppm boron concentration RWST water.

The inadvertent discharge was initiated when an operator in the CR remotely cycled a valve while another operator out in the plant simultaneously opened a manually operated valve as part of the RHR boron recirculation activities. As indicated in the CR, the RWST high-level alarm was received while the PZR level was dropping rapidly. The blowdown was terminated after a relief crew supervising operator (SO) in the CR suggested that the CR, licensed, balance of plant (BOP) operator remotely close the RHR valve being stroke-tested.

If the event had not been quickly terminated in 66 seconds @ ≈225 psig (and decreasing), a continuing 350 psig/300°F RCS blowdown through the unpressurized portion of the RHR system would have uncovered the RCS hot leg and most likely would have introduced a two-phase, steam-water mixture into the RWST header line in 3 minutes (and possibly less). If the blowdown had lasted 6 minutes, a 90% void fraction in the RWST header line would develop and remain until the blowdown was isolated.

Event Surprises:

(1) Unrecognized design vulnerability - very severe potential problem of flashing in common ECCS header.
(2) Incompatible work activities - RHR loop boron recirculation while stroke testing certain valves
(3) Lost ≈9300 gallons of RX coolant in ≈66 seconds!
(4) Heated up ECCS supply header from RWST so as to jeopardize the ability of safety injection to function (at all).
(5) Compressed outage schedule - planned for 40 days with previous shortest of 47 days.
(6) Difficulty of operators to rely on and follow shutdown procedural guidance during LOCA and loss of RHR in this event.
(7) Poor mental model of system valves by some operators and understanding that valve stroking was not to be performed in Mode 4.

Licensee Corrective Actions:

(1) Enhance RHR operations procedure SYS EJ-120 to alert operator of potential RCS blowdown should a misalignment occur with HV-8716A or HV-8716B and BN-8717.
(2) Install a caution placard on manual valve BN-8717.
(3) Evaluate inclusion of licensee's "Incident Investigation Team Report 94-04" into operator training.
(4) Change boron concentration requirement in the RHR procedure to minimize the need to perform a boration evolution while shutting down.

ATHEANA Summary

Deviation From the "Expected" Scenario:

(1) The principal deviation from the "expected" scenario is probably how large and how quickly RCS was lost (i.e., ~9,200 gallons in ~66 seconds).
(2) Another deviation from the "expected" scenario is that the RCS loss was the result of actions performed by two, independent operators (one in the plant and the other in the control room). The "expected" scenario probably would be the result of a single action.

Key Mismatch(es):

(1) The principal mismatch was the incompatible work activities of RHR loop boron recirculation and RHR valve stroking testing. Although several factors are cited as reasons for this mismatch, the omission of the pre-requisite of being in Mode 5 or 6 (rather than Mode 4) for the stroke testing procedure certainly was a factor.
(2) The shutdown procedural guidance was apparently not a good match with the conditions the operators faced during this LOCA and loss of RHR.

Most Negative Influences:

(1) Poor mental model of system/valves by some licensed operators.
(2) Stress: workload: A compressed outage schedule was in place to accomplish all identified work in about 40 days. This schedule was several weeks shorter than previous outages at Wolf Creek. The shortest previous Wolf Creek outage ever was 47 days (completed in November 1994). Manual alignments of components which did not automatically actuate w/ SI and concerns re: the operability of SI "B."
(3) Control and outage planning heavy reliance on the control room crew to identify potential problems and ensure that plant conditions could support the planned activities.
(4) BOP operator did not take the time to perform an adequate brief, review the procedure, or review the prints prior to performing SYS EJ-120 borating RHR train "B"
(5) NSO was not adequately briefed before performing SYS EJ-120 borating RHR train "B."

Most Positive Influences:

The blowdown was terminated (in about 66 seconds) after a relief crew SO in the CR suggested that the CR, licensed, balance of plant (BOP) operator remotely close the RHR valve being stroke-tested.

Significance of Event:

Extreme or unusual conditions. None initially. Subsequently, lost ~9300 gallons of RCS (in 66 seconds).
Contributing pre-existing conditions. Isolated RHR loop boron concentration low because of leaky check valves, requiring recirculation of train "B" to RWST to raise concentration.
Misleading or wrong information. None.
Information rejected or ignored. None.
Multiple hardware failures. None.
Transitions in progress. Several activities in progress, most important of which were the stroke testing of one valve (from the control room) simultaneous with the opening of a manually operated valve (in the plant) as part of the RHR boron recirculation activities.
Similar to other events. Not known.

KEY PARAMETER STATUS	
Initial Conditions	**Accident Conditions**
Power level: 0% (subcritical) RCS temperature(°F): (via RHR in/out) 302/234°° RCS pressure: ≈350 psig RCS level: Nominal Other: PZR nearly full and filling (i.e., almost solid); boron concentration ≈2000 ppm; SGs filled up,; cold overpressure protection (COP) system armed (i.e., PZR PORVs reset to lift at ≈460 psig)	Power level: 0% (subcritical) RCS temperature (°F): ≈309 (≈+7°F due to PZR outsurge) RCS pressure: 225 psig RCS level: Lost ≈9300 gallons of reactor coolant to RWST (with overflow to radwaste hold-up tank). Other: Pressurizer low (< 17%); RCS boron concentration ≈2000 ppm; SGs filled up; at < 17% in PZR, backup heaters deenergized and RCS pressure control lost

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configurations	**Accident Conditions and Consequences**
Evolution and activities: (1) Cooling down & reducing pressure in RCS per procedure GEN-006, Rev. 27. (2) Removing RX decay heat & RCP heat for ≈4 hours by RHR Train "A." (3) Filling PZR in anticipation of going solid. (4) Testing of EDF "B" into 23th of 24 test-run. **Configuration:** (1) RHR Train "A in service to remove RX decay heat & heat input from the 2 operating RCPs. (2) 2 of 4 RCPs secured (at least 8 hours) - the other 2 help provide RX flow & RCS pressure control. (3) EDG "B" paralleled to the grid, thus the 2 secured RCPs could not be restarted (because they draw high starting current). (4) RCS/CVCS letdown flow reduced to only one 75 gpm orifice to help charging pump completely fill PZR and cool it down and keep it < 200°F for cold. (5) PZR PORVs reset to life at ≈460 psig (cold overpressure protection (COP) system armed) & positive displacement pump + 1 of 2 centrifugal charging pumps secured & their breakers locked open to help COP. (6) PZR level high alarm activated & high level indications since PZR is being filled solid and its level is above the high level alarm setpoint. (7) RHR train "B" needs to be unisolated as a backup to train "A." **Preexisting operational problem:** (1) Isolated RHR loop boron concentration low due to leaky check valves, requiring recirculation of train "B" to RWST to raise concentration. (2) Positive displacement pump and 1 of 2 centrifugal charging pumps secured & breakers locked open to help ensure cold overpressurization protection (COP). (3) Locked manual valve BN-8717 (RHR pump discharge to RWST for RHR train boron recirculation). **Initiator:** (1) Loss of RCS resulted when two valves in the RHR system were opened simultaneously.	**Automatic Response:** (1) RWST level high alarm actuated. (2) PZR level high alarm cleared. **Failures:** **Human-System Interactions** **Defeated defenses:**

A.5.3 ACTION SUMMARY

Event Timeline:

Pre-initiator	Initiator	Post-Accident
00:01	04:10	04:11
^ ^	^	^
H1 H2	U1 U2	R1

Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
H1	Operator (in control room) lined up & put into service RHR train "A" & its supporting systems to continue RCS cooldown.
H2	RX operation (in control room) raises PZR level to continue RCS cooldown.
U1	NSO (out in plant) opens 8" manual valve BN-8717* to set up for RHR train "B" recirculation to increase RHR boron concentration to within 50 ppm of RCS concentration.
U2	BOP operator (in control room), with SS's permission, strokes open HV-8716A** remotely for first time and closes same via control board pushbuttons and strokes the valve open a second time (≈30 seconds later)
R1	BOP operator recloses HV-8716A on the basis of advice of Relief SS

* BN-8717 - RHR pump discharge manual isolation valve in common 8" discharge line to RWST for RHR train boron recirculation.

** HV-8716A - RHR Train A isolation valve in (10") cross-over line to hot leg recirculation loops 2 and ? (remotely operated from control room)

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**
U1, U2	Cascading effect (because of poor communications and situation assessment)	Simultaneous and uncoordinated ex-control room actions result in loss of RCS. Opened two valves simultaneously which violated the RCS pressure boundary (i.e., initiated RHR recirculation concurrently with valve stroking).

Unsafe Actions Analysis — **Wolf Creek**

U1 EOC, Mistake NSO (out in the plant) opens 8" manual valve BN-8717 to set up for RHR train "B" recirculation to increase RHR boron concentration to within 50 ppm of RCS' concentration.

Error Forcing Context

Plant Conditions	Performance Shaping Factors	Failures of Information Processing
Evolution and activities: 1) Removing RX decay heat and RCP heat for ≈4 hours by RHR Train "A." *Configuration:* 2 1) RHR train "B" needs to be unisolated as a backup to train "A." *Preexisting operational problem:* 1) Isolated RHR loop boron concentration low because of leaky check valves, requiring recirculation of train "B" to RWST to raise concentration. *Administrative controls:* 1) Locked manual valve BN-8717 (RHR pump discharge to RWST for RHR train boron recirculation) (i.e., requires manual set-up for isolated RHR train "B."	*Training:* 1) NSO had a poor mental model of system/valves. *Communications:* 1) NSO was not adequately briefed prior to performing SYS EJ-120 borating RHR train "B." *Stress:* 1) Time of day.	

U2 EOC, Mistake BOP operator (in control room) strokes open HV-8716A remotely twice (30 seconds between stroking) via control board pushbuttonss.

Initial Conditions: 1) RCS temperature(°F): (via RHR in/out) 302/234° 2) RCS pressure: ≈350 psign 3) RCS bsron concentration ≈2000 ppm ° *Evolution and activities:* 1) Removing RX decay heat and RCP heat for ≈4 hours by RHR Train "A." *Configuration:* 1) RHR train "B" needs to be unisolated as a backup to train "A." *Preexisting operational problem:* 1) Isolated RHR loop boron concentration low because of leaky check valves, requiring recirculation of train "B" to RWST to raise concentration. *Administrative controls:* 1) Locked manual valve BN-8717 (RHR pump discharge to RWST for RHR train boron recirculation) (i.e., requires manual set-up for isolated RHR train "B."	*Procedures:* 1) Stroke testing documentation had a pre-requisite requiring this test be done in Mode 5 or 6. It was actually performed in Mode 4 and the pre-requisite was improperly marked "N/A." *Training:* 1) BOP operator did not take the time to perform an adequate brief, review the procedure, or review the prints before performing SYS EJ-120 borating RHR train "B". 2) Poor mental model of system/valves by some licensed operators. *Supervision:* 1) "On-shift SO did not exercise proper command and control techniques to maintain full awareness of plant conditions." SO authorized the simultaneous performance of two incompatible work activities. *Organizational Factors:* 1) Control and outage planning heavy reliance on the control room crew to identify potential problems and ensure that plant conditions could support the planned activities. 2) Operators failed to plan and appropriately control work activities in that two incompatible activities were allowed to be performed simulataneously. *Stress:* 1) A compressed outage schedule was in place to accomplish all identifed work in about 40 days. This schedule was several weeks shorter than previous outages at Wolf Creek. The shortest previous Wolf Creek outage ever was 47 days (completed in November 1994). Manual alignments of components which did not automatically actuate w/ SI and concerns re: the operability of SI "B." 2) Time of day	*Situation Assessment:* 1) Failed to monitor and recognize RCS heatup and increasing PRZR level after RT and SI.

A.5.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	RESPONSE
20:00	Cold Overpresure Protection (COP) system armed; PDP & 1 of 2 CCPs secured and their motor breakers open.	
21:25		SS held discussions with maintenance staff involved with retest of HV-8716A which includes valve stroking with concurrent packing adjustment.
00:01	H1: Operator (in control room) lines up and puts in service "A" RHR train and its supporting systems to continue RCS cooldown.	
	H2: RX operator (in control room) controlling CVCS to slowly increase PZR level in preparation for going solid.	
03:00		Again, SS held discussions with maintenance staff involved with retest of HV-8716A. SS also granted permission to adjust packing.
04:10	**U1**: NSO slowly starts to open 8" manual valve BN-8717 to manually set up for RHR train "B" recirculation to match RCS boron concentration.	
	U2: BOP operator strokes open HV-8716A, remotely for the first time.	
04:10 : 30	**U2**: BOP operator strokes open HV-87167A, remotely for second time (30 seconds after first)	

A.6.1 EVENT IDENTIFIER - Davis-Besse

Plant Name:	Davis-Besse
Plant Type and Vendor:	PWR/B&W
Event Date, Time:	06/09/85, 1:35 am
Event Type:	Loss of Main and Auxiliary Feedwater
Secondary Initiator:	None
Unit Status:	Full-power
Data Sources:	NUREG-1154, July 1985
Data Input By:	John Wreathall, Wreathall & Co., (614) 791-9264 [Susan Cooper, SAIC, (302) 234-4423]

A.6.2 EVENT SUMMARY

Event Description: In June 1985, Davis-Besse, following a history of main feedwater pump (MFP) spurious trips, was operating with 1 of 2 MFPs in manual control. The other MFP tripped, causing a reactor trip. The operator, anticipating the Steam Generator (SG) low-level signal to initiate auxiliary feedwater (AFW) automatically, attempted to use manually the Steam Feedwater Rupture Control System (SFRCS) pushbuttons to initiate AFW. However, he inadvertently pressed the pushbuttons that isolate AFW from the SGs. After a brief delay, the operators reset the SFRCS and initiated AFW. Because of two separate common cause failures, the AFW system failed to provide feedwater. Equipment operators (EOs) were dispatched to recover operation of the AFW pumps and valves and to initiate the manual startup (SU) feedwater system. However, the SGs reached "dryout" conditions, thus meeting the requirement to begin RCS feed-and-bleed cooling. The operators delayed feed-and-bleed cooling in the belief that SG feed and secondary inventory for RCS heat removal were about to be recovered, which it was.

Event Surprises: None.

Licensee Corrective Actions: None.

ATHEANA Summary

Deviation From the "Expected" Scenario:

1) Multiple common-mode failures of the AFW system was a significant deviation from the operators' expectations of equipment performance in their scenario and delayed their response.
2) The operator's attempt to use, and the lock-out feature of, the SFRCS that prevented automatic initiation of the AFW system was a deviation from the expected scenario.

Key Mismatch(es):

1) The time required to restore the failed AFW system compared with the operators' expectations of restoring the system was a key mismatch.
2) The operators' confidence in restoring AFW compared with the procedural guidance of when to initiate feed-and-bleed operations mismatched.

Most Negative Influences:

1) For the delay of feed-and-bleed, the operators perception that the consequences of feed-and-bleed were very drastic and their confidence that some sort of feedwater would be recovered dominated.
2) Various common cause hardware failures, including those that resulted in the loss of all feedwater, occurred.
3) For inadvertent isolation of AFW, human engineering of the panel (i.e., location and layout), lack of training and experience, and perhaps, the time of day were important.

Most Positive Influences:

1) Timely ex-control actions of the equipment operators saved the plant from damage.

Significance of Event:
Extreme or unusual conditions. None initially. Subsequently, steam generators reach "dryout" conditions and feed-and-bleed criteria.
Contributing pre-existing conditions. Multiple conditions that probably contributed to this event, (e.g., recent history of spurious feedwater pump trips, feedwater pump #2 in manual control, torque switches on AFW isolation valves incorrectly set, and SPDS was inoperative in the control room).
Misleading or wrong information. PORV position indicated that valve was shut (when it was actually stuck open).
Information rejected or ignored. Sonic signals indicating open PORV. (Block valve was closed as a precaution despite the fact that operators did not understand that the PORV was open.)
Multiple hardware failures. AFW system (once because of operator error, twice because of separate common cause failures), PORV stuck open, control room HVAC tripped into emergency mode, main turbine did not go to turning gear.
Transitions in progress. None.
Similar to other events. Recent experience with spurious MFW pump trips at power. MFW pump #2 in manual control for this reason.

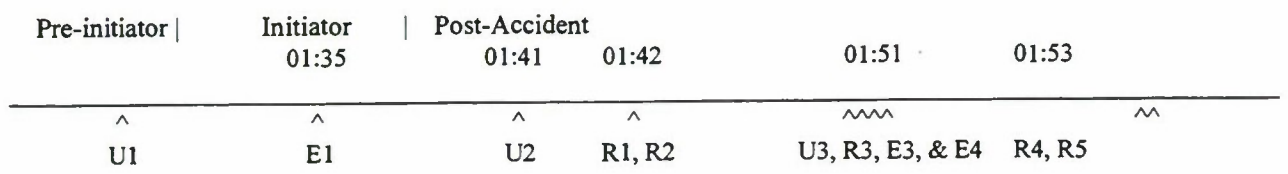
KEY PARAMETER STATUS	
Initial Conditions	**Accident Conditions**
Power level: 90% RCS temperature (°F): 582 RCS pressure: 2170 psig RCS level: Nominal Other: PZR level - 200," SG level - normal	Power level: 0% RCS temperature (°F): 592 RCS pressure: 2440 psig RCS level: Other: PRZ level - 76-300", SG level - 8". Minimal inventory loss via PRZ PORV.

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configurations	**Accident Plant Conditions and Consequences**
Configuration: Normal **Preexisting operational problem:** Repeated recent history of spurious MFP trips at power (1) MOV torque switches incorrectly set (unknown to plant) (2) Main feedwater pump #2 in manual control. (3) Positive displacement pump and 1 of 2 centrifugal charging pumps secured & their breakers locked open to help ensure COP. (4) One source range NI channel inoperable. (5) PZR high level alarm & indications were unavailable, since the PRZ is being filled solid and its level is above the high alarm setpoint. (6) SPDS inoperative in control room. **Initiator:** Loss of main and auxiliary feedwater resulted from an combination of human and hardware (including common cause) failures.	**Automatic Response:** (1) RT because of a loss of main feedwater. **Failures:** (1) AFW turbine pumps (2) tripped; would not reset. AFWTP trips caused by flashing of saturated water in turbine nozzles. (2) AFW isolation valves (2) failed closed. AFW isolation valves – bypass contacts on torque switches mis-set. (3) PZR PORV stuck open on 3rd opening. (4) CR HVAC spuriously tripped to emergency mode. (5) Main turbine did not go to turning gear. **Human-System Interactions** **Latent failures:** (1) AFW isolation valves with incorrectly set torque switches (design unsafe act) **"Aggravating actions":** (1) Operator inadvertently caused isolation of both SGs – slip **"Things left undone":** (2) Intentional failure to initiate feed-and-bleed

Unsafe Actions Analysis		Davis-Beese
U1 EOC, Unknown maintenance personnel miscalculated torque switches on AFW isolation (isol.)		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Not Known		
U2 EOC, Slip Operator inadvertently selects wrong buttons on SFRCS		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Notes: NUREG-1154 does not discuss any causes of this event.	*Training:* 1) Operation of the SFRCS often not covered in training. 2) Manual anticipation of automatic operation "common." *Human-System Interface:* 1) Poor location of panel. 2) Confusing layout of switches. *Stress:* 1) Time of day. *Other:* 1) Operator had never used SFRCS before.	*Response Implementation:* - Operator inadvertently selected wrong pushbuttons on a confusingly designed and poorly located control panel.
Notes:		
U3 EOO Correct violation Operators decline to implement "feed-and-bleed"		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Three consequence of feed-and-bleed operations would have been 1) to breach one defined raiological barrier (RCS boundary); 2) to create operational difficulties and uncertainties in reaching cold shutdown; and 3) delayed restart to clean up contaminated areas.	*Communications:* 1) Shift supervisor was in phone communications with the operations superintendent when SG s were "drying out"; potentially delayed response. *Human-System Interface:* 1) SG level indication not adequate to determine if feed-and-bleed criteria met (8″ indicated on a scale of 0-250″). 2) SPDS out of service (could have provided backup indication of SG level). *Stress:* 1) Fee-and-bleed judged to be "pretty drastic."	*Response Planning:* - Operator deliberately elected to delay implementing feed-and-bleed in the expectation that feed flow would be available shortly.
Notes: The delay in implementing feed-and-bleed instructions once the criterion of dryout (8″) had been met was only 3-5 minutes. The operator had knowledge of the actions to restore SG cooling.		

A.6.3 ACTION SUMMARY

Event Timeline:



Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
U1	Maintenance personnel miscalibrated torque switches on AFW isolation (isol.) valves.
E1	MFW pump "1" trips – RX & turbine trip on high RCS pressure.
U2	Operator inadvertently selects wrong buttons on SFRCS (low SG pressure) in anticipation of automatic low SG level – isolates both.
R1	Shift supervisor (SS) resets SFRCS & correctly presses low SG level buttons.
E2	AFW isolation valves fail to open.
R2	EOs dispatched to equipment areas to recover: AFW pumps, SU feedwater pump, AFW isol. Valves.
E3	SG atmospheric dump valve sticks open.
E4	PZR PORV sticks open.
U3	Operators decline to implement "feed-and-bleed" despite (1) procedures, and (2) management instructions.
R4	AFW train 2 has significant flow.
R5	AFW train 1 has significant flow.

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**

A.6.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	Response
01:35	MFW pump 1 trips; reactor and turbine trip shortly thereafter	Operators attempt to increase feedwater flow using Pump 2 but insufficient to prevent trip.
01:36	MSIVs closed	
01:40	MFW pump 2 terminates feeding because of low steam pressure	
01:41	Falling SG water levels noted by secondary-side operator (< 27″)	**U1:** In attempting to anticipate the automatic initiation of AFW, operator inadvertently isolates SGs.
01:42		**R1:** Shift supervisor resets SFRCS, attempts to start AFW. Multiple hardware failures cause failure of both trains of AFW.
01:42	Failure of AFW system	**R2:** Operators dispatched to manually start SUFP and recover AFW equipment.
01:42	Both SGs meet "dried out" criterion as defined in EOPs (pressure < 960 psig)	
01:51	RCS pressure at 2425 psig and falling (Pressurizer PORV stuck open - **E3 & E4**)	**R3:** Operator does not diagnose PORV stuck open ("demand" position, not actual position indicated; overlooks sonic signals), but closes PORV block valve as a precaution (also PZR spray valve).
01:51	SG levels and pressure (<8″ , <960 psig) meet feed-and-bleed criterion	**U3:** Operators postpone feed-and-bleed instruction in procedure.
01:51	SUFP operating, feeding SG #1	
01:53	AFW train 2 providing "significant flow" - **R3**	
01:54	AFW train 1 providing "significant flow" - **R4**	
02:04	Plant stable	

APPENDIX B
ATHEANA EXAMPLE -
DEGRADATION OF SECONDARY COOLING

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that would result in the inappropriate reduction of secondary cooling in a pressurized water reactor (PWR). More specifically, it is an illustration of the use of ATHEANA to identify and quantify those circumstances (contexts) that may induce human actions involving the inappropriate degradation or nonrestoration of secondary cooling during an event where secondary cooling has been initially disrupted and needs to be properly restored and maintained to provide adequate core cooling.

This is a plant-specific example, as all fruitful examinations of context must be. However, the plant analyzed is a composite PWR, not exactly matching any particular plant. The example is realistic in that all specific design, procedures, training and operating and maintenance practice information used in the analysis have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate a similar issue at their plant.

The example follows the steps discussed in the ATHEANA process in Section 9 of this document.

B.1 Step 1: Define and Interpret the Issue

This analysis identifies the possible conditions that might induce nonrestoration, shutting off, or at least, inappropriate reduction of secondary cooling in a PWR in response to an event involving an initial loss or serious degradation of steam generator secondary cooling flow during full-power plant operation. Throttling of secondary flow is part of the normal response after reestablishment of secondary cooling following a reactor trip in response to such an event. However, industry experience includes events where premature or excessive throttling of secondary cooling has occurred. In light of this experience, the purpose of this analysis is to identify those circumstances (contexts) that may induce human actions involving the inappropriate degradation or nonrestoration of secondary cooling during such an event. The results of the analysis are to be used to make any improvements (procedure changes, training changes, human/machine interface changes...) that would lessen the likelihood of operators inappropriately reducing secondary cooling during an event of this type.

B.2 Step 2: Define the Scope of the Analysis

Based on the description of the issue provided in Step 1, a review of representative initiators from Table 9.1, a direct internal plant transient, specifically loss of main feedwater (MFW) while at full power, was selected as the most relevant type of initiating event to use as the basis for examining this issue. The following reasons are offered for this selection.

First, loss-of-coolant accidents (LOCAs) involving the reactor coolant system (RCS), except for the smaller breaks, do not need nor are sensitive to the success of secondary cooling in order to achieve successful mitigation of the event. This is shown, for example, by the large LOCA event tree reproduced here from this plant's PRA (see Figure B.1). It shows no need for secondary cooling to achieve successful mitigation of the event. For the breaks of smaller sizes, the lack of proper

secondary cooling does contribute to how the scenario proceeds, but it is generally not as important as early RCS injection in determining the outcome of the event (safe or core damage). In addition, while the small LOCA and loss of main feedwater scenarios have similar needs for secondary cooling, the expected frequency of a small LOCA is two to three orders of magnitude less than that for a loss of main feedwater event, making the latter event much more likely to be experienced and therefore of more interest.

Second, virtually all transients (e.g., turbine trip) at this plant involve a concurrent initial loss of the normal feedwater anyway since the main feed regulating valves close on low T_{avg} (554°F) which is expected to occur in most events involving reactor trip. While other transient initiators with a concurrent loss of main feed may add complexity to the event, the complexities will be considered in this analysis to the extent that they do not represent other specifically analyzed initiators in this plant's PRA. For example, even though loss of instrument air is a form of transient that could contribute to the loss of main feed and add other complexities to the scenario, loss of instrument air is explicitly treated as another type of initiator in the PRA and will be considered outside the scope of this illustrative analysis.

Third, the loss of main feedwater event chosen has the characteristic that the need to reestablish secondary cooling is paramount. In this type of initiating event, human actions involving the disruption or prevention of secondary cooling could have serious consequences and even cause damage to the core if this and alternative means of cooling the core (e.g., feed and bleed) are not established. Based on these observations, the loss of main feedwater scenario is chosen as the most relevant form of accident for which to examine the defined issue.

The plant's PRA already covers the loss of secondary cooling (including the loss of auxiliary feedwater) due primarily to equipment failures. This loss is shown as contributing to core damage sequences 4 and 5, as well as the outcome to 6 [depending on the steam-driven auxiliary feedwater (AFW) train] in Figure B.2, for the loss of main feedwater initiator in the PRA. This ATHEANA analysis examines the potential contexts and the likelihood of a loss or degradation of secondary cooling due to operator actions not already covered in the PRA. Hence, the operator actions of interest contribute to those same sequences in ways not included in the current PRA.

Since this is a specific issue to be analyzed, there is no requirement to consider additional limitations of scope in this step beyond limiting the analysis to the loss of main feedwater initiator. Also, since this example is analyzing a specific issue, there is no need to prioritize among numerous issues or analyses that might be performed.

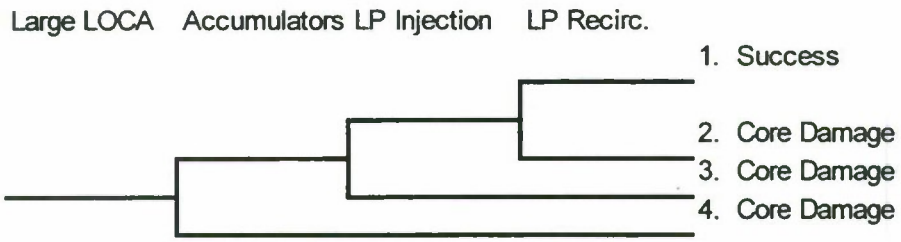


Figure B.1 Large LOCA Event Tree

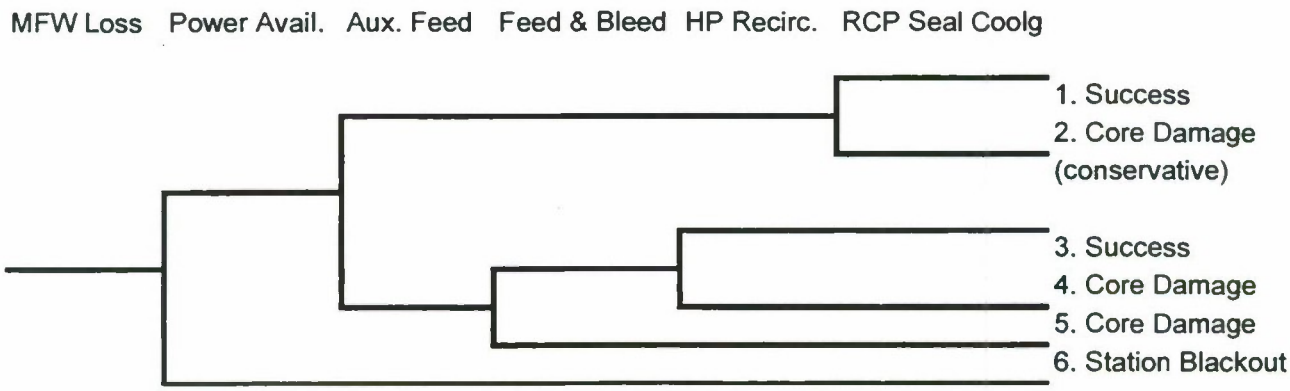


Figure B.2 Loss of Main Feedwater Event Tree

B.3 Step 3: Describe the Base Case Scenario

B.3.1 Introduction

This step of the analysis process defines a base case scenario for the loss of main feedwater event from which to develop other scenario contexts that may challenge the operating crew in ways that may be "error forcing." Ideally, the base case scenario has the characteristics shown in the first row of Table B.1; i.e., the scenario description represents a consensus of the expected plant response by most operators, it is well defined operationally, there are well-defined physics descriptions and adequate documentation of the plant response, and the scenario is realistic. As will be explained below, the base case scenario for this analysis has the characteristics shown in the second row of Table B.1.

Table B.1 Characteristics of Base Case Scenario

Base Case	Consensus Operator Model	Well-Defined Operationally	Well-Defined Physics	Well-Documented	Realistic
Ideal	Exists	Yes	Yes	Yes	Yes
Loss of main feed scenario	Based on what is "expected" by most operators as described in the text	Yes, in accordance with consensus operator model	Will start with a final safety analysis report (FSAR) version (called reference scenario)	Will start with a FSAR version (called reference scenario)	Yes, by modifying the FSAR version to make it more like the consensus operator model

The discussion starts with a well-documented reference scenario (from the FSAR) for the loss of main feed event and develops a "base case" scenario that is more in line with the expected plant and operator response for a loss of main feedwater event while the plant is operating at full power. The expected plant and operator response represents that which is well within the operators' training background and coincides with their limited experience of responding to an actual event at this plant. Purposely, no equipment failures or other complexities are considered in the expected scenario (the "base case" scenario) since these will be considered later as possible "deviations" from the base case scenario. Hence, this step provides a base case "signature" for a loss of main feed event from which additional complexities are later proposed that may make the operator response to the event "error-forcing" in a way described by the issue as summarized in Step 1.

B.3.2 Use of a Reference Case Scenario (from FSAR)

The base case loss or degradation of main feedwater scenario while the plant is at power is derived from the plant's FSAR Chapter 14, safety analysis, loss of normal feedwater accident analysis. This accident analysis serves as what will be referred to as the "reference scenario" from which the base

case scenario is derived. Operations staff receive periodic training on this type of event and thus a "knowledge of the event" and expectations of how the plant responds to such an event have been formulated in the minds of the plant's operators.

Based on the FSAR reference scenario, the loss of main feedwater while at power is an anticipated abnormal event which should not pose a threat of offsite radiation consequences. As stated in the FSAR, *a loss of normal feedwater results in a reduction in capability of the secondary system to remove the heat generated in the reactor core.* The FSAR cites the following features that protect against the loss of normal feedwater:

- *Reactor trip on low-low water level in either steam generator*
- *Reactor trip on steam flow; feedwater mismatch coincident with low water level in either steam generator*
- *Two motor-driven and one turbine-driven auxiliary feedwater pumps that start automatically on low-low level in either steam generator* [among other signals]

There are a number of conservative assumptions included in the FSAR analysis which apply to the reference scenario that is used to develop a description of the base case (expected) scenario. Among these are the following:

- the initial steam generator water levels are minimized
- initial plant power is 102%
- use of a heat transfer coefficient in the steam generators assuming natural (not forced) circulation
- use of a conservative heat generation rate
- credit for only one motor-driven auxiliary feedwater pump to only one of the two steam generators
- fouled steam generator tubes
- coincident loss of offsite power so that natural circulation flow exists in the reactor coolant system
- no credit for the nonsafety steam generator pressure control features.

These conservative assumptions tend to maximize the "effect" of the scenario and collectively result in an exaggeration of what is normally expected during a loss of main feedwater. Hence, the FSAR

analysis as the reference scenario is not fully consistent with the *base case* and more realistic plant response. Nevertheless, the FSAR analysis can be used to form the base case response.

The FSAR describes the expected sequence of events as follows:

> *Following the reactor and turbine trip from full load, the water level in the steam generators will fall due to the reduction of steam generator void fraction and because steam flow through the safety valves continues to dissipate the stored and generated heat ...following the initiation of the low-low level trip the auxiliary feedwater pump is automatically started reducing the rate of water level decrease. Sufficient heat transfer is available to dissipate core residual heat without water relief from the primary system relief or safety valves. If the auxiliary feed delivered is greater than that of one motor driven pump...the result will be a steam generator minimum water level higher than shown... .*

The FSAR concludes:

> *The loss of normal feedwater does not result in any adverse condition in the core, because it does not result in water relief from the pressurizer relief or safety valves, nor does it result in uncovering the tube sheets of the steam generator being supplied with water.*

The FSAR provides figures for the reference case which are duplicated here and where the following points are clearly presented:

- Figure B.3 shows that the average coolant temperature within the core region (T_{avg}) quickly drops upon reactor scram, then rises due to the initial mismatch between the heat generation and the degradation of heat removal because of the loss of main feedwater. Upon the initiation of the AFW system and as it provides sufficient water to the steam generator, the core coolant temperature then gradually falls again as reactor decay power continues to decrease and heat sink capability is fully restored via at least one steam generator.

- Figure B.4 shows the pressurizer liquid volume, which shrinks, expands, and then gradually decreases, following a trace roughly coincident with the T_{avg} plot above. Since the mass of the RCS is not changing, pressurizer level is a direct function of T_{avg} (i.e., RCS volume is proportional to T_{avg}).

- Figure B.5 shows the steam generator water level response within the fed steam generator, which falls due to steam flow/feed flow mismatch until the AFW system (AFWS) initiates and restores the water level.

B.3.3 Base Case Scenario

The base case scenario, largely on the basis of the "expected" consensus opinion of the operators (i.e., a consensus operator model), differs from the above reference scenario in that (a) all AFWS pumps successfully respond, (b) feeding to both steam generators occurs, (c) nonsafety RCS and

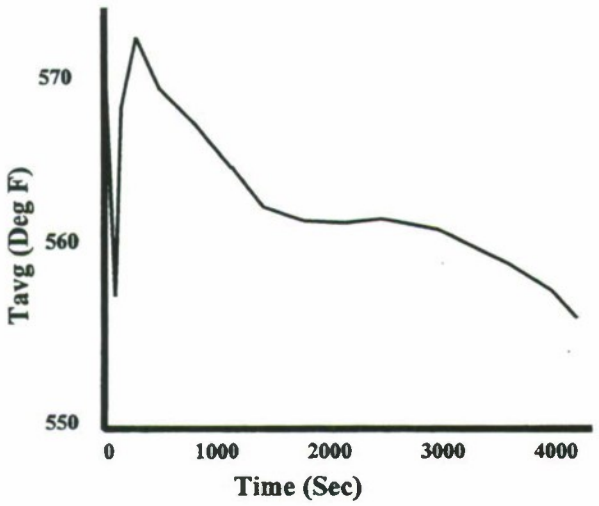


Figure B.3 T_{avg} During Loss of Main Feed.

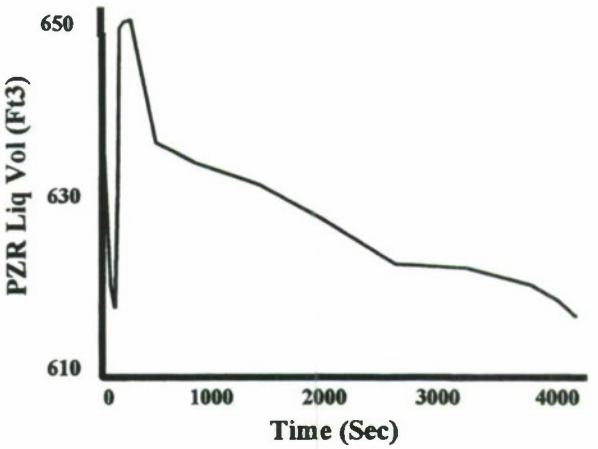


Figure B.4 Presurizer Volume During Loss of Main Feed.

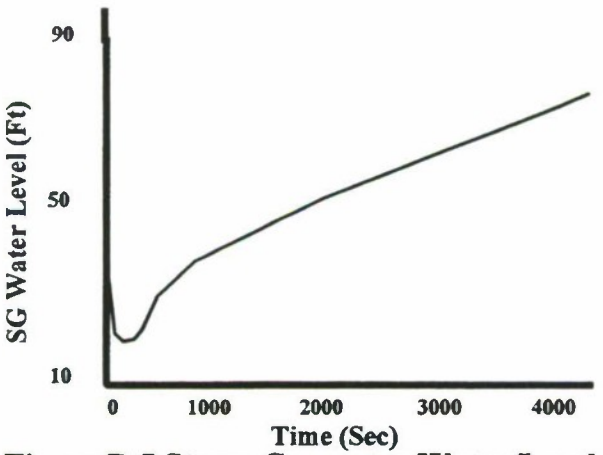


Figure B.5 Steam Generator Water Level During Loss of Main Feed.

steam generator control systems also function, and (d) the conservative assumptions used in the reference scenario do not exist. These are the primary features of the operators' consensus opinion of what is expected to occur in this type of scenario. As a result, the effects of the event would not be quite as severe for the base case scenario, which is defined to have the features of the consensus operator model. In particular, both steam generator water level responses would be similar since both steam generators are assumed to be fed. In addition, the changes in T_{avg} and pressurizer level may be slightly different due to operation of nonsafety equipment such as the steam dumps and pressurizer heaters. Nevertheless, the base case plant response can be approximated by that illustrated by the three figures above. These figures, along with other figures presented below, are considered sufficient to generally describe the base case scenario.

Based on the above reference case from the FSAR analysis, knowledge of the emergency operating procedures (EOPs) (discussed later), expert judgment, and with no equipment faults or inappropriate operator actions, the following is presented as a summary of the "base case" and realistic plant response to a loss of main feedwater type of initiating event. This summary and the accompanying representations of the key parameter indications observable to the operators and shown in Figures B.6 through B.12 provide the expected "signature" of the event and what the operators are likely to expect and respond to as the scenario progresses, assuming there are no additional complexities (i.e., deviations).

- Initial Condition: The plant is operating at full power when a loss of normal feedwater occurs as a result of valve malfunctions, feedwater control anomalies, or similar faults. Indications or alarms of the loss of flow condition are the first cues to the operators.

- The rapid drop in steam generator levels and the steam-feed flow mismatch quickly cause a reactor trip.

- Sufficient low levels in the steam generators auto start all available auxiliary feedwater pumps if operators have not already manually started the system.

- Following plant trip until the plant is stabilized, the expected responses occur as highlighted by the following:

  (1) Reactor power decreases nominally following the reactor trip, as evidenced by the typical indications and power (flux) time history shown in Figure B.6.

  (2) The turbine trips and the generator load drops as evidenced by the typical indications and turbine pressure time history as shown in Figure B.7.

  (3) All electric buses (key support system) continue to operate (including required bus transfers) and appear normal based on breakers indicating "closed," available bus voltages and related indications that are nominal; and expected operating loads that are operating as evidenced by current, flow, and similar readings.

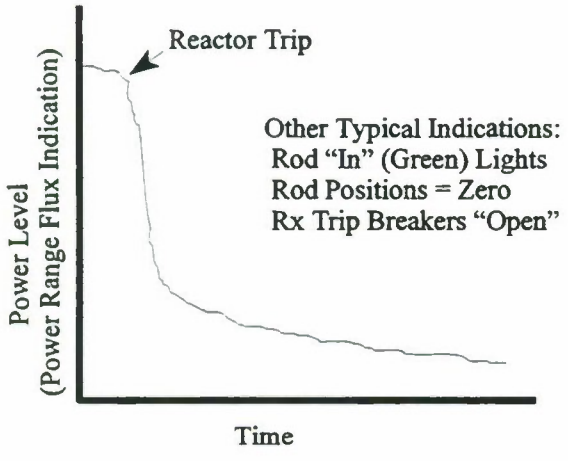


Figure B.6 Power Level vs. Time

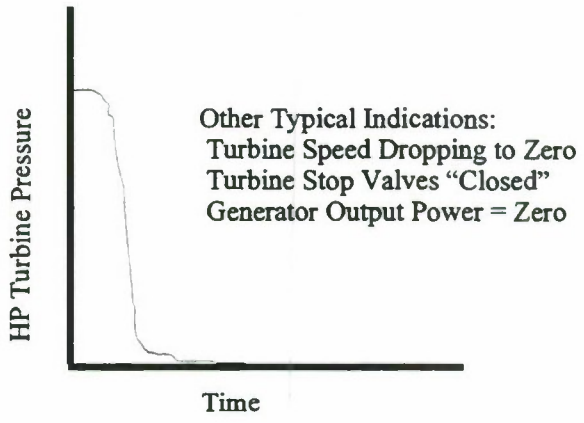


Figure B.7 Turbine Pressure vs. Time

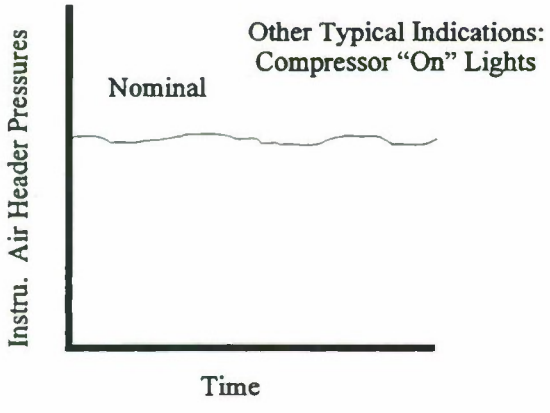


Figure B.8 Instrument Air Pressure vs. Time

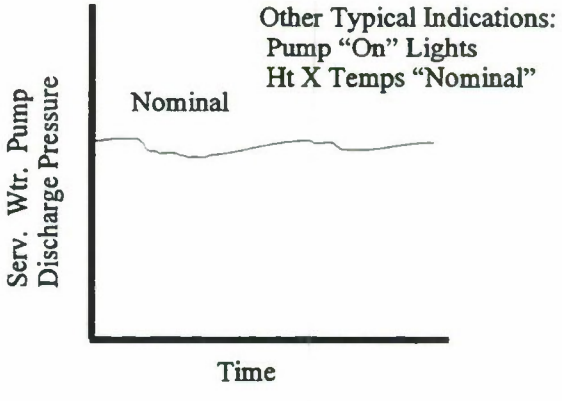


Figure B.9 Service Water Pressure vs. Time

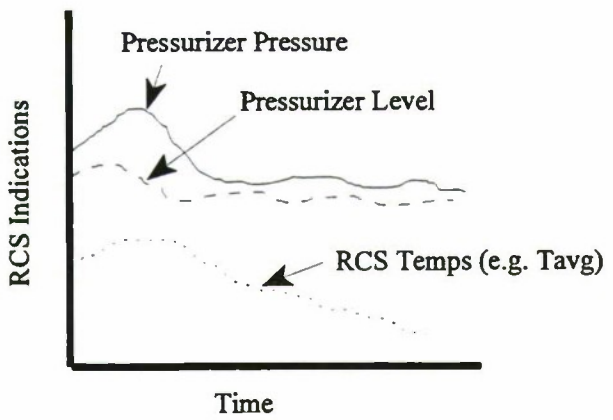


Figure B.10 RCS Conditions vs. Time

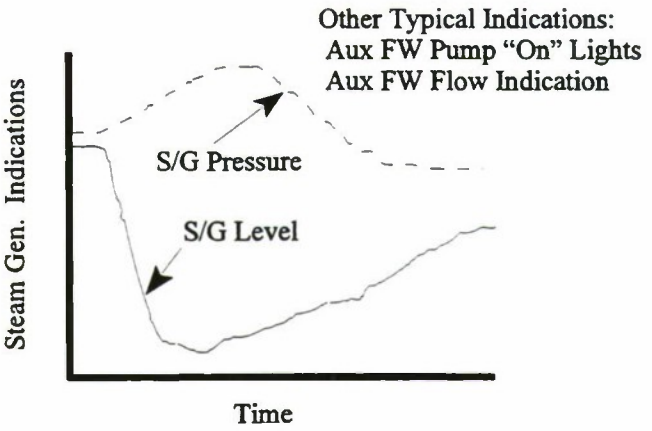


Figure B.11 Steam Generator Status vs. Time

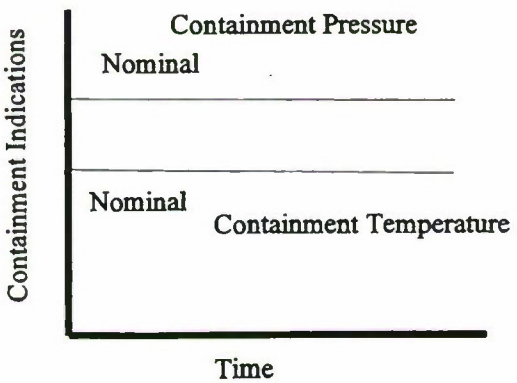


Figure B.12 Containment Conditions vs. Time

(4) Instrument air, a support system, is available, as evidenced by no change in header pressures over time as shown in Figure B.8 and appropriate compressor "on" lights.

(5) As another set of key support systems, component cooling water (CCW) and service water (SW) pump lights are "on," pump discharge pressures remain nominal over time as illustrated in Figure B.9, and service water load temperatures are nominal. Note that some momentary disturbances in the pressures and flow rate may be evident if some loads are isolated or other realignments occur. These disturbances are momentary.

(6) Key indications for the status of the RCS go through time history responses typical of that shown in Figure B.10. These are indicative of a rapid loss of heat sink (as feedwater is lost to the steam generators but is eventually recovered with auxiliary feedwater) along with the effects of reduced power (when the reactor trips) and normal operation of chemical volume control system (CVCS) charging or letdown and pressurizer heaters or sprays as they compensate for disturbances in RCS conditions. Neither pilot-operated relief valve or safety relief valve (PORV/SRV) demands occur nor is safety injection actuated in this event. Key indications such as pressurizer pressure, level, and RCS temperatures (T_{hot}, T_{cold}, T_{avg}...) rise as the RCS heats up and swells due to the degrading heat sink. Then they are restored and maintained within normal limits as the reactor power decreases, heat sink is eventually restored with auxiliary feedwater, and the charging or letdown and pressurizer spray or heater systems function normally. Pressurizer pressure does not reach PORV set points or drop to a safety injection limit. Similarly, pressurizer level does not reach high or "solid" condition or drop to that requiring safety injection. RCS temperatures do not reach extreme high or low levels requiring quick changes to reactor coolant pump (RCP) pump operation or other significant human actions.

(7) Steam generator levels drop dramatically at first due to the loss of feedwater, but with auto (or manual) start of auxiliary feedwater, levels soon show signs of restoring as shown in Figure B.11. Steam generator pressures rise at first as RCS heat continues to be dumped to the degrading steam generator, but with reactor trip and recovering steam generator levels, pressure is restored and ultimately controlled via the steam generator blowdown system. Main steam safety valves (MSSVs) are not actuated unless there is a corresponding and sudden main steam isolation. Auxiliary feedwater pump indications and valve alignment lights indicate flow into the steam generators. As the steam generator heat sinks are recovered, auxiliary feedwater is throttled down by the operator and if not needed, the turbine pump is shut down and placed in "pull-to-lock."

(8) Nominal containment conditions remain unchanged, as represented in Figure B.12.

(9) No radiation indicators or alarms are present.

(10) No other adverse indications or alarms such as ventilation problems are present.

- With no developing complexities (i.e., no "deviations" from the base case response to a loss of main feedwater event), an early focus by the operators is on recovering and then controlling steam generator pressures and levels within prescribed limits to restore and maintain proper heat sink. The turbine-driven auxiliary feedwater pump is shut down and put in pull-to-lock to avoid overcooling while flow from the other auxiliary feedwater pumps is throttled as necessary. Steam dump is performed to the condenser (most likely still available) or using, for instance, atmospheric dump valves to control steam generator pressure and eventual depressurization.

- Cooldown of the plant and shutdown of unnecessary equipment commences, achieving either a stable hot shutdown status or proceeding to cold shutdown if required.

Note that in the base case scenario, operator actions primarily involve: (a) verification of the above automatic equipment responses and that no additional failures of equipment have occurred via available indications, (b) controlling steam generator levels and pressures, including throttling of auxiliary feedwater flow so as to not overfill the steam generators, and (c) cooling down the plant and shutting down unnecessary equipment as required.

B.4 Step 4: Define Human Failure Events (HFEs) and Unsafe Actions (UAs)

Based on the issue as defined in Step 1, functional failure modes 2, 3, and 5 from Table 9.6 are the most relevant given the desired automatic recovery of secondary cooling via AFWS and the use of steam dumps and other equipment. From Table 9.7, corresponding HFEs associated with these functional failure modes involve equipment being inappropriately terminated, isolated, or controlled, as well as failing to be backed up upon automatic failure, among other similar examples. Based on these examples of HFEs, two general types of HFEs are defined here that are relevant to the issue as defined in Step 1. These are:

HFE 1: Operator actions that involve the inappropriate termination/isolation/realignment or at least severe reduction of secondary cooling via the steam generators because it is envisioned as the appropriate response (even though it is actually inappropriate). Of interest are those actions that lead to degradation of secondary cooling and hence additional challenges for the safe recovery from the loss of main feedwater event. Note that such actions could, for instance, involve a number of different specific UAs such as shutting down the AFWS pumps, severely throttling auxiliary feedwater flow via operation of the flow control valves, restricting steam generator pressure control and subsequent cooldown, or other specific unsafe actions that result in operator-caused insufficient secondary cooling. [An error of commission (EOC)].

HFE 2: Operator failure to back up the failed or lost function of secondary cooling (such as that due to multiple AFWS equipment failures) when backup or restoration is required. Other problems competing for operator attention could be, for instance, the cause for such inaction. Illustrative of this HFE is the unsafe action of not attempting to manually restart an AFWS train. [An error of omission (EOO)].

In a PRA context, either HFE, if it persists, is another way of causing AFWS failure in the sequences shown in Figure B.2, and could therefore result in the need for feed-and-bleed cooling or even challenge the scenario to the point of potentially causing core damage due to the loss of heat removal and the subsequent heatup of the RCS.

Another form of HFE that instead leads to overfill of the steam generators or some other form of overcooling could also be of interest. However, that HFE is not the subject of the issue as defined in Step 1; thus it is not included here.

B.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

This step is the first involving the identification of deviations from the base case scenario that may introduce contexts in which the relevant HFEs are potentially likely. Consideration of characteristics of the scenario, formal rules and procedures, informal rules, operator tendencies and biases, potential procedural difficulties, and potential timing and workload issues are among the factors involved in identifying such deviations. This step reviews potential vulnerabilities that may make the HFEs likely. As such, this step provides insights into the traits of the deviations that should be included in the next step which explicitly develops the possible scenario deviations.

B.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

Examination of Table 9.10, which addresses event types and related potential operator vulnerabilities, results in the following observations relevant to this analysis.

- The loss of main feedwater event fits a class of events that are anticipated several times during the life of the plant and for which operators at this plant are trained relatively frequently compared with other abnormal and accident events. As such, their training for such an event as well as a few actual plant transients of this type have provided an "expectation" as to what such a scenario "looks like" and the expected plant equipment and indicator responses.

- The base case scenario, i.e., without complications, has been included in training and actually been experienced in a real event by a few of the operators. Some complications have also been included in training, particularly those included in the FSAR, such as scenarios involving partial losses of auxiliary feedwater.

Based on the above observations, it should be the focus of the deviation analysis (which follows later in Step 6) to identify scenario complexities involving other (nontrained or infrequently trained) equipment failures, subtle dependent failures, or other reasons for unexpected abnormalities that make the event different from operators' conditioned expectations and might alter the operator response in a way that results in the HFEs of interest. A scenario(s) with such mismatches between operators' expectations and the actual events represents a vulnerability that may induce typically expected actions by the operators that may be wrong or at least "not ideal" for the actual situation.

B.5.2 Time Frames of Interest

As a further insight into the potential for the HFEs of interest to occur, four time periods of interest to the scenario can be identified relative to the potential for operator influence. These are summarized in Table B.2.

Table B.2 Relevant Time Frames for the Loss of MFW Scenario

Time Frame	Major Occurrences	Potential Operator Influence
Initiator	Loss of MFW Reactor scram or turbine trip T_{avg} drops upon reactor trip Pressurizer level drops with T_{avg}	The trip may be the first warning. If so, the operators have no chance to affect the initiator. If the problem develops slowly, operators may identify MFW problems and manually trip the plant.
0-2 minutes	AFWS starts automatically, when steam generator (SG) levels shrink to low-low level SG pressure is controlled per self-actuating blowdown Other auto equipment responses	Operators verify initial plant responses (particularly those that are automatic such as lowering power level, etc.) per EOPs; particularly AFWS starts in this case. Operators may even manually start AFWS before it auto starts.
2 min-1 hour	Heat sink restored (SG levels) Plant conditions restabilize Some throttling or shutting down of equipment (e.g., AFWS) begins	Operators are expected to throttle and then shutdown some AFW pumps to avoid overfilling the SGs; or respond to lack of cooling (and enter other EOPs) if heat sink apparently not restoring. They perform other actions as necessary (e.g., pressurizer heater on or off) to keep plant stabilized.
>1 hour	Unnecessary equipment shutdown Achieve stable hot or cold shutdown	Operator shuts down unnecessary equipment and transitions plant to hot/cold shutdown if desired

The above summary indicates that in the first few minutes expected operator actions involve verification of expected, and typically automatic plant responses. In order for the operators to not respond, for instance, to an initial degradation or failure of AFWS (an example of HFE 2), a significant diversion believed to be extremely important is likely to be required in order for the operators to not notice or otherwise not respond to a failure to restore secondary cooling. Much later in the scenario, throttling back and/or shut down of equipment associated with secondary cooling is "expected." Therefore, deviations of interest that might cause HFE 1 would most likely need to involve the appearance that the requirements for these expected actions have been met when in actuality, they have not. Hence, these types of vulnerabilities should be considered for examination later in Step 6.

B.5.3 Operator Tendencies and Informal Rules

Of the operator action tendencies summarized in Table 9.12a, the tendency of most interest to the issue as defined in Step 1 is that involving the operators' tendency to decrease plant cooldown. Such a tendency could lead to the cut back or shut down of secondary cooling which is the issue of concern as defined in Step 1. Based on a review of Table 9.12a and of the formal steps in the EOPs,

observable plant indications that would strengthen the tendency to want to decrease cooldown and hence represent a vulnerability of interest include:

- pressurizer pressure is continuing to decrease or is lower than expected
- too much core heat removal (i.e., higher or faster than expected) as evidenced, for instance, by falling RCS temperatures
- steam generator conditions suggest too much cooldown, as evidenced by higher or faster rising generator levels than expected, and/or by declining or too low steam generator pressures

In addition to the above plant indications that tend to induce the action of decreasing cooldown, operators are also cautioned and trained to avoid excessive cooldown and the potential for entering the pressurized thermal shock regime. This training, based in both formal and informal rules, further supports the conclusion that any appearances of too rapid a cooldown could be a vulnerability that might induce HFE 1 especially.

In addition, there are two informal rules that may be particularly relevant to the HFEs of interest. These are:

- Protect equipment. Operators are acutely sensitive to signs of equipment degradation (e.g., fluctuating pump current reading) and rapidly shutting down this equipment if it is not deemed to be necessary. This sensitivity came about due to a recent incident in which a degrading main feedwater pump was not shut down in time to prevent serious damage and resulted in a costly repair. Deviations of the base case scenario involving apparent equipment degradation may induce the HFEs of interest.
- Lack of detailed knowledge of the subtleties of the instrumentation and control (I&C) circuits and their potential vulnerabilities and effects. Deviations of the base case scenario involving subtle I&C failures associated with the key indications or equipment responses may contribute to the likelihood of the HFEs of interest.

B.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

This evaluation looks for vulnerabilities associated with ways the EOPs and other formal rules may lead operators to the HFEs of concern. The EOPs are the primary input to the operators' formal rules

for responding to a loss of main feedwater event. This examination is developed by tracking those portions of the plant's EOPs that are most germane to that type of scenario.

Figure B.13 (on two pages) displays in a simplified flowchart the portions of the EOPs most likely to be followed in the base case loss of main feedwater scenario as well as possible pathways to other EOPs if complications develop. Note that this simplified flowchart is not meant to duplicate the EOPs. However, it does show where (a) branch points from the most applicable procedure to other procedures, (b) where specific steps exist that call for stopping equipment that is particularly germane to the scenario, or (c) where a major reconfiguration of equipment is called out. Such places in the EOPs represent possible vulnerabilities where it may be more likely for the HFEs of interest to occur as a result of entering a wrong procedure, or where equipment might be shut down or reconfigured inappropriately. Where deemed beneficial, information is provided in Figure B.13 that summarizes the following:

- actions to be taken
- potential for ambiguity
- a judgment on the significance of taking the wrong branch or inappropriate action.

In addition to the information in Figure B.13, the EOPs also provide for continuous monitoring of "critical safety functions". EOP F-0.3 heat sink is most relevant to this scenario and requires monitoring of the following:

- feed flow rate (>200gpm?)
- SG levels (>4% in one or both SGs?; <67% in both SGs?)
- SG pressures (<1130 psig or <1070 psig in both SGs?)

Depending on the outcomes of these decisions, other function recovery procedures may need to be entered if additional complications occur during the scenario. These other procedures generally call for increasing or decreasing the heat sink capability. Note that too much cooldown while at high RCS pressure could cause entrance into the pressurized thermal shock regime, which the operators are trained to avoid. Too little cooldown could cause heat buildup in the RCS, along with further recovery complications or even core damage.

A review of the above portions of the EOPs for potential vulnerabilities that might lead to the HFEs of interest suggests the following observations:

- Any deviation scenario that contains the following characteristics is of interest:
  - too much cooldown during the scenario, which if false or otherwise interpreted inappropriately, could cause the operators to over-react and cut back feed flow or secondary cooling
  - too little cooldown during the scenario, which if not addressed in a timely manner due to resource diversions caused by other complexities, could cause further heatup in the RCS or even core damage.

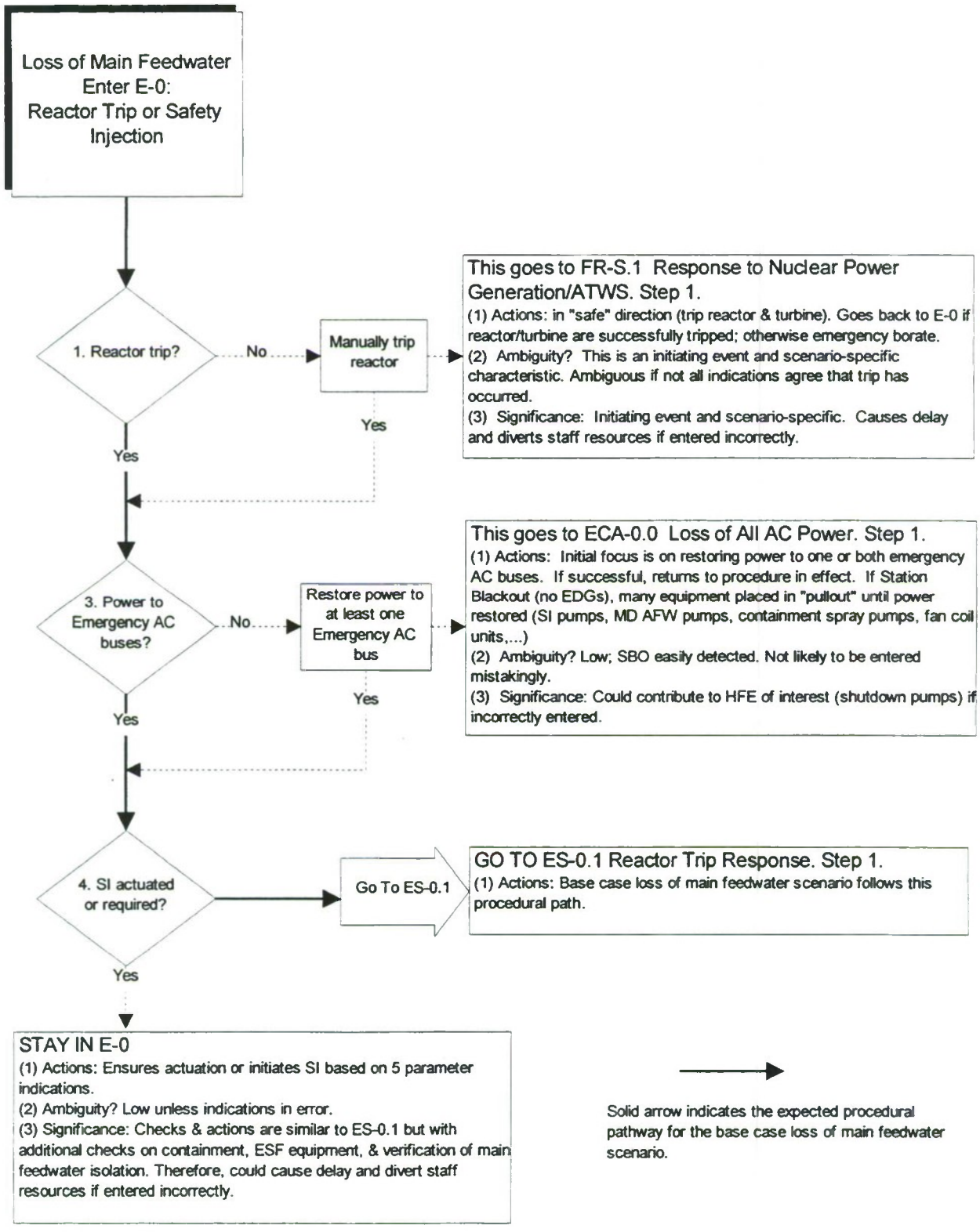


Figure B.13 EOP Highlights Related to Loss of Main Feed Scenario

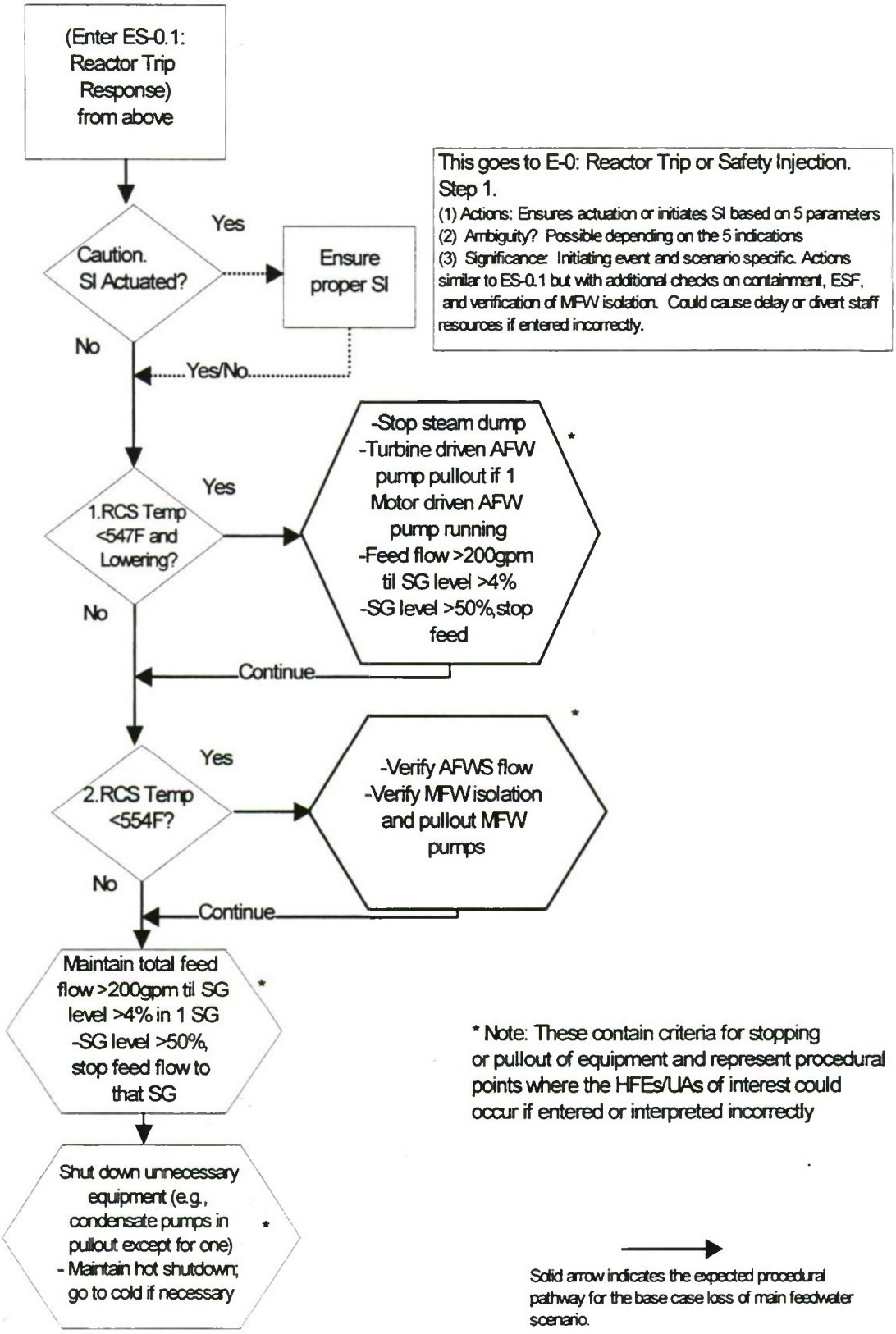


Figure B.13 EOP Highlights Related to Loss of Main Feed Scenario (continued)

- It does not appear that failure of reactor trip (actual or falsely indicated) would necessarily induce the HFEs of concern other than because it could compete for operator attention and hence resources. Most actions invoked by FR-S.1 would likely require operators to ensure even more secondary cooling, not less, because of the higher power levels involved if failure to scram were to occur. Other HFEs could certainly result because of operators attempting to deal with a much more complicated situation, but they are not the subject of this analysis. Only because of the possible competition for operator resources, will this form of complication to the base case scenario be further considered.

- If an actual or perceived blackout were to occur, actions involving "pullout" of equipment are called for, including motor-driven auxiliary feedwater pumps. Because of the possibility of inappropriately diagnosing a blackout or of failing to restore secondary cooling equipment following blackout recovery, further investigation of partial or total losses of electric power as a complicating factor in the scenario that might induce the HFEs of interest seems appropriate. This and other complicating failures of support systems may warrant further consideration.

- Safety injection, especially if falsely required, will likely add to cooldown of the plant and if deemed unnecessary, might induce actions to reduce the cooldown and possibly the HFEs of interest (especially HFE 1). Further investigation of this complication in the base case scenario seems warranted.

- Sufficiently low temperatures in the RCS and/or subsequent shutdown actions call for steam generator feed flow to be reduced and eventually stopped if sufficient generator levels are reached. False indications or similar complications might induce the HFEs of interest (especially HFE 1), and are worth further investigation.

This information is revisited during the deviation analysis in Step 6 to assist in determining the likelihood and significance of taking wrong branches or inappropriate actions because of the deviation.

B.5.5 Summary of Potential Vulnerabilities

The traits of possible deviations from the base case scenario (to be developed in the next step) that take advantage of the potential vulnerabilities and possible pitfalls identified in this step include the following:

- complexities involving other (nontrained or infrequently trained) equipment failures, subtle dependent failures, or other reasons for unexpected abnormalities

- indications of too much cooldown, as evidenced, for instance, by low pressurizer pressure, low RCS temperatures, high steam generator level, low generator pressures

- indications of equipment degradation that may provoke equipment shutdown

- complexities that seriously compete for operator attention and hence resources
- the possibility of a perceived blackout, other electric power anomalies, or other support system faults, particularly if they have subtle effects
- the possibility of a safety injection, especially if falsely indicated as required, that might induce actions to reduce the cooldown.

B.6 Step 6: Search for Deviations from the Base Case Scenario

In this step, ways in which the plant and operator response might deviate from the base case scenario are identified. Of interest are those deviations that may contribute to "error-forcing" situations such that the HFEs of concern become quite plausible.

The following is a series of searches for possible deviations and related contexts from the base case scenario that could induce the HFEs/UAs of interest as a result of the potential vulnerabilities identified in the previous step (Step 5).

B.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

The search for possible scenario deviations that make the HFEs/UAs more likely is begun by first considering deviations in the initiating event itself as well as in the scenario as a whole. In this case, a useful approach is to apply guide words typical of HAZOPs to investigate differences relative to the base case event involving loss of main feedwater. The base case loss of main feedwater is assumed to be an abrupt and total loss as the initiating event, followed by successful operation of all mitigating systems (safety and nonsafety). The following discussion documents possible types of deviations associated with the initiating event and the scenario progression.

Table B.3 shows the possible deviations that have been considered in this search. The types of initiator or scenario deviations that seem to have the most potential for inducing the HFEs/UAs of interest involve confusion as to the true status of the main feedwater system and whether it is sufficient to remove decay heat, as well as equipment malfunctions during the plant response.

Table B.4 summarizes more specifically how deviations carried forward from Table B.3 might "trigger" relevant cognitive processes, error mechanisms, and related error types based on a review of Tables 9.15a and b as well as 9.16a and b, in ways that might induce the HFEs/UAs of concern. For the possible physical deviations being considered, the contents of Tables 9.15a and b and 9.16a and b most relevant to the HFEs/UAs of interest are shown in the second column of Table B.4. The third column of Table B.4 summarizes the potential errors that could occur, considering the general error types provided in those tables. For the slower/partial/repeated type of initiator deviation, slower than expected parameter changes enhanced by the "belief" that the situation has become stabilized with main feed flow (potentially incorrect situation assessment) could make either HFE 1 or 2 more plausible (i.e., success is anticipated and so action to "disable" AFWS could be taken too soon). For instance, if a degradation of MFW is sufficient to cause a reactor trip on steam/feed

Table B.3 Loss of MFW Initiating Event: Scenario Deviation Considerations

Guide Word	Possible Physical Deviation	Significance	Carry Forward in the Analysis?
No/not/never	Initiator - N/A Scenario - multiple equipment failures	Relative to the initiator, "no" loss of main feed eliminates the initiator and so there is no event. Use of this guide word is not applicable. Relative to the scenario, these guide words are used to address "no" overall plant response (never) to the event (e.g., no RPS and no AFWS and...). Such a case is considered too improbable.	No.
More/early/ quicker/ shorter	Initiator - N/A Scenario - starting steam generator levels, response of automatic or nonsafety equipment differs from "expectations"	These constitute a quicker loss of main feed or subsequent plant response than assumed in the base case scenario. The base case scenario already assumes an abrupt and clearly discernible loss of main feed. Therefore, these guide words are not applicable to the initiator. The plant response might be somewhat quicker than operator "expectations" (such as that due to particularly high or low initial steam generator levels and/or equipment malfunctions). Possible specific considerations will be addressed in the second search regarding parameter responses and relevant rules.	Consider equipment malfunctions and related parameter indications during the scenario in the second search regarding relevant rules.
Less/slower/ longer/late/ partial/ repeated/as well as	Initiator - MFW is not totally and abruptly lost initially, but is only partially, slowly, or repeatedly lost over time or involves an additional complexity. Scenario - starting steam generator levels, response of automatic or nonsafety equipment differs from "expectations"	For the initiator, this is a possible situation that could add confusion as to the extent or nature of main feedwater loss or raise doubt as to whether it is lost. Such confusion might enhance the chance of disabling or otherwise cutting back auxiliary secondary cooling before the nature and extent of the main feed loss are completely understood so that appropriate actions are taken. The plant response could occur more slowly, involve additional equipment failures, or cause partial or even repeated responses so as to be different than operator "expectations" (such as that due to particularly high or low initial steam generator levels and/or equipment malfunctions). Possible specific considerations will be addressed in the second search regarding parameter responses and relevant rules.	Consider a less than abrupt and total loss of main feed initiator Consider equipment malfunctions and related parameter indications during the scenario in the second search regarding relevant rules.

Table B.3 Loss of MFW Initiating Event: Scenario Deviation Considerations (Cont.)

Guide Word	Possible Physical Deviation	Significance	Carry Forward in the Analysis?
Reversed	Initiator - Main feedwater is apparently restored but it is still not sufficient or is later lost again (repeated). Scenario - equipment malfunctions occur later that reverse the earlier plant response trends.	For the initiator, this is a possible situation that could add confusion as to the extent or nature of main feedwater recovery. Such confusion might enhance the chance of disabling or otherwise cutting back auxiliary secondary cooling before the nature and extent of the main feed recovery are completely understood so that appropriate actions are taken. The plant response could involve later equipment failures so that recovery trends reverse and the plant degrades again. Possible specific considerations will be addressed in the second search regarding parameter responses and relevant rules.	Consider a less than total recovery of main feed. Consider late equipment malfunctions and related parameter indications during the scenario in the second search regarding relevant rules.

Table B.4 Results of the Loss of Main Feed Initiating Event: Scenario Deviation Analysis

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Main feedwater is not totally and abruptly lost initially, but is only partially lost or is lost slowly or repeatedly over time.	No change in parameters or a smaller change than expected. [No indication or slower or smaller than expected changes in plant parameters (e.g., steam gen. levels dropping less than anticipated since partial main feed available)] Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. (Starts as partial loss of main feed but which could degrade and become more severe at some later time) Familiarity and simple expectations about the event need to be overcome if situation changes. (Situation could worsen over time, perhaps unexpectedly, requiring situation assessment and response change) Expectation bias (trained loss of MFW event) must be overcome because of dilemma. (With both MFW and AFWS potentially available, which to use as well as too little vs. too much cooldown represent possible tradeoffs or dilemmas as to the appropriate actions)	May take no action or delayed action to prevent further degradation of main feedwater. Not relevant to HFEs of interest. Could believe situation has stabilized (become static) with some MFW flow and thus assumed to not be very serious; so could disable or otherwise stop AFW too soon to avoid overfilling SGs or overcooling (as an overeager response to the dilemma/tradeoff between MFW and AFWS operation). Problem could later worsen if MFW subsequently and totally lost, requiring further detection and reestablishment of AFW, which could be missed if seriousness of new situation is not realized. Possibility of either HFE 1 or 2.	Yes. Should carry forward as a possible complication for the initiator due to the error mechanisms potentially "triggered" by such a physical deviation. Hence, this type of deviation should be considered in any deviation scenario of interest.
Main feedwater subsequently is partially recovered but is still not sufficient or is later lost again.	Familiarity and simple expectations about the event need to be overcome if situation changes or reverses. (Reversing parameter trends, requiring reassessment)	It may be difficult for operators to change their actions in response to changing MFW conditions. In particular, they could act too soon (overeagerness) to disable or stop AFW to avoid overfilling SGs or overcooling in the belief that MFW is sufficiently recovered. An example of HFE 1	Yes. Another example of a possible initiator complexity adding to an error-forcing context of potential interest in a deviation scenario.

Table B.4 Results of the Loss of Main Feed Initiating Event: Scenario Deviation Analysis (Cont.)

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Various equipment malfunctions that change the pace or sequence of events for the scenario	No change on a smaller change in parameters than expected. [No indication if slower/smaller than expected changes in plant parameters (e.g., steam gen. levels dropping less than anticipated)] Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. (Starts as partial loss of main feed but which degrade and become more severe at some later time) Familiarity and simple expectations about the event need to be overcome if situation changes. (Situation could worsen over time, perhaps unexpectedly, requiring situation assessment and response change) Expectation bias (trained loss of MFW event) must be overcome because of tradeoff or dilemma. (With both MFW and AFWS potentially available, which to use as well as too little vs. too much cooldown represent possible tradeoffs or dilemmas as to the appropriate actions)	Operators may take inappropriate action or correct action too soon (overeagerness) in response to changing scenario. Of particular interest is delayed action on none in response to degrading secondary cooling condition (HFE 2) or action of cutting back cooling too soon (HFE 1). Specific scenario and related parameter differences and potential operator actions will be examined in second search.	Yes. Specific possibilities will be addressed in subsequent search.

flow mismatch but some main feed flow still exists so that steam generator levels are not yet sufficiently low to cause AFWS initiation (low-low level), operators might be induced to think that sufficient feed flow is available to handle post-trip cooling and therefore be inclined to prevent or quickly cut back AFWS flow. If this action is performed in a way that would prevent subsequent auto-start of AFWS such as by pulling to lock the pumps, any further degradation or subsequent total loss of main feedwater (a later change requiring a change in the situation assessment) may not be addressed by manually restarting AFWS in a timely manner, especially if there are other unrelated distractions while responding to the event. For the second type of initiator deviation involving a partial restoration (reversal) of main feedwater flow, a similar effect may be possible in that it might be assumed that the main feed is restoring secondary cooling, potentially causing premature shut down of AFWS. As for deviations related to scenario changes caused by equipment malfunctions, this universal type of deviation will be examined more closely in subsequent searches, especially the second search. In that search, plant parameter changes and hence relevant rule responses will be reviewed to identify specific and particularly troublesome scenario deviations.

Hence, because of the potential to be contributing factors to contexts that could make HFE 1 or 2 more likely, (a) a partial or slowly degrading (but not total) loss of MFW, (b) an event involving a partial but still insufficient recovery of MFW, and (c) an event involving malfunction complexities are all carried forward as a potential part of any deviation from the base case scenario that might induce either HFE 1 or 2.

B.6.2 Search of Relevant Rules

This portion of the analysis examines whether the HFEs/UAs of interest could be induced as a result of deviations from the base case scenario so that incorrect "rules" (provided primarily by the EOPs and other informal rules) are followed, or the EOP decision and action statements can be applied in ways that would cause the HFEs.

Figure B.13 and the related text presented: (a) the expected EOPs that would be entered in the base case scenario, (b) key decision points in those EOPs, and (c) a discussion of the most relevant critical safety function EOP, F-0.3, related to heat sink conditions. In stepping through the various EOPs shown in Figure B.13, EOP F-0.3, and subsequent EOPs that might be entered if further complications developed in the scenario, nothing was found that would directly cause the HFEs/UAs of interest simply by following the EOPs. Still, the following discussion summarizes the conditions in all these EOPs that would result in shutting down (at least temporarily or partially) secondary cooling:

- Generally, secondary cooling via flow to the SGs is to be maintained until the narrow range level in the SGs is at least 4%, at which point throttling back can occur, attempting to control level in the 4%-50% range.

- If SG narrow range level gets too high (>67%), isolate AFW flow to the affected SG.

- If SG pressure gets too high (>1130 psig) and cannot be decreased, isolate AFW flow to the affected SG.

- If an SG is determined to be faulted, as indicated by SG pressure decreasing in an uncontrolled manner or an SG is completely depressurized, it is isolated (note that at least one SG is suppose to be maintained for cooldown).

- If a station blackout is determined to be in progress, the motor-driven AFWS pumps are placed in "pullout" until power is restored.

- Whenever steam dumping is not warranted and the motor-driven AFWS pumps are running, the turbine-driven AFWS pump is shut down and placed in pullout, especially when the RCS temperature is less than 547°F.

- Main feedwater is also isolated under the above and other related conditions.

Besides the above "formal rules," one of the informal rule vulnerabilities mentioned in Step 5 is:

- Protect equipment. Operators are acutely sensitive to signs of equipment degradation (e.g., fluctuating pump current reading) and rapidly shutting down this equipment if it is not deemed to be necessary. Hence apparent equipment problems could further enhance the desire to not use or otherwise shut down secondary cooling equipment.

Based on the above summary, in order for either of the HFEs of concern to occur when following the EOPs or the above informal rule, one or a combination of the following must occur:

- SG levels are indicating higher than they really are or the operators perceive them as doing so.

- SG pressures are indicating higher than they really are or the operators perceive them as so.

- SG pressures are indicating lower or decreasing faster than they really are or the operators perceive them as doing so.

- Operators believe a station blackout is in progress and the turbine-driven AFW pump is also inadvertently shut down.

- The turbine-driven AFW pump is inadvertently shut down even when the motor pumps are not running.

- Trouble with secondary cooling equipment occurs, or is perceived as such, and operators shut down equipment that is actually needed.

Each of these conditions is examined in Table B.5. The potential error mechanisms affecting human response and subsequent error types come from review of the error mechanisms and related error types in Tables 9.15a and b and 9.16a and b (just as was done for the entries in Table B.4).

Table B.5 Results of Relevant Rule Deviation Analysis

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
SG levels are indicating higher than they really are or the operators perceive them as doing so	Uncontrolled blowdown (e.g., MSSVs stuck-open) temporarily indicates high level	Familiarity and simple expectations about the event need to be overcome if situation changes. There is a change from the "expected" yet it can be explained by expectation that levels should rise. Overeagerness to respond in an inappropriate way may be possible.	If operator does not detect actual failure and wait for re-stabilized (sustained) condition, could inappropriately cut back feed flow based on eagerness to respond to temporary high levels	Yes.
	Multiple SG level indicators in error	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly high SG level conditions.	Could inappropriately cut back feed flow (overeagerness) based on erroneous but anticipated level indications.	Yes, but only if operator focuses on a few indications or a common-cause failure occurs. Otherwise, too many failures have to occur.
SG pressures are indicating higher than they really are or the operators perceive them as doing so	Multiple SG pressure indicators in error	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly high SG pressure conditions.	Could inappropriately cut back feed flow (overeagerness) based on erroneous pressure indications.	Yes, but only if operator focuses on a few indications or a common-cause failure occurs. Otherwise, too many failures have to occur.

Table B.5 Results of Relevant Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
SG pressures are indicating lower or decreasing faster than they really are or the operators perceive them as so	Temporary blowdown system malfunction or uncontrolled blowdown (MSSV stuck open then recloses)	Familiarity and simple expectations about the event need to be overcome if situation changes. Unexpected but large or fast change in parameter may cause preoccupation with this parameter (tunnel vision) and eagerness to respond	If operator does not detect actual failure and wait for re-stabilized (sustained) condition, could inappropriately cut back feed flow based on eagerness to respond to temporary low or decreasing pressure	Yes.
	Multiple SG pressure indicators in error	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly low SG pressure conditions.	Could inappropriately cut back feed flow (overeagerness) based on erroneous pressure indications.	Yes, but only if operator focuses on few indications or a common-cause failure occurs. Otherwise, too many failures have to occur.
Operators believe a station blackout (SBO) is in progress and the turbine-driven AFW pump is also inad-vertently shut down	Numerous false indications of SBO	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly SBO conditions	Seems it would also require a slip to shut down turbine AFW.	No. Seems unlikely to misdiagnose SBO and make slip as well.
The turbine-driven AFW pump is in-advertently shut down even when the motor pumps are not running	Erroneous indications of motor pump operation	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" a response to shutdown turbine.	Seems it would also require a slip to shut down turbine AFW	No. Seems it would require multiple indication failures and maybe even require distractions–improbable.

Table B.5 Results of Relevant Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Equipment trouble induces shutdown by operator	Indication of equipment trouble	Training bias; informal rule, protect equipment. "Double bind"– maintain cooling vs. shutting off equipment	May take inappropriate action to shut down needed cooling equipment.	Yes

Based on the Table B.5 summary, it appears that the operators could inappropriately shut down or otherwise prevent proper secondary cooling and thus render HFE 1 or 2, primarily if (a) a temporary condition arises that indicates it is appropriate to throttle back or shut down secondary cooling flow and the operators do not wait for conditions to restabilize, (b) multiple indication failures for at least one parameter (e.g., level) exist, (c) a significant distraction due to other complications occurs and operators anticipate or otherwise misread parameter indications, (d) evidence of equipment trouble occurs, which if false or not critical could possibly induce inappropriate shutdown of the equipment, or (e) a combination of these. Note that in the case of erroneous indications, additional factors related to operators tending to focus on a single parameter (due to training or other crew tendencies) will likely be part of the context. These possible deviations are carried forward in the analysis to be considered in any context that might induce either HFE 1 or 2.

B.6.3 Search for Support System Dependencies

A review of the support system dependencies from the PRA for the plant revealed that a number of support system faults during the event could add to the complexity of the scenario and thus potentially contribute to any error-forcing context. Of all the support system faults that might occur coincident with a loss of main feedwater event (involving equipment cooling; heating, ventilation, and cooling; instrument air; electric power), loss of power is of most interest since it has the potential to contribute to the cause of the initiator, fail some of the responding equipment, potentially cause erroneous indications, and add to the complexity associated with the scenario, all at the same time.

In considering the ways an electrical power disruption might occur, two broad categories are addressed. The first is a plant-wide disruption, exemplified by a loss of offsite power. The second is a loss of only one or two buses, thereby affecting only portions of the plant systems and/or indications. Each of these conditions is examined in Table B.6. The potential error mechanisms affecting human response and possible error types come from review of Tables 9.15a and b and 9.16a and b.

A plant-wide electric power loss is likely to be easily detected (for instance, control room lights go out) and is one that operators are trained on from time to time. Such a deviation is probably more "unexpected" if it is delayed and happens later during the response to an event. When a widespread loss of power happens, interruption of operating equipment also occurs. Depending on diesel starts or subsequent power recovery, the crew looks for restarting of important mitigating equipment or attempts to manually start equipment. If the loss of power is delayed and occurs some time after the occurrence of the initiating event, it may be even more "unexpected" than if it occurred as part of the initiating event. Furthermore, if emergency diesel power also all fails, then only the turbine-driven AFWS pump train can operate until at least limited power is restored. Per the EAC-0.0 procedure in the case of station blackout, much mitigating equipment is placed in "pullout," which could delay or even prevent a mitigating equipment response once power is restored, depending on the crew's response (or lack thereof, which could be unsafe acts) to reactivate the equipment. Even if diesel power is established, operators could miss or at least be delayed in ensuring that sufficient equipment has reactivated and proper recovery of plant conditions is occurring. In addition, further complications occur such as loss of pressurizer heater and spray control. A particularly important unsafe act could be the failure to ensure proper restoration of AFWS equipment following the power loss.

Table B.6 Results of the System Dependency Deviation Analysis

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Widespread loss of electrical power	Loss of offsite power to the plant	Complacency and expectations about the event need to be overcome if situation changes. Focused attention or obsession on power loss and diesel start or power recovery (tunnel vision) may be possible. If loss occurs later in scenario, must respond to late change in situation.	May draw attention away from ensuring proper actions concerning restoration of AFWS	No. Next condition seems more problematic.
Partial loss of electrical power (e.g., instrument buses that serve SG level indications)	Instrument bus fault	Complacency could lead to missing the fault if indications of fault can be subtle or non-compelling. Fixation or focused attention or obsession on power loss (if detected) and power recovery may occur. Plant-unique feature of some SG levels failing to midscale will further the likelihood to cut back AFWS.	Lack of awareness of subtle failure or unrecognized effect on indications could lead to incorrect assessment of secondary cooling status or failure to recognize serious situation. May also draw attention away from ensuring proper restoration of AFWS	Yes, because as the fault indication is subtle and "triggers" a unique plant failure of some SG level indicators to midscale (could be particularly troublesome).

The second class of deviation addressed in Table B.6 could be more subtle, harder to detect, and therefore represent an even greater challenging context. This is the loss or degradation of one or two electrical buses, either as part of the initiator or as a delayed event some time after the initial response of the plant. Detection could be harder or at least delayed because the loss is not widespread and may be at a level within the electrical network that is not specifically alarmed or indicated (i.e., covered only by a general alarm). While such a "partial loss" of electrical power in the plant would seemingly not cause the crew to follow EAC-0.0, the operator tendencies are similar (attempt to recover the power if detected) and the plant response is more complicated because of the need to detect and respond to the effects of such partial losses of electrical power.

Depending on the specific buses lost, some indications could also be affected, further complicating the ability of the crew to understand the status of the plant. For instance, at this plant, failure of a particular set of instrument buses has been found to lead some steam generator level indicators to fail to midscale, a situation that could be particularly troublesome in ensuring proper heat sink conditions. This plant-unique finding along with the operators' tendency to focus on the steam generator level as a key indication of the status of secondary cooling (discussed in the previous step), together could provide an interesting element of an error-forcing context should any of the instrument buses fail.

In both cases, the tendency to attempt to recover power is not necessarily unsafe as long as it does not divert attention too much from the overall plant status and restoration is not attempted while an electrical fault still exists. Should the latter situation be the case, attempts to restore power could cause repeated failures to restore equipment or even expand the effect of the lost bus by tripping other buses when power recovery is attempted.

Table B.6 and the related discussion suggest that a loss or degradation of main feedwater coupled with a loss of power could provide a form of deviation from the base case scenario that could hamper the plant and crew response. If such a failure could either (a) actually cause a temporary rapid cooldown of the plant or (b) even worse, cause the appearance (falsely) of a rapid cooldown of the plant, there appears to exist the possibility of the crew cutting back too soon or even stopping AFWS flow if RCS temperatures appear to drop below that indicated in ES-0.1 and/or if SG levels appear to rise to too high a level (as caused by the midscale reading). There appear to be potential opportunities to throttle or even place much of the AFWS in "pullout," thinking that too much cooling is occurring (the potential unsafe act). If such steps were to be taken inappropriately, SG conditions could once again become degraded, requiring the operator to restore AFWS. Failure to do so in a timely manner (a potential unsafe act) could cause heatup of the RCS and even core damage if the condition persists.

Therefore it is suggested that a particularly challenging deviation associated with electrical power, and having the following characteristics, appears worth further review in subsequent steps in the ATHEANA process:

- a delayed failure of an instrument electrical bus in the plant

- the selected bus fault should disrupt cooldown control (if possible to further complicate the cooldown issue), and cause the affected SG level indicators to fail to midscale (in addition, one or two SG level indicators could also be removed from service, such as for calibration, as part of the total context)

- to further ensure the appearance of too rapid a cooldown, an actual but subtle and temporary cause for cooldown may also need to be part of the context, such as a leaking pressurizer spray valve

- the bus failure is such that a fault condition continues to exist, thereby hampering its restoration and becoming a further diversion of resources and attention

The above combined conditions could have the following characteristics:

(1) Indication of too rapid a cooldown (to further strengthen the tendency to decrease cooldown) as evidenced by decreasing (more than expected) pressurizer pressure, level, and RCS temperature indications. (This could be caused by a leaking pressurizer spray valve, for instance.)

(2) A rise in "some" of the steam generator level indicators (to midscale) caused by electrical bus failure. (This could falsely indicate that sufficient steam generator levels have been reached to allow cutback/shutdown of secondary cooling.)

(3) Together these indications may compel the operator to perform HFE 1.

A coincident bus failure could similarly be a contributing factor to HFE 2 to the extent that if it contributed to the appearance of a rapid cooldown while in fact there was a partial or total loss of secondary cooling due to equipment faults, actions might not be taken (or at least be significantly delayed) to restore the lost function. In such a case, the context would have the same characteristics as listed above but with the additional actual failure of secondary cooling as part of the scenario.

B.6.4 Search for Operator Tendencies and Error Types

This portion of the search process for possible deviations of the base case scenario is approached by keying on categories of deviations that may make the HFEs of concern more plausible based on certain human behavioral tendencies. From the information provided on general tendencies in Table 9.12a, it is evident that one of the operator tendencies is of particular interest to this analysis. It involves the scenario appearing to have the indications of overcooling so that the operator behavioral tendency for decreasing core cooling is intensified. Table B.7 summarizes information regarding this operator tendency, which has already been somewhat addressed in the previous searches.

Relative to HFE 1, the formal steps in the various EOPs that call for throttling back and eventually shutting down secondary cooling flow were addressed in a prior search. Hence any deviation that

Table B.7 Summary of Deviations Involving Operator Tendencies

Condition	Human Behavioral Tendency	Significance	Further Analysis?
Indication of overcooling (real or falsely indicated)	Slow down or stop overcooling	If inappropriately diagnosed, might induce action illustrative of HFE 1	Yes.

might cause HFE 1 must: (a) falsely indicate these required conditions have been met, (b) make an actual cooldown appear sufficiently threatening that in spite of the above requirements the operators incorrectly reduce or shut down secondary cooling, or (c) a combination of these characteristics.

Other supporting evidence might include evidence of falling pressurizer and steam generator pressures, significant subcooling readings, shrinking pressurizer level, etc. This is illustrated in Figures B.14a and b where multiple parameters indicate levels other than that normally expected in the base case loss of main feed scenario. The more evidence there is of a rapid cooldown, the more likely the operators will believe that this is the case and the stronger will be their tendency to stop the cooldown.

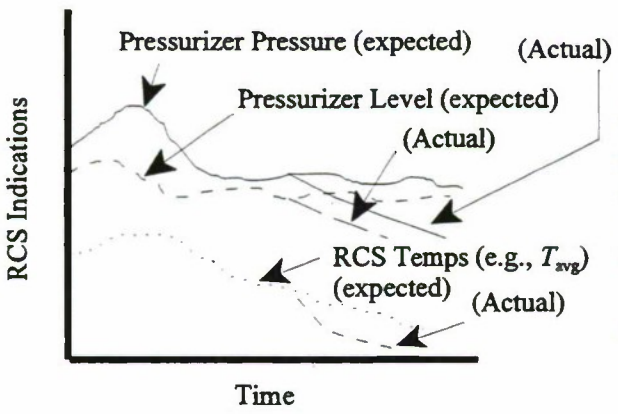


Figure B.14a RCS Response vs. Time

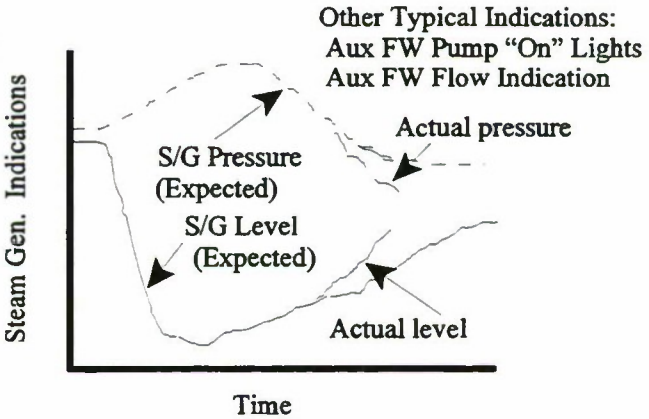


Figure B.14b SG Response vs. Time

As for an actual cooldown situation, such a deviation from the base case scenario must not be sufficient to ensure continued and adequate cooling of the core over the long term, or only be temporary. Further reenforcement of the need to cut back secondary cooling might exist if at least some of the steam generator indications falsely indicate that the requirements for throttling or shutting down feed flow have also been met. There are many ways that a cooldown may initially become greater than desired or anticipated, though not sustained. As for hardware faults associated

with the RCS, possible excessive cooldown might initially be caused by such failures as a demanded and stuck open PORV, a faulty operating pressurizer spray (e.g., stuck-open or leaking spray valve), an RCS leak or break, or a loss of pressurizer heater function, among others. Faults in the secondary plant with a similar effect might involve too rapid an initial steam generator blowdown such as that due to malfunction of the blowdown control system or a demanded and stuck-open main steam safety relief valve. Initial heat loss such as through a PORV, RCS leak, or malfunction in the secondary plant, or the addition of a cooling effect such as the pressurizer spray malfunction, could initially indicate that excessive cooldown is in progress.

In such cases, the operators' first priority is to search for the reason for the cooldown and if they find it, attempt to isolate or otherwise recover from the cause of the cooldown. It seems unlikely such a cooldown by itself would induce HFE 1 unless the source of the cooldown could not be identified. Hence, a subtle source of the cooldown would be more likely to contribute to an error-forcing context than an easily detected cause. If there was the added difficulty of at least some false steam generator indications, the context might be even more convincing.

In addition to the above, Tables 9.15a and b and 9.16a and b were reviewed for additional complicating factors (e.g., possible impasses, "red herrings") or error mechanisms (e.g., apathy) and related error types that might be "triggered" by possible scenario deviations that would induce human response tendencies similar to the HFEs of interest. No deviations other than those already addressed by this and the previous searches have been identified at this time.

In summary then, it would seem that the operator tendency to over-react to a seemingly rapid cooldown event and thus cause HFE 1 would need to involve:

- multiple indications of failures so that a rapid cooldown is falsely inferred, particularly if operators are also preoccupied with the one or two false parameters (especially steam generator level), or
- an actual but nonsufficient or temporary cooldown to which the operators respond inappropriately by not waiting long enough for conditions to stabilize, or
- a combination of the above conditions

B.6.5 Summary Description of Deviation Scenarios

The above searches have all contributed to the identification of the characteristics of a number of contexts that could make HFE 1 or 2 more plausible in a scenario involving an initial loss or degradation of main feedwater flow during normal plant operation. Based on these searches and the recognition that certain characteristics were repeatedly identified, it can be stated that the plausibility of the HFEs depends on deviation scenarios containing the following major elements to create a relevant error-forcing context:

- for HFE 1, there is a conflict over whether overcooling or undercooling is occurring so that overcooling appears to be the greater concern

- for HFE 2, a significant diversion occurs so that a delayed loss of secondary cooling is not addressed in a timely manner

- for both HFEs, malfunctions occur is key indications as to the degree of cooling (e.g., steam generator levels) so that both HFEs are more likely

In deviation scenarios with the above contexts, the likelihood of the HFEs would be much higher than normally expected. The most relevant error mechanisms and error types potentially "triggered" by such contexts are summarized in Table B.8, based on information developed in the prior searches. For instance, the conflict of over- vs. undercooling concerns brought about by the EOPs, other procedures, and related operator tendencies (supported by training) potentially "triggers" a fixation on this concern and the desire to avoid overcooling nearly as much as undercooling. Operator training, the EOPs, and the heat sink functional recovery procedure produce a significant reliance on indication of the steam generator level, thereby potentially setting up tunnel vision with regard to this specific parameter and when to throttle or cut back secondary cooling. The desire to avoid overfilling the steam generators, thereby contributing to an overcooling transient, also potentially "triggers" an eagerness to throttle back secondary cooling once this function appears satisfied.

In addition, a number of specific occurrences that could cause the plant conditions in Table B.8 were identified during the ATHEANA searches. For example, the plant conditions identified could occur through the following chain of events:

Deviation Scenario 1; Example chain of events

Pre-initiator: Plant operating nominally at full power. At least one (or more) steam generator level indicator among the Division A indicators is being tested and calibrated. (This lessens the redundancy of steam generator level indications relied on by the crew for secondary cooling status and thus contributes to the overall context.)

Initiator: A degrading main feedwater flow event such as that caused by controller malfunction, regulatory valve failure, or some other similar situation occurs that does not immediately or completely cause the loss of all main feed. It is, however, sufficient to cause dropping steam generator levels and a steam-flow mismatch such that an auto reactor trip will occur. (This could cause some early confusion as to the availability of main feed and create some doubt as to the need for AFWS because of overcooling concerns.)

Early failures: Because the initial rise in RCS temperature and pressure will occur as the heat sink (steam generators) degrades, the pressurizer spray valve is expected to operate. In the deviation scenario, the spray valve "leaks" even though it is indicating "closed." (This becomes a source of hard-to-detect cooldown, thereby adding to the overall context and concern about overcooling.)

Table B.8 Deviation Scenarios

HFE	Overall Plant Condition	Most Applicable Error Mechanisms of Concern	Applicable Error Types	Comments
1	A scenario in which there is uncertainty about whether under- or overcooling is occurring Key indicator (e.g., steam generator levels) as to the degree of cooling suffers a fault so that it adds to the uncertainty by indicating sufficient cooling.	Sets up a "tradeoff dilemma" as to what to do when both MFW and AFWS seem available, causing a fixation on a possible overcooling event. Tunnel vision or a focus on steam generator level indicators on the basis of training and procedure biases. With normal expectation to throttle AFWS in loss of MFW events, potential eagerness exists about shutting down AFWS, especially if it appears SG levels have been adequately satisfied.	All of the identified applicable error mechanisms can contribute to inappropriate actions, taking correct actions too soon, or failing to take (or delaying) needed actions.	The overall plant condition and the error mechanisms potentially "triggered" by the condition could all support the possibility that the operators will perform an unsafe act indicative of HFE 1 (degrade or shut off secondary cooling) because they are concerned about overcooling and some faulty steam generator level indicators (some indicating midscale) make it appear that the shutoff conditions for secondary cooling have been met.
2	A scenario involving an initial degradation of MFW followed by partial success of AFWS A significant diversion occurs as part of the scenario, along with the key indicator problem A "late" failure of the remainder of all feed occurs	Sets up a "tradeoff dilemma" as to what to do when both MFW and AFWS seem available, causing a fixation on a possible overcooling event. Tunnel vision or a focus on the significant diversion. Potential complacency once the scenario has progressed to the point that the operators believe core cooling concerns are satisfied.	All of the identified applicable error mechanisms can contribute to inappropriate actions, taking correct actions too soon, or failing (or delaying) needed actions.	With an added uncertainty as to whether AFWS is really needed initially, such a plant condition with a significant diversion could lead to a delay or failure to restore AFWS following a "late" failure of all feed after the operators believe core cooling concerns are satisfied (especially with the added complexity of a faulty SG level indicator).

Early success: All other plant response is as "expected," with no failures. This includes complete response of AFWS.

Delayed failures: All other "normal" actions occur, but before both steam generator narrow range indications reach 4%, a delayed and complete failure of main feed (if it is still partially functioning) occurs coincident with a fault on an electrical bus that serves the steam generator Division B indicators. (This provides a common-cause effect that will cause the affected indicators to fail to mid-scale, potentially causing the true status of steam generator levels to appear to have reached adequate levels to throttle back or shut down all feed.)

The above chain of events making up the deviation scenario for HFE 1 develops a context that is expected to increase the likelihood of an unsafe action representative of HFE 1 in which steam generator cooling is cut back too soon. The scenario raises the possibility of the crew becoming overly concerned with the apparent and potentially increasing cooldown rate (caused by the leaking spray valve, which they may or may not detect, and the possibility of continued or rapidly recovered main feed) so that secondary cooling is throttled back (via various means such as throttling or shutting down AFWS pumps or cutting back the steam dump) *before* the proper criteria have been met (unsafe acts illustrative of HFE 1). The likelihood is further increased by the inaccurate SG levels caused by both the unavailability of some indicators due to test and calibration as well as the instrument bus loss.

There are certainly other specific ways to create a deviation scenario that will have effects similar to the one described above. They all, however, should provide a context of confusion as to the status of main feed, provide an actual or apparent increase in the "expected" cooldown rate, and take advantage of the crew's tendency to rely on indicators of steam generator level. What is being postulated is a form of scenario that makes the plant status indicators respond much like that depicted in Figures B.14 a and b relative to "expectations." It is believed that this type of deviation scenario increases the likelihood of operators cutting back or even shutting down secondary cooling (via various means) *before* the proper conditions have been met and are stabilized.

Deviation Scenario 2; Example chain of events

Pre-initiator: Plant operating nominally at full power. At least one (or more) indicator of steam generator level among the Division A indicators is being tested and calibrated. (This lessens the redundancy in steam generator level indicators relied on by the crew for secondary cooling status.)

Initiator: A degrading main feedwater flow event such as that caused by controller malfunction, regulatory valve failure, or some other similar situation that does not immediately or completely cause loss of all main feed. It is, however, sufficient to cause a drop in steam generator levels and a steam-flow mismatch so that an auto reactor trip will occur. A few minutes following the trip, the main feed fails totally if it has not already been isolated. (This could cause some early confusion as to the availability of the main feed.)

Early failures: One of the two AFWS motor pumps fails on demand (nonrecoverable).

Early success: All other plant response is as "expected," with no failures.

Delayed failures: All other "normal" actions occur up to and including the expected shutdown and pull-to-lock of the turbine-driven AFWS pump, leaving one motor pump operating. Before the motor pump, is also shut off, a fire or failure occurs in an instrument bus (with a fire alarm) that will cause failure of some of the redundant Division B indicators of steam generator level. (This will be a potentially significant diversion as well as cause the affected indicators to go to midscale, thereby inaccurately indicating the status of the SG levels, just as in the scenario for HFE 1.) A few minutes later, with no warning, the running AFWS train fails, possibly with a noncompelling signal indicating failure of the injection path.

The above chain of events making up the deviation scenario for HFE 2 develops a context that is expected to increase the likelihood of an unsafe action representative of HFE 2 in which steam generator cooling is not restored or is restored too late following its "late" loss. The example scenario adds a potentially significant diversion regarding the fire that occurs as part of the instrument bus fault. The likelihood of not adequately responding to the late loss of all secondary cooling may be increased by the inaccurate SG levels caused by both the unavailability of some indicators due to test and calibration as well as the instrument bus loss and the diversion of attention to the fire.

There are certainly other specific ways to create a scenario that will have effects similar to the one described above. They all, however, should provide a context of a significant diversion (in this case the fire), a delayed failure of all secondary cooling once parameters seem to reach nearly recovered conditions, and take advantage of the crew's tendency to rely on indicators of steam generator level. It is believed that this type of deviation scenario increases the likelihood of operators not responding to the total loss of secondary cooling since it happens unexpectedly "late" in the event and in the context of a competing diversion.

B.7 Step 7: Identify and Evaluate "Complicating Factors" and Links to Performance Shaping Factors (PSFs)

The deviation scenarios, as described above, already include a number of the types of additional complicating factors discussed for this step in Section 9. These include:

- degraded equipment operation, such as the initial degraded MFW condition
- instrumentation unavailabilities and anomalies (for steam generator levels) adding potential confusion about the plant's status

- the crew's tendency to rely on steam generator level as a single key indication of secondary cooling status as a result of existing training and procedure biases that focus on these levels as an indication of heat sink adequacy

- other hardware failures potentially causing diversions of the crew's attention and resources (particularly the bus fault in the first scenario and the bus fire in the second scenario), thereby adding to the workload and attention load of the crew. This could strain communication among crew members and add to the likelihood of the HFEs

One additional PSF that is being "triggered" in the described scenarios is the potential unawareness of the specific effects of the bus fault. Since it is expected that most crew members would not realize that the steam generator level indicators have been affected, this could lead the crew to believe that the levels are indeed adequate and it is time to shut down secondary cooling.

All of these complicating factors are considered to be already present by virtue of the deviation scenarios as they have been defined, and hence the factors support the likelihood that the HFEs might be committed in such circumstances.

B.8 Step 8: Evaluate the Potential for Recovery

Even if the scenarios and subsequent human failure events occur as postulated in the previous steps, there is a chance that the operators will recover from the degrading plant conditions before serious damage results. The possibilities for recovery include restoration of secondary cooling before dryout of the steam generators, or the restoration of feed in time to ensure sufficient core cooling. If neither is performed, core damage could occur, initiating in about 1 hour following the loss of secondary cooling.

For the postulated scenarios, and assuming the HFEs occur, the plant conditions will deteriorate since secondary cooling is not available to remove heat from the reactor coolant system. Various cues of this deteriorating condition should eventually become available. These are indicated by the simplified plots in Figure B.15 and the anticipated scenario progression log in Table B.9.

As summarized in the scenario progression log, the key to a rapid recovery of the degrading condition is the crew's assessment that the SG levels are in fact falling from an already "low" condition and that many of the SG level indicators are actually malfunctioning. Actions that could increase the likelihood of diagnosing the actual SG level conditions include placing the tested channel indicators back into service, identifying the effects of the faulted bus on the SG level indicators, or otherwise conservatively responding to any confusion about the true status of the SGs. If a diagnosis of the actual lowering of SG levels not made (which is still likely because of the original belief that SG levels are adequate, which contributed to the HFEs in the first place), other parameters indicating the condition of the RCS will appear "nearly normal" for a time until the RCS begins to heat up again. Once it does, the potential for operator recovery is spurred by the desire to

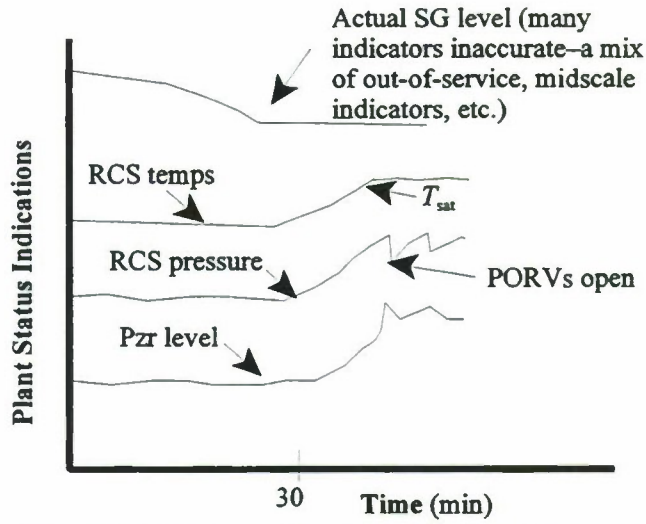


Figure B.15 Plant Status after HFE Occurs

find the reason(s) for the unexpected RCS conditions. During this time, the functional recovery procedures largely call for adjusting charging or letdown flow and similar actions. However, if the severely degraded SG level condition is still not diagnosed, RCS conditions will worsen. Once the SGs are dry, recovery is further hampered since any restoration of secondary feed is limited by an allowable flow rate at first, as a result of the dry SG conditions, and sufficient primary system cooling is difficult to obtain once the secondary heat sink is unavailable.

In summary, recovery from the original HFEs is possible if the actual degrading SG condition is diagnosed early in spite of out-of-service or otherwise malfunctioning indicators of SG level. However, the subtle failure of these indicators may make such a diagnosis difficult. Without such a diagnosis, RCS conditions are likely to get quite bad before sufficient evidence exists (in the form of an RCS void indicator and/or core thermocouple readings) for the crew to recover. By that time, recovery will be hampered by the "lateness" of the attempted recovery due to uncooperative thermal hydraulics.

B.9 Quantification Considerations

While much has been learned from the above analysis about the potential for the HFEs of interest to occur and the types of deviation scenarios that may increase the likelihood of the HFEs, it may be desirable to obtain a quantitative approximation as to the overall likelihood of such an occurrence.

In Section 10 it is seen that such an assessment requires estimating the frequency of the error-forcing context (made up of the frequency of the plant condition occurring × the probability of relevant PSFs), the probability the crew will perform the unsafe act(s) illustrative of the HFE, and the probability that the crew will not recover from their original mistake by the time serious damage to the plant occurs. Each of these is discussed and estimated below.

Table B.9 Scenario Progression Log Regarding Possible Recovery from HFEs

Approx. Timing after HFE Occurs	Symptom	Actions
0–30 minutes	Few (if any) steam generator level indicators show the actual lowering of SG levels as a result of no feed. Some indicators are being calibrated and tested and others show midscale readings from the failed bus.	Depending on the degree of confusion by operators' as to SG levels, they may (or may not) rush getting the SG indicators in test back into service and/or figure out the anomalies caused by the faulted instrument bus. If such actions are not taken, the crew may not immediately conclude that levels are dropping.
0–30 minutes	Other parameters are following "near normal" expectations (see Figure B.15) since it will take time for the steam generators to enough dry to cause re-heatup of the RCS. So for a while, there is little indication of the degrading situation.	Parameters remain within expected limits and thus no significant actions may be taken if the actual lowering of SG levels is missed.
30–60+ minutes	Parameters show the signs illustrated in Figure B.15 as the RCS heats up. RCS high-pressure, temperature, and pressurizer high-level alarms occur as RCS volume heats up and expands. PORVs eventually lift and quench tank alarms sound as well. If as the situation further degrades, reactor vessel level instrumentation system (RVLIS) void indication and core thermocouple readings will eventually indicate a very serious situation.	While actions will likely be taken to address the RCS condition problems, these will most likely involve checks or adjustments of charging or letdown flow. No significant core cooling restoration actions will be called upon by the functional recovery procedures until the RVLIS void fraction and eventual core exit thermocouples indicate a serious situation (if actual falling SG levels are not properly diagnosed). The RVLIS and thermocouple indications will likely occur well after the SGs are dry and primary cooling should have been established. Recovery at this late stage could be difficult.

B.9.1 Deviation Scenarios Challenging HFE 1

Frequency of Error-Forcing Context
The plant condition postulated to set up HFE 1 involves four elements that need to be quantified:

(1) frequency of a degraded MFW condition that causes the plant trip and eventually progresses to a total loss condition

(2) probability of an additional, small cooldown source, such as the suggested "leaking" spray valve

(3) probability that some SG level indicators are unavailable (e.g., as due to testing)

(4) probability that several SG level indicators fail but their failure is not readily apparent (e.g., the postulated drop to midscale caused by a bus loss

The frequency of the degrading MFW initiator condition is estimated using the current PRA information for the plant. The PRA documents the frequency of an initiating event with MFW available as approximately 2-year and the frequency of a transient involving a total loss of MFW as about 0.14 a year. Considering the in-between nature of the postulated deviation scenario involving a degrading and eventual total loss of MFW, it is assumed that such an event has a likelihood somewhere between the two PRA extremes and nearer the total loss frequency. Hence a value of 0.5 a year will be used to estimate the frequency of the postulated initiating event.

The probability of a small source of additional cooldown can be estimated from a couple of viewpoints. First, the probability of a leaking spray valve as postulated in the deviation scenario can be estimated from typical PRA data values for valves failing to close, which are around 3E-3 per demand. Considering the potential for a couple of demands of the spray valve, and recognizing that there are other potential sources of cooldown (e.g., letdown problems, pressurizer heater problems), an estimate in the E-2 range or greater seems reasonable. In addition, actual experience at this plant demonstrates overcooling concerns in about 1 out of 10 trips. Together, these viewpoints suggest a probability of 1E-1 as a reasonable estimate.

Most SG level instrumentation checks do not take long and only occasionally require recalibration during power operation. Plant experience indicates a probability that some of the SG channel readings will be unavailable at the time of the event as about 1E-3.

The probability of a loss of multiple SG level indicators so that their malfunction is not obvious (e.g., due to the postulated bus fault) can be estimated on the basis of typical inverter, bus, and similar equipment failure probabilities which from the plant PRA are as high as nearly 1E-4 per hour. Given that the failure must coincidentally occur probably during the first half-hour of the accident response, but that there are multiple equipment failures that could cause the same "bus loss" effect, a probability of 5E-4 is assigned.

The probability of many of the SG level indicators being simultaneously unavailable or faulted can be approximated by the above 1E-3×5E-4, or 5E-7. However, there may be other common cause failures not yet accounted for, such as lightning strikes, that may also cause multiple SG level indicators in both divisions to malfunction. To capture this additional possibility, a 1E-6 probability will be used to estimate the likelihood that multiple SG level indicators in both divisions are malfunctioning or otherwise misindicating.

Collectively, the above values multiplied together provide an approximation of the frequency of the postulated plant condition of about 5E-8 a year [0.5/year × 0.1 × 1E-6]. This is considered to not be a very likely scenario in light of other accident frequencies in the PRA, but not so small as to be insignificant either.

The probability that the relevant PSFs exist and are "triggered" by the plant conditions makes up the remainder of the overall frequency of the error-forcing context. As discussed in Step 7, it is believed that the training and procedure biases do provide a strong tendency towards "tunnel vision" on the SG level indicators for heat sink status. In addition, the crew would have to not recognize or otherwise not identify the potential bus fault effects at the time of the event. The PSFs are considered to be "triggered" as a result of the plant conditions and so the probability of the PSFs is assigned "1.0." Hence, the frequency of the error-forcing context is estimated at 5E-8 a year.

Probability of Unsafe Act(s) Illustrative of HFE 1

Given the plant conditions and PSFs above, it is the analysts' opinion that a very strong context exists for cutting back or shutting down secondary cooling in the belief that it has been adequately satisfied when it actually has not. As discussed earlier, the plant condition and PSFs will invoke the error mechanisms shown in Table B.8 that collectively all support the tendency to cut back cooldown. In spite of this strong context, however, performing the HFE is not judged to be "assured." Therefore, a 50-50 probability is assigned to this part of the quantification.

Probability of Nonrecovery

Section B.8 contains a discussion as to the recovery potential and notes that the greatest chance of success is judged to be associated with the recognition that the SG levels are indeed lower than originally believed by the crew. This could come about, for example, by restoring unavailable SG level indicators, restoring the bus (or other) fault causing the other SG level malfunctions, recalling the potential bus–indicator interactions, or other means. Since the other plant parameters will not provide early evidence of severe plant conditions, these are not likely to provide clues regarding the true heat sink condition.

Given the event, there could be some desire to reactivate SG level channels that are in test and to restore the failed bus or similar fault. Whether such actions would be done in time to recover from the original HFE depends on the ability to restore the equipment in a short time, and the extent of the personnel resources at the time, which could be a function of the time of day, etc. Even if the true SG level conditions are not diagnosed, the later symptoms of degrading plant status do prevent a late (but probably difficult) chance of recovery.

Considering all the above, it is difficult to derive a substantial basis for a nonrecovery probability since it depends on numerous factors, all of which are difficult to estimate as to their likelihood beforehand. Judgmentally, however, it seems hard to justify a nonrecovery probability lower than 10%-50% range, considering the strong tendency before and after the HFE to focus attention on SG levels (which may or may not be restored) and the lack of early cues from other plant parameters.

Frequency of the Entire Event Leading to Core Damage
Multiplying all of the above values together yields an overall frequency of such an event resulting in core damage, including the HFE and nonrecovery, in the E-9 per year range.

B.9.2 Deviation Scenarios Challenging HFE 2

Frequency of Error-Forcing Context
The plant condition postulated to set-up HFE 2 requires a combination of the initiating event, an eventual total loss of AFW (via a combination of failures and shutting down the turbine train), and the concurrent SG level anomalies that sufficiently challenge the operators so that they may not recognize and therefore recover the lost secondary cooling function. This involves five elements that need to be quantified:

(1) frequency of a degraded MFW condition that causes the plant trip and eventually progresses to a total loss condition

(2) probability that some SG level indicators are unavailable (e.g., due to testing)

(3) probability that one AFW train fails or is otherwise unavailable

(4) probability that several SG level indicators fail but that their failure is not readily apparent (e.g., the postulated failure to midscale caused by the bus loss) coincident with a strong distraction such as a fire (alarm)

(5) probability that the remaining motor AFW train fails "late" in the scenario after the turbine pump has been shut down and placed in pull-to-lock; at this point, all secondary cooling would be lost and the operator will need to restart the turbine AFW train or provide some other core cooling

The likelihoods of items 1, 2, and 4 are provided above with the exception that the coincident fire or other serious diversion has not yet been accounted for as part of item 4. Serious diversions could take the form of a significant fire, a coincident pipe breach that causes steam and/or flooding concerns, etc. Considering, for instance, nearly 20 years of nuclear plant experience with approximately 40 fires during that time and a similar estimated number of serious flooding or pipe breach events over the same period, coupled with a current average of approximately 100–200 plant trips per year for the U.S. industry, results in a rough estimate of about one serious diversion event per 50 plant trips or about one per plant lifetime. Hence a 1/50 multiplicative factor needs to be added to the combined likelihood of items 1, 2, and 4. This results in 0.5 per year × 1E-6 × 1/50 = 1E-8 per year.

The probability of the first AFW train failing early or being unavailable can be estimated from current PRA values and is assessed to be about 5% or 5E-2.

The probability of the second AFW train failing to continue to operate can be similarly estimated and, taking into account potential common-cause failure mechanisms between the two trains, is assessed to provide another 5E-2 factor.

Collectively, the above values multiplied together provide an approximation of the frequency of the postulated plant condition of less than 1E-10 per year [1E-8 per year × 5E-2 × 5E-2]. This is considered to be a very unlikely scenario in light of other accident frequencies in the PRA, and probably not worth further consideration.

Frequency of the Entire Event Leading to Core Damage
Considering the above estimate, and even if PSF, HFE, and nonrecovery are now assumed to have probabilities of 1.0 in light of this combination of events, which includes both SG level indicator problems and a distracting event, the expected frequency of such a chain of events proceeding to core damage is assessed as very low since the plant condition has a very low frequency of occurrence.

This observation does suggest the following additional questions: "What if the plant condition involved the loss of all secondary cooling as postulated above, with a serious coincident diversion,

but the SG level indicators were not malfunctioning or otherwise unavailable? Would this be sufficient to divert attention from the lost function and cause the operators to not recover AFW?

In considering the above change in the chain of events, it should first be recognized that the search process carried out in Step 6 did not suggest that such a scenario would be sufficiently error forcing to cause HFE 2 (i.e., the focus on monitoring SG level would still require the anomalies in these indicators). Further thought simply does not suggest a diversion that is so compelling or threatening that the operators would not monitor the status of the secondary heat sink (a critical safety function) and therefore not notice it had been lost. With the SG level indicators properly tracking the falling SG levels, it is difficult to imagine the operators not restarting the turbine-driven AFW train to recover the lost function. Hence such a chain of events is not judged to be error forcing and therefore is not important.

B.10 Issue Resolution

This illustrative example of the ATHEANA prospective analysis process indicates that while the issue of concern is not among the dominant risk contributors in the plant's PRA, some concern is warranted about conditions that could lead the operating crew to inappropriately cut back or shut down secondary cooling to avoid apparent overcooling concerns. The estimated frequency of such an event progressing to core damage is not so small as to be insignificant. On the other hand, the

likelihood that the operating crew will miss the total loss of secondary cooling because of a serious attention diversion in the plant and thus fail to respond is too small to be considered further.

As for the potential error of commission involving inappropriate cut back or shut down of secondary cooling, a number of "lessons learned" are available which, if enacted, should considerably decrease the chance of such an event. These include:

- discussions with the operating staff as to the results of this analysis and the potential contexts of concern
- training improvements to remove the focus (tunnel vision) on steam generator level indicators as the nearly sole source of heat sink information
- additional procedures and training on the appropriate actions to take when it appears that both MFW and AFW are providing initial feed to the steam generators, thereby creating the tradeoff dilemma raised in this analysis
- fixing the instrument bus–SG level indication interactions so as to avoid the midscale failure mode
- adding simulator exercises to specifically address the concerns raised in this analysis as part of the operating crews' future training

APPENDIX C
ATHEANA EXAMPLE -
LARGE LOSS OF COOLANT ACCIDENT (LLOCA);
A "DIRECT INITIATOR SCENARIO"

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that could seriously degrade plant response to a fast-acting direct initiating event. More specifically, it is an illustration of the use of ATHEANA to identify and quantify those conditions (error-forcing contexts) that may induce unsafe acts by humans. In particular, this example addresses the question: Can physical characteristics associated with the progression of a large loss-of-coolant accident (LLOCA) in a pressurized water reactor (PWR) adversely affect the human operators in ways that have the potential to transform a design basis accident (DBA) into a core damage accident?

This is a plant-specific example, as all fruitful examinations of context must be. However, the plant analyzed is a composite PWR, not exactly matching any particular operating plant. The example is realistic in that all specific design, procedures, training, and operating and maintenance practice information used have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate similar issues in their plants. The illustration follows the steps discussed in the ATHEANA process in Section 9 of this document.

C.1 Step 1: Define and Interpret the Issue

This ATHEANA example analysis is performed to determine if physical characteristics associated with the progression of a LLOCA initiator can adversely affect the human operators in ways that have the potential to transform a DBA into a core damage accident. The plant PRA identifies the functional failures that lead to core damage.

C.2 Step 2: Define the Scope of the Analysis

In this case, the event type, a LLOCA, is defined by the issue. Characteristics of the LLOCA that are challenging include rapid blowdown, which can lead to uncovery and melting of the core if safety injection or recirculation cooling are interrupted for even a short time. Because of the narrow scope of the issue and the characteristics of the LLOCA, little additional focus on setting priorities should be necessary. However, the question of narrowing the scope must be revisited after identification of the base case LLOCA, the associated human failure events (HFEs), and the search for deviation scenarios.

C.3 Step 3: Describe the Base Case Scenario

The ideal base case, as described in Step 3 of Section 9 and illustrated in the first row of Table C.1, corresponds with a consensus operator model (COM) of the event; i.e., a mental model of the event that operators have developed through training and experience, and that is consistently understood by most operators. Furthermore, it is well defined in both an operational and an engineering sense (thorough neutronics and thermal-hydraulics analysis support the scenario). Finally, it is well documented and realistic. Note that Table C.1 also previews the results of the LLOCA base case development that will be presented in the following paragraphs. For the LLOCA, the base case is very near the ideal case. It will be used as the stepping off point for the deviation analysis. Because the COM is a result of required training based on the DBA, the COM will not be presented separately, but is discussed during the description of the reference case and the base case.

Table C.1 Characteristics of the Base Case Scenario

Type of Base Case	Consensus Operator Model	Well Defined Operationally	Reference Analysis		Realistic
			Well-Defined Physics	Well Documented	
Ideal	Exists	Yes	Matches COM	Yes, public information	Yes
LLOCA base case	Yes; the DBA is well known	Yes; annual training scenario	FSAR DBA closely matches the COM, but the analysis ends after stabilization, but before the long-term scenario is complete	Yes; FSAR	Reasonably realistic; the reference analysis is modified to account for more rapid use of water and long-term issues

C.3.1 The Reference Case LLOCA Scenario

The reference case LLOCA scenario is given in the plant Final Safety Analysis Report (FSAR) Chapter 14 Safety Analysis, Section 14.3.2 Major Reactor Coolant System (RCS) Pipe Ruptures (Loss-of-Coolant Accident), pages 14.3-7 to 14.3-12 plus associated figures and tables in Section 14.3.2.

The LLOCA is a Condition IV limiting fault ("faults which are not expected to take place, but are...the most drastic occurrences which must be designed against...[and] are not to cause a fission product release to the environment resulting in an undue risk to public health and safety in excess of guideline values of 10 CFR 100."). As specified by 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Power Reactors," the FSAR analysis is conservative in many of its details,[1] but the predicted time progression of the major plant parameters is a reasonable representation of the progression of the event. A number of more realistic analyses exist,[2] but are not available in the open literature. Therefore the FSAR case has been selected to define the "reference" case for the analysis.

[1]Conservatisms include break size and location, maximum allowable deviation (drift and error) in actuation setpoints, delay in actuation of safety injection, minimum allowable volumes, minimum heat transfer, maximum initial power, maximum fission product inventory, minimum fuel or clad temperature limits, etc.

[2]Other analyses include the backup document for the Westinghouse Emergency Response Guidelines and various proprietary WCAP thermal-hydraulic reports.

The FSAR analysis assumes a double-ended guillotine rupture of the largest RCS pipe. The FSAR describes the expected sequence of events as follows:

> *Should a major break occur, depressurization of the Reactor Coolant System results in a pressure decrease in the pressurizer. Reactor trip signal occurs when the pressurizer low-pressure trip setpoint is reached. A Safety Injection System signal is actuated when the appropriate setpoint is reached. These countermeasures will limit the consequences of the accident in two ways:*
>
> 1. *Reactor trip and borated water injection complement void formation in causing rapid reduction of power to residual level corresponding to fission product decay heat.*
>
> 2. *Injection of borated water provides heat transfer from core and prevents excessive clad temperatures.*
>
> *At the beginning of the blowdown phase, the entire Reactor Coolant System contains subcooled liquid which transfers heat from the core by forced convection with some fully developed nucleate boiling. After the break develops, the time to departure from nucleate boiling is calculated, consistent with Appendix K of 10 CFR 50 (Reference 1). Thereafter, the core heat transfer is unstable, with both nucleate boiling and film boiling occurring. As the core becomes uncovered, both turbulent and laminar forced convection and radiation are considered as core heat transfer mechanisms.*
>
> *When the Reactor Coolant System pressure falls below 700 psia, the accumulators begin to inject borated water. The conservative assumption is made that accumulator water injected bypasses the core and goes out through the break until the termination of bypass. This conservatism is again consistent with Appendix K of 10 CFR 50.*

The results of the FSAR analysis are shown in Figures C.1 through C.9, where the following points are clearly presented:

- Figure C.1. Power drops almost instantly to about 10%, then decreases more gradually.
- Figure C.2. Break flow (not directly measured and not available to the operators) drops quickly for the first 4 seconds, then more slowly until it bottoms out at about 20 seconds.
- Figure C.3. Core pressure drops smoothly to match containment pressure in about 20 seconds.
- Figure C.4. The containment pressure peaks at less than 20 seconds, as core pressure and break flow approach zero.

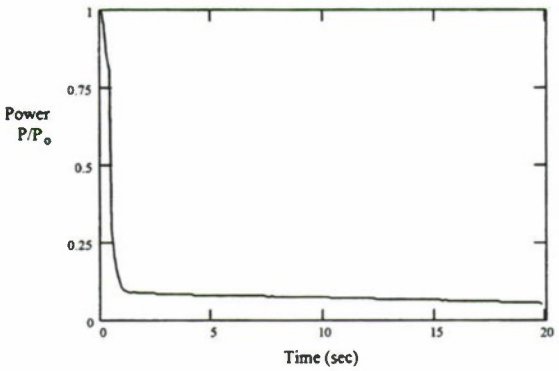


Figure C.1 Core Power during LLOCA Reference Case

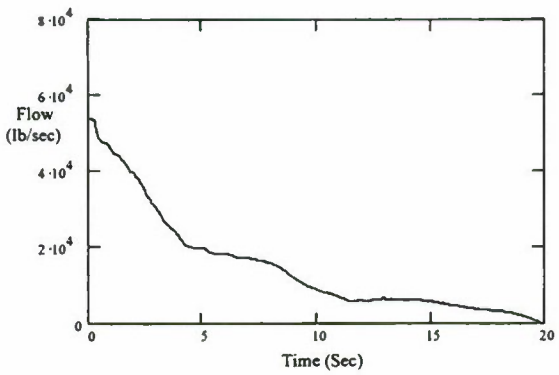


Figure C.2 Break Flow Rate during LLOCA Reference Case

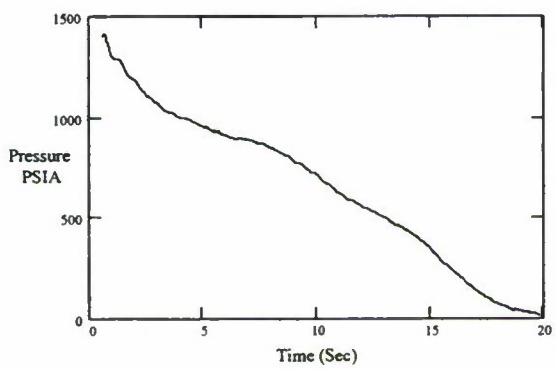


Figure C.3 Core Pressure during LLOCA Reference Case

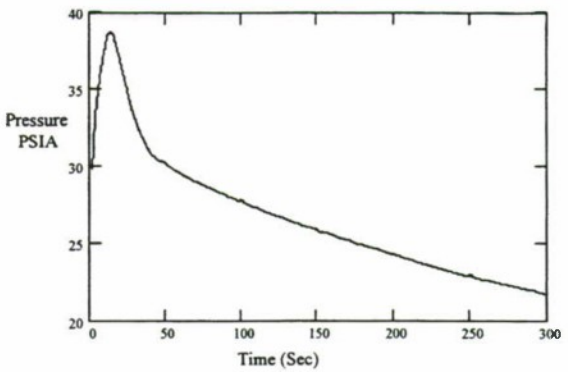


Figure C.4 Containment Pressure during LLOCA Reference Case

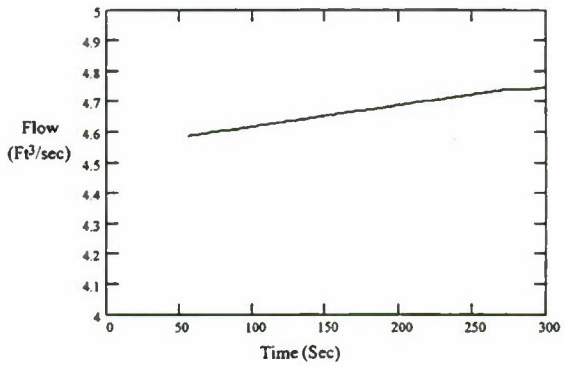


Figure C.5 Safety Injection Flow during LLOCA Reference Case

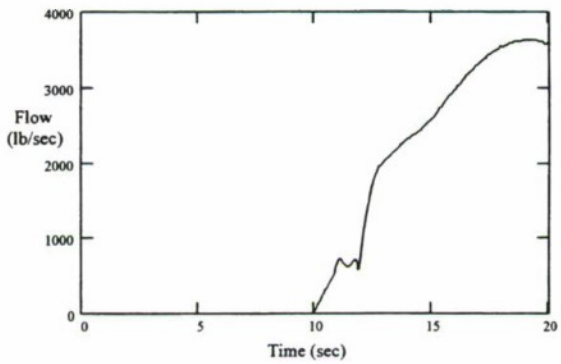


Figure C.6 Accumulator Flow (Blowdown) during LLOCA Reference Case

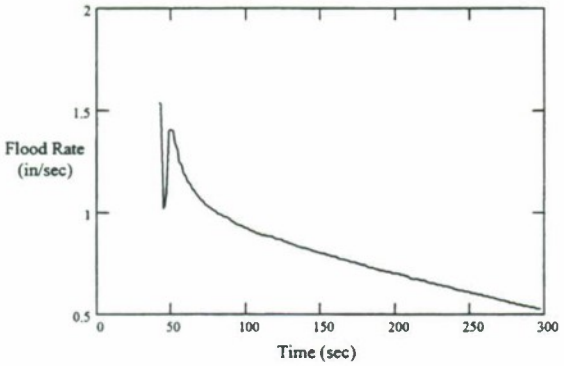


Figure C.7 Reflood Rate during LLOCA Reference Case

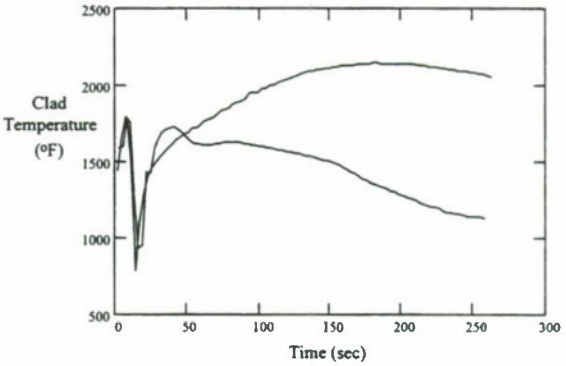


Figure C.9 Peak and Average Clad Temperature during LLOCA Reference Case

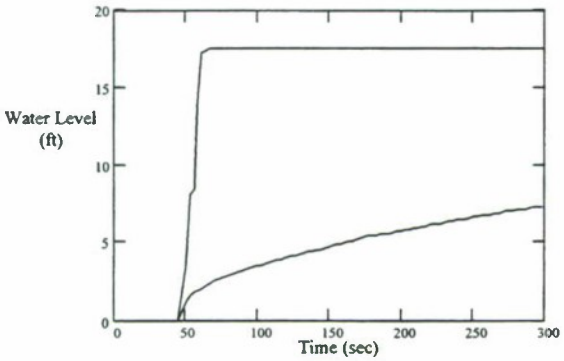


Figure C.8 Reflood Transient Water Level during LLOCA Reference Case

- Figure C.5. Emergency core cooling system (ECCS) flow is credited from about 30 seconds and remains about constant.[3]
- Figure C.6. The accumulators dump into the RCS beginning at 10 seconds and flow peaks at about 19 seconds.
- Figure C.7. Core reflood rate (not directly instrumented) starts at its maximum, when ECCS is assumed to start at 30 seconds. After an initial transient, it decays slowly.

[3]High-pressure ECCS flow would begin almost immediately, while low-pressure flow (about 80% of total flow) would begin as core pressure falls below the shutoff head of the pumps and would reach full flow before 20 seconds.

- Figure C.8. The core is reflooded to 5 feet at about 3 minutes. The reactor vessel downcomer refloods early on. Note that downcomer level is not instrumented and core level [reactor vessel level instrumentation system (RVLIS)] is not calibrated during LLOCA conditions.

- Figure C.9. By about 3 minutes, the most severe effects on the core have peaked, with no core damage.

The key parameters observable to the operators are summarized in Figure C.10. This composite trajectory of the parameters over time constitutes a signature or pattern for the LLOCA, confirmed in reading the FSAR and training materials, and, in the simulator, where the DBA is standard fare.

The reference scenario ends when the core is reflooded and immediate danger to the core is over; i.e., at about 3 minutes. Long-term stability is assumed, as are the operator actions necessary to ensure that stability.

C.3.2 Description of the Base Case LLOCA Scenario

The base case scenario is equivalent to the reference scenario for the LLOCA over the first 3 minutes for several reasons:

- Conservatisms (beyond the initiator itself) in the FSAR analysis of the LLOCA have only minor impact on the sequence of events and parameter changes that occur.

- The view of LLOCA held by operators is guided by their training, which includes the DBA, the double-ended guillotine rupture of the largest RCS pipe of the reference case:

  - operators undergo simulator training on the DBA routinely
  - essentially all operators would define a LLOCA in terms similar to the reference case, i.e., the COM matches the reference case

- Significant variations in the LLOCA, such as break size and location, are not familiar to most operators, except a trained-in belief that the DBA "envelopes" all smaller LOCAs.

The base case scenario, however, extends well beyond the reference scenario in time. The parameters in Figures C.1 through C.9 would return to stable conditions; power continues its gradual decline, core pressure remains essentially flat and equal to containment pressure, break flow (not directly measured and not available to the operators) remains flat at the spill rate and matches injection flow, containment pressure remains flat at near-atmospheric pressure, ECCS flow remains about constant until manual switchover to recirculation cooling at about 20 minutes, accumulator flow continues to fall for several more seconds and becomes zero when accumulator pressure equilibrates with RCS pressure, and core reflood rate (not directly instrumented) continues to decay slowly, reaching zero when the core is completely reflooded. Peak and average clad temperature continue to decrease, approaching the RCS temperature.

Key points in the base case scenario not present in the reference scenario are:

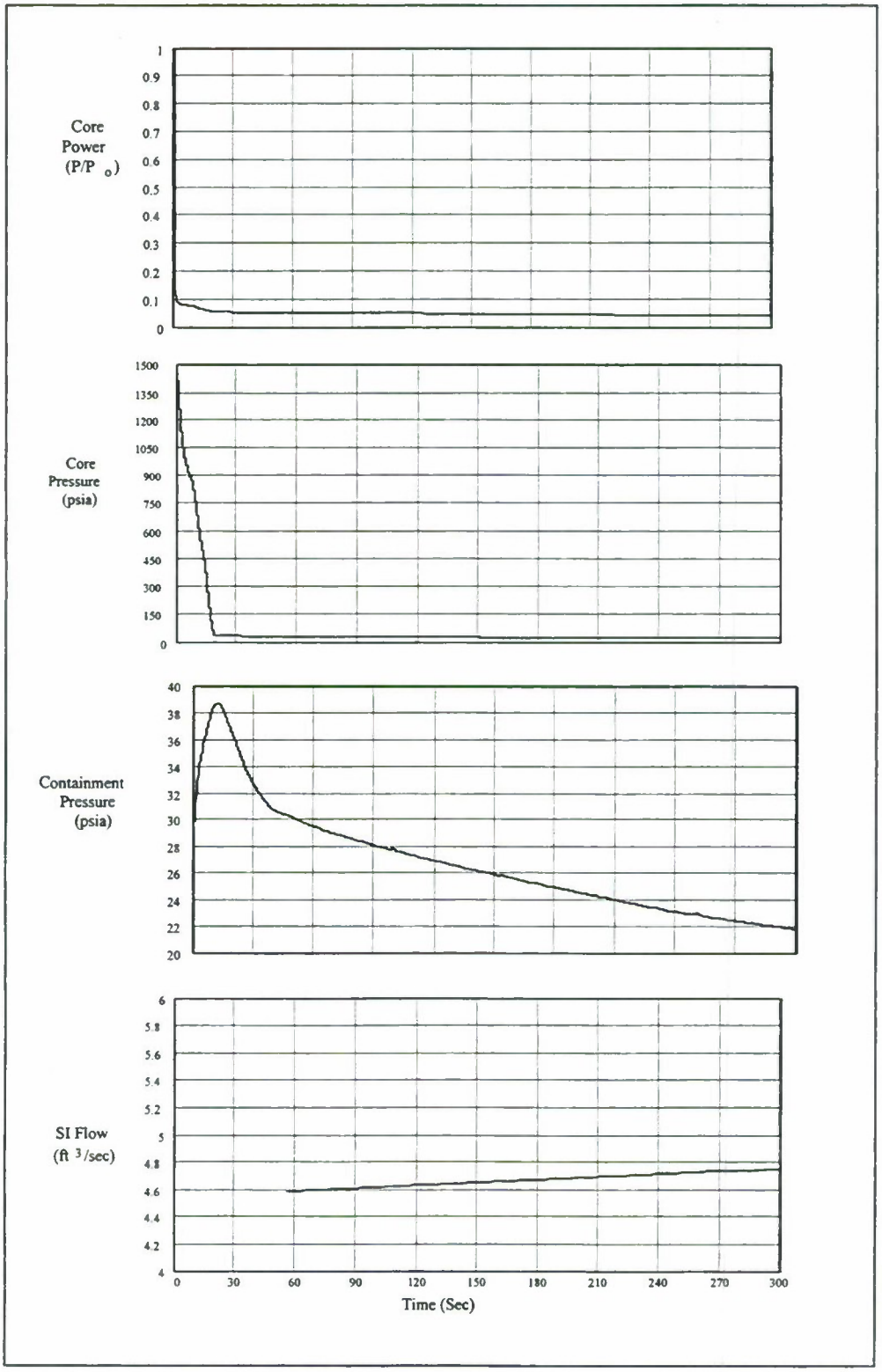


Figure C.10 Observable Parameters during LLOCA Reference Case

- Operators isolate the accumulators after switchover.[4]

- Operators perform the switchover to recirculation cooling after refueling water storage tank (RWST) level reaches 37% [to ensure sufficient emergency sump level to supply the residual heat removal (RHR) pump suction] and must complete the switchover before the pumps lose suction from the RWST (to prevent air binding, pump damage, and starving the core).

- Operators perform switchover from cold leg injection to hot leg injection late in the scenario (to break up any boron crust forming in the reactor vessel, which could interfere with the effectiveness of recirculation cooling)[5]

C.4 Step 4: Define HFEs and/or Unsafe Actions

The LLOCA event tree from the plant IPE is shown in Figure C.11. As shown in the figure, systemic response to the LLOCA (6-inch to double-ended guillotine rupture of the largest cold leg pipe) includes:

- injection of the accumulator water (one of two required)

- low-pressure safety injection [(LPI), one of two RHR pumps to the intact loop]; assumptions: insufficient time for manual recovery, mission time, 1 hour

- low-pressure recirculation cooling [(LP recirculation), one of two trains required]; includes a required operator action

- each sequence ends in success or core damage

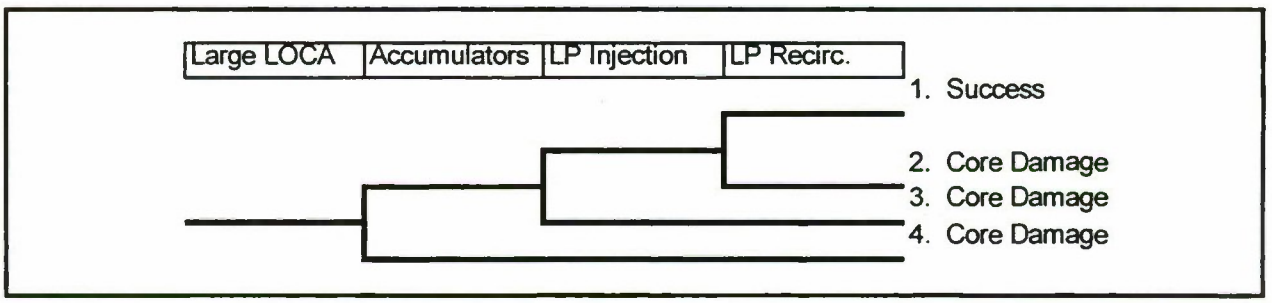


Figure C.11. Large LOCA PRA Event Tree

[4]This step is generally omitted from PRAs because thermal-hydraulic analyses in support of a PRA indicate that nitrogen injection into the loops is not likely to significantly interfere with core heat removal.

[5]This step is generally omitted from PRAs because the best judgment is that boron crust formation is unlikely, except in particular size LOCAs and, even if it forms, can easily be broken up at a later time by shifting to hot leg recirculation.

The ATHEANA process asks that the systemic event tree of the plant PRA be reconstituted as a functional event tree and that other systems and human actions that can provide the same function be identified. For the LLOCA this transformation is quite simple, as shown in Figure C.12. The functions are identified as early makeup (accumulators and low pressure injection, long-term makeup (operators align containment sump recirculation (LP recirculation) at an RWST level of 37% and confirm operation of recirculation cooling), and long term cooling (also provided by LP recirculation, with the cooling function provided by aligning component cooling water (CCW) to the RHR heat exchanger). A reasonable assumption is that the LLOCA progresses so quickly, voiding the core region immediately, that operator action to actuate an initially failed injection system would be ineffective. In addition, because of the stringent requirements of the LLOCA, no other systems than those identified in the PRA event tree are sufficient to provide the same functions.

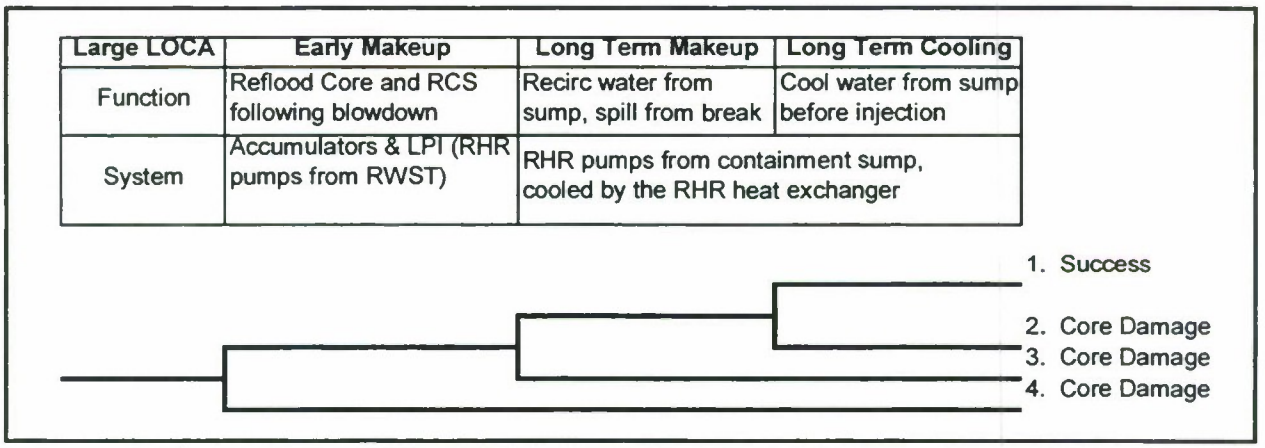


Figure C.12. Large LOCA Functional Event Tree

Application of the HFE identification process (Tables 9.6 and 9.7) leads to the following HFEs:

- Operator improperly removes early makeup from armed or standby status (i.e., improper manual valve lineup blocks accumulator or RHR injection paths, control circuits blocked, or RHR pumps not in auto).
- Operator interrupts early makeup (i.e., operator inappropriately terminates RHR pumps).
- Operator fails to properly align containment sump recirculation cooling.
- Operator prematurely secures long-term makeup or cooling (RHR pumps or CCW to the RHR heat exchangers).
- Operator inappropriately diverts resources (sump water).

All of these HFEs are within the scope of the issue defined in Step 1.

C.5 Identify Potential Vulnerabilities in the Operators' Knowledge Base

To this point, the development and description of the base case LLOCA have been based on thermal-hydraulic calculations for similar events and highlights of the most salient operator actions that are required for successful response to the scenario. A more complete operational view of the LLOCA can be obtained by examining characteristics of the scenario, including information on similarities with training and experience, event timing, identification of operator tendencies, tracking of the emergency operating procedures (EOPs) against the scenario, and identification of informal rules that may affect operator thinking. During this process, we develop information that is helpful in identifying potential vulnerabilities that may make the HFEs more likely than they are under nominal conditions. We post this information on our blackboard for ready access during the search for deviations in Step 6.

C.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

No operators have ever experienced a LLOCA scenario at a U.S. PWR. However, all PWR operators receive regular training on the DBA LLOCA of the base case scenario. Therefore their expectations are very strongly aligned with the base case. However, few operators receive training on smaller LLOCAs (including those called "intermediate LOCAs" in the PRA), so deviations of this sort will be outside of their training and experience. Rules (formal and informal) may not conform with scenarios that deviate from the base case.

Despite extensive training and the clarity of symptoms of this direct initiator, the base case LLOCA is a severe event that no operator expects to see in a real plant. Disbelief may be strong, despite training.

C.5.2 Time Frames for the LLOCA

From the FSAR analysis in Step 3 and the discussion of the base case scenario, five distinct time periods can be identified. These are listed in Table C.2, along with a note of the potential for operator influence.

By the end of the second time frame, 0-20 seconds, the LLOCA blowdown is complete; i.e., the LOCA has ended. By the end of the third time frame, the potential for immediate damage is over; i.e., the LOCA and its direct consequences are finished, without damage to the core. All that remains is the long-term control of stable conditions. Note, however, that the operators have a number of important activities remaining, especially switchover to recirculation cooling at about 20 minutes.

Table C.2 Time Frames for the Base Case Large LOCA

Time Frame	Occurrences	Influences on/by Operators
Initial conditions	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention
Initiator/simultaneous events	Reactor power prompt drop Pressure drops below SI initiation point	These events are over before the operator even recognizes what is happening
Early equipment initiation and operator response: 0-20 seconds	Break flow is complete Pressure drops to essentially zero Containment pressure has peaked and is falling ECCS flow begins Accumulator flow occurs	During this time frame the operator is checking parameters and ensuring appropriate standby equipment has started. Some early decisions in the EOPs may have occurred
Stabilization phase 1-3 minutes	Core reflood begins at about 30 seconds and has reached stable conditions Fuel temperatures have peaked and are falling	During this time, the operators have moved into the LOCA EOP and have passed a number of decision points
Long-term equipment and operator response	Isolation of the accumulators Shift to cold leg recirculation cooling Shift to hot leg recirculation cooling Repair and recovery	During the 20 minutes until switchover to cold leg recirculation cooling, the operators are occupied with confirmatory steps in the EOPs. Any complications beyond the base case scenarios can affect their performance This longer time frame extends to days and months. There are no critical operations concerned with the base case scenario. Problems during this phase would be the concern of a low power and shutdown PRA.

C.5.3 Operator Tendencies and Informal Rules

Of the operator tendencies presented in Table 9.12a of the ATHEANA process, most factors in the LLOCA base case scenario induce appropriate tendencies to control the scenario. For example, low pressurizer level and pressure induce the appropriate tendency to increase injection. They also point toward isolating LOCA paths, decreasing letdown, and turning on pressurizer heaters. However, the heaters would not be helpful for the LLOCA because the pressurizer would be empty. In fact, if the heaters were actuated and not protected by low-level control circuits, they would burn out, which could attract attention and cause some confusion. Finally, high core heat removal (here due to the LOCA blowdown) would in itself encourage undesirable tendencies to decrease injection. It would also create a tendency to decrease RCS forced flow. High containment pressure and temperature would encourage containment isolation, cooling, and spray, all useful tendencies.

A number of informal rules and practices that operators in this plant tend to observe could affect the base case LLOCA and deviations from it. A generic list of informal rules was provided in Table 9.13 of the process and, using the table to guide our thinking, we have evaluated these rules on a plant-specific basis. We have also evaluated plant-specific practices. The results follow:

- Protect equipment. A recent history of running two balance-of-plant pumps to destruction through cavitation and overheating has made operators acutely aware of the hazards of operating pumps with insufficient net positive suction head (NPSH) and dead-headed. Vibration noise is one of the factors they are most sensitive to.
- Recent history of performance. A series of recent problems with the channel A pressurizer pressure instrument has made operators suspicious of its performance. They tend to follow channel B, rather than auctioneered pressure.
- Crew characterization. Formal communication, strong shift supervisors (lower watch standers seldom question supervisor's judgments), low tolerance for perceived gaps in knowledge.
- Lack of deep technical knowledge. Few shift operators have deep understanding of instrument sensor design and the algorithms used in the I&C circuits. Instrument technicians are available during the day shift and can be contacted or recalled on back shifts.

Step 6 will investigate potentially negative impacts of these tendencies and informal rules in the face of deviations from the base case or other complicating factors.

C.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

Perhaps the best operational view of the scenario can be developed by tracking those elements of the EOPs that are processed in the LLOCA. A map of these procedures is provided in Figure C.13 (shown at the end of this chapter because of its large size). The expected procedural pathway for the base case LLOCA is shown by solid arrows. The procedure map tracks all key decision points in the EOPs: (a) branch points to other procedures, (b) internal steps that disable plant functions (i.e., stopping particular plant components that can supply functions that are sometimes needed), and (c) steps that require a major reconfiguration of equipment. Figure C.13 (located at the end of this appendix) combines all procedures carried out during the base case LLOCA scenario. At each decision point (e.g., E-1, Step 2 in Figure C.13), a table in the figure provides the following information:

- actions to be taken
- the potential for ambiguity in the decision criteria in the base case
- a judgment on the significance of taking the wrong branch or inappropriate action

All steps that disable plant functions are indicated by hexagonal boxes (e.g., E-0, Step 20 in Figure C.13). This information is expanded to support the deviation search process by indicating deviation classes under which ambiguity is increased and changes in the significance of taking wrong branches due to effects of possible deviations. For cases where the significance could be high, the box is **bold** and the key aspects of the significance are shown in ***bold italics***. For those cases, relevant potential

ambiguity is also shown in ***bold italics***. The examples cited above show these characteristics. This information will be used later in Step 6, in combination with information concerning informal rules and operator tendencies, to help insure that the consideration of deviations includes identifiable "bad actors."

The path through the procedures for the base case LLOCA is very clear and unambiguous. Taking wrong branches that preclude being alert for early switchover to recirculation cooling (i.e., any path off the LLOCA path) could have serious consequences because the time available for switchover is short and failure will lead directly to core damage.

In addition to the Figure C.13 information, the EOPs provide for continuous monitoring of critical safety functions. EOP F-0.6, inventory, is the earliest indicator of problems and requires monitoring of the following:

- Pressurizer level (>19%)
- RVLIS (void fraction % stable or decreasing or reactor coolant pumps (RCPs) A and B OFF ≥100%)

Depending on the outcomes of these decisions, other function recovery procedures may need to be implemented if additional complications occur during the scenario. These procedures ensure that operators are reminded that injection is required if pressurizer level is low. If the level is high, steps are recommended to compress voids.

C.5.5 Summary of Potential Vulnerabilities

At the close of Step 5, we have posted the information collected on training and experience, time frames, operator tendencies and informal rules, and the EOP map on our blackboard and are ready to begin a systematic search for deviations from the base case scenario in Step 6. Before moving ahead with the search, it will be helpful to summarize the most interesting potential vulnerabilities uncovered during Step 5. That summary is presented in Table C.3.

C.6 Step 6: Search for Deviations from the Base Case Scenario

This search is structured to identify key elements of plant conditions and some aspects of performance-shaping factors that can be primary elements of error-forcing contexts for scenarios that deviate from the base case LLOCA. The resultant error-forcing context (EFC) elements will be refined in later steps of the process. Up to this point in the analysis, the process has been straightforward, proceeding in a well-defined, step-by-step progression. However, the searches described in Step 6 of Section 9, while structured, involve substantial iteration, free-wheeling exploration, and intuitive integration.

Table C.3 Summary of Potential Vulnerabilities for LLOCA

Consideration	Observation	Vulnerability or implication
Training and experience	LLOCA has never happened; seems impossible	Disbelief
	Annual DBA training	Expectations aligned with base case; similarity bias
	No training or experience on LLOCAs<DBA	Unfamiliar, therefore weak knowledge; must adapt DBA
Time frames	LLOCA stabilized by 3 minutes	Intervention during this time period, while unlikely, could be serious
	RWST low level at 20 minutes, recirculation cooling required	Short time available to effect switchover
Operator tendencies	Tendencies: most are appropriate and helpful. However, the tendency for high core heat removal is to decrease injection	Taken alone, overcooling implies reduced injection flow
Informal rules	Pumps will be damaged by low NPSH and deadheading	Strong tendency to stop pumps with suspected vibration noise
	History of channel A pressurizer pressure problems	Believe channel B
	Crew follows formal communication practice, with very strong shift supervisors	Low tolerance of knowledge gaps Lower-level watch standers are hesitant to question shift supervisors
	Lack of deep technical knowledge of I&C, especially instrument and sensor design, and physics algorithms. No technicians on back shifts.	Operator confusion is likely if deviations from base case operations require detailed knowledge of I&C systems
Formal rules/EOPs	No significant ambiguities identified for the base case. A number of steps with high potential significance were identified, which could become ambiguous, depending on the deviation from the base case.	See Figure C.13 for details. Potentially significant consequences can be found at: E-0, Steps 3, 4, and 20 E-1, Steps 1, 2, 12, 14, and 16-19.

Caveat: The analyst new to ATHEANA must resist being fooled by the stepwise presentation of the search in the following paragraphs. What you are about to read is the result of many trials, dead ends, and misdirections. As described in Section 7, the ATHEANA analysis requires a broad range of multidiscliplinary knowledge: behavioral and cognitive science, the plant-specific design and

PRA, understanding of plant behavior (including thermal-hydraulic performance), understanding of the plant's operational practices (including procedures, training, and administrative practices), and generic and plant-specific operating history (including incident history, backlog of corrective maintenance work orders, and current workarounds). The analysts bring this catalog of knowledge to bear, along with the blackboard full of information collected in Step 5, to find the most significant deviation cases. The mental process that allows this integration is complex, not well understood, and not well suited to a step-by-step description, just as the view of a chess game by an expert is more complex and effective than a brute-force lookahead computer program. The process requires a strong facilitator or integrator, who has broad general knowledge of all the disciplines and can challenge any other experts involved in the process. Finally, even if a single analyst can bring all the requisite knowledge to the table, it is essential that others be involved to challenge assumptions, shortcuts, and possibly overly narrow analysis.

C.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

This search proceeds in the manner of a hazard and operability analysis by applying the series of guide words introduced in the process description to the base case LLOCA scenario. For each guide word, we seek physical changes associated with the initiating event that could enable the plant behavior described by the guide word. [Scenarios can also deviate from the base case because indicators (instruments) follow the guide word, while the scenario is otherwise undisturbed until the control systems or operators intercede; as a result of the deviation in instrument response. Such situations are reserved for Step 7, where other complicating factors are considered.]

Using Section 9.6.3 of the process description, the first guide word we apply is "no or not." The idea is that the guide words trigger the imagination of the analyst to identify potentially significant scenarios. There is no concern that the guide words be independent and no effort should be wasted worrying whether a particular deviation case should be categorized under one guide word or another. The guide words are not tools for categorization, but stimulants to the imagination.

What does it mean for there to be "no" LLOCA? It can mean that the loss of coolant itself is less than that assumed in the DBA of the base case. It can also mean that some physical parameters of the plant behave as if the LLOCA were smaller.

"No" LLOCA Deviation Case (<DBA). The LLOCA can be smaller than the base case if the break size in the RCS is smaller than the large double-ended guillotine break of the cold leg; e.g., a break nearer the 6-inch lower size of the PRA's LLOCA. Breaks of this size would offer a variety of challenges to the operator. First and most importantly, breaks of this size (well above the 2 inch size of the small LOCA (SLOCA), but much smaller than the DBA) are not analyzed in the FSAR safety analysis and are generally not discussed in training or exercised on the simulator. Therefore, the operators will not be familiar with the timing and exact sequencing of events. Figure C.14 sketches the kinds of change in parameter trajectories associated with this deviation. Depressurization occurs more slowly and would substantially extend the time until switchover if containment spray (CS) did not rapidly deplete the RWST. Note that while the scenario takes longer to evolve than the base case

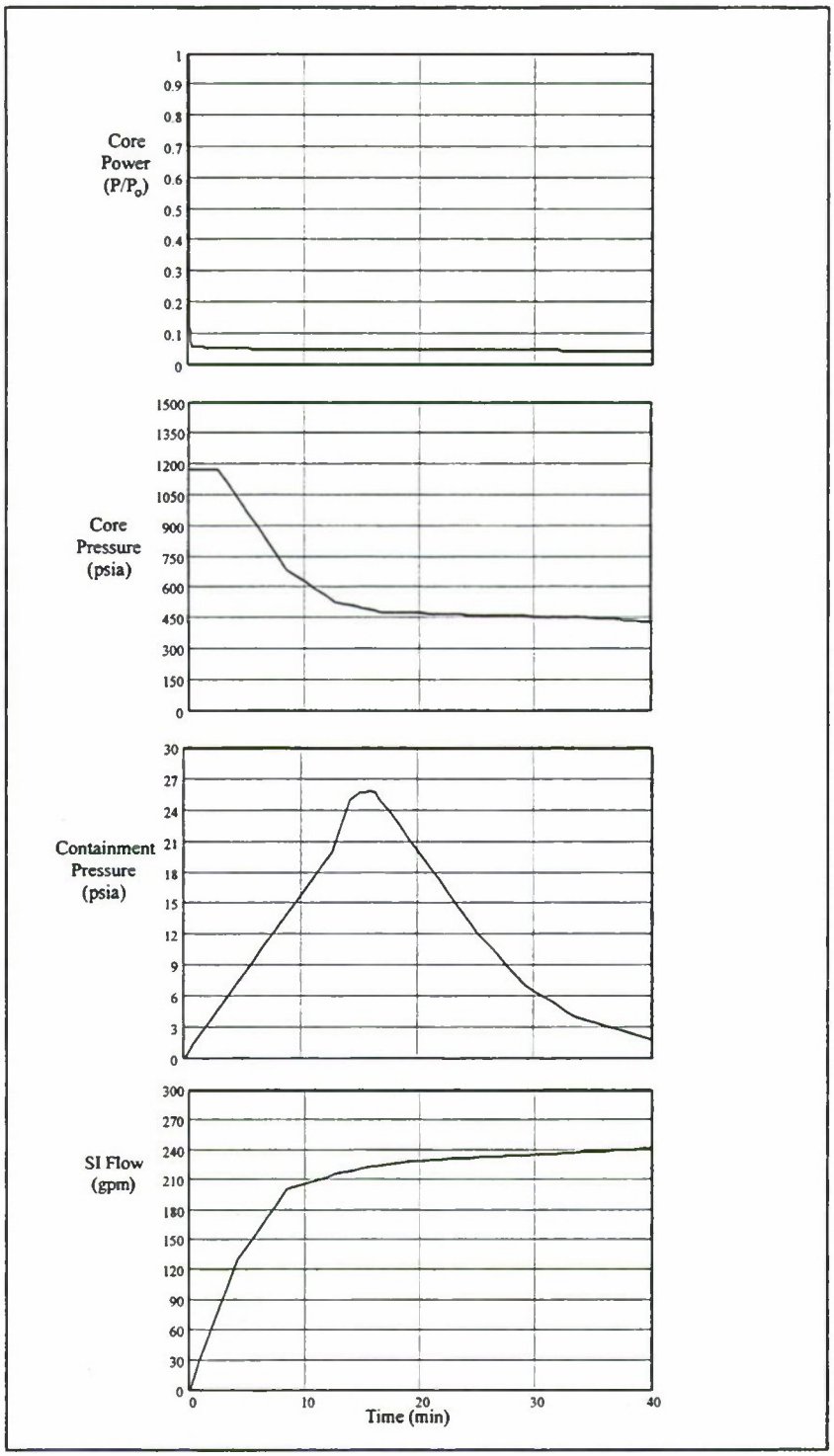


Figure C.14 Observable Parameters during "No" LLOCA Deviation (<DBA) Case

LLOCA, it is substantially faster than an SLOCA. If the operator is thinking SLOCA, the time to switchover could come quickly and the time available for switchover will be significantly reduced. Breaks of this size, while very unlikely, must be more likely than the base case LLOCA (DBA).

To begin the evaluation of this deviation case, we play the scenario against the EOPs, as represented in the map of Figure C.13. Walking through the EOPs, with the timing of Figure C.14 in mind, shows first of all that the procedure works; i.e., it is technically correct. However, differences in timing with respect to two familiar cases (the base case LLOCA and the FSAR small LOCA) have the potential to make some of the ambiguities raised in Section C.5 more significant. Specifically, with no further complicating context, the operators are expected to have no problems due to the deviation in E-0 and should successfully transition to E-1. In E-1 all should go smoothly and at step 18 RCS pressure will be >150 psig, so the operators should transition to ES-1.2. Because the base case did not make this transition, ES-1.2 is mapped separately in Figure C.15, which is also shown at the end of this appendix.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes, while not a major effect, could create confusion. Next, a warning is provided at depressurization steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing pressurizer (Pzr) level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. Nevertheless, if the context becomes sufficiently challenging beyond the deviation scenario condition, old rules can be enabled, such as the "Don't go solid" informal rule. Finally, the SI pump stop criteria in step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading due to an incorrect action. Transfer to sump recirculation could be delayed because of a belief that transfer to RHR cooling will occur soon. In addition to all this, the goal of ES-1.2 is to place the RCS on long term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the emergency director does not choose to place RHR in service in step 24.c (e.g., because of concerns about residual steam in the RCS binding RHR flow) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

Two of the HFEs identified in ATHEANA Step 4 could be enabled, but are not likely without further and sufficiently challenging context (note that the "No" LLOCA deviation case slightly changes one of them):

- Operator interrupts early makeup
- Operator fails to properly align containment sump recirculation cooling or RHR

Returning to the vulnerabilities summarized in Table C.3, we observe that:

- training and experience are weak for this deviation case

- the operator tendency to reduce injection for overcooling is very unlikely to have any impact, unless something causes them to fixate on temperature alone (a massive instrument problem would be required to miss the strong indications of LOCA)

- the history of channel A Pzr pressure problems would be unimportant without failure or erroneous indication on channel B

At this point, the possible physical deviation is well-defined and has been determined to be important enough to proceed to the next part of the analysis. The results of the application of the guide word "No" to the LLOCA base case are summarized in Table C.4, which comes at the end of the guide word analysis of this section. What remains is to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

Next the deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9.15 and 9.16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that the "No" LLOCA (< DBA) case involves at least five different, potentially troublesome characteristics:

- Large change in parameter; under the deviation scenario, this can affect situation assessment and response planning. In itself, this may have minor impact. The change is well within the range observed in training scenarios.

- Low rate of change in parameter compared with the base case LLOCA; can affect situation assessment and response planning.

- Relative rate of change in two or more parameters is not what would have been expected; can affect situation assessment.

- Changes in two or more parameters in a short time; can affect situation assessment.

- Direction of change in parameters over time is not what would be expected; can affect situation assessment. The situation is outside of operator training and, therefore, the operators' mental model.

All these human complications would spell difficulty for the operator and could support the two HFEs listed above, except that the procedure can guide them through it successfully. It is likely that additional factors are needed, such as those identified as causing increased ambiguity in the EOP discussion above, for this to become a significant EFC. For example, lack of crew discussion of confusing situations (informal rules and practices) could compound any misdirection.

The other class of "No" LLOCA scenarios that deviate from the base case LLOCA involve physical parameters of the plant behaving as if the LLOCA were smaller. Parameters identified in the reference case included:

- *Power.* It could fail to drop on LLOCA, if it were over-moderated because of a fuel load error or a violation of control rod program management. This is certainly outside the range of training and operator mental models and could result from human unsafe acts. For now we assume that the probability of such events is low compared to other possible contributors, but it might be worth pursuing at a later date.

- *Pressure.* No phenomenological reason for delayed pressure drop has been identified.

- *Break flow.* No phenomenological reason other than actual smaller LLOCA for lower break flow has been identified.

- *Containment pressure.* The impact of passive heat sinks in the containment could significantly delay pressure rise and peak values. No important impact on operator performance has been postulated.

- *ECCS flow.* ECCS flow can be blocked because of pump or valve failure and these cases are modeled in the PRA. Such failures could be due to a previous HFE in which the operator improperly removed the equipment from the armed/standby status. Given the plant surveillance process, such a situation is very unlikely (although it happened at TMI). It is eliminated from consideration in this analysis, because it is outside the scope of the issue defined in Step 1, limiting the question to the impacts of *physical characteristics* associated with the LLOCA progression. Under other issues, this case may be worthy of pursuit.

  "Less" ECCS flow can occur, because of obstructions or impaired pump performance, or because a smaller LLOCA has occurred and pressure remains too high for full RHR pump flow. The smaller (< DBA) LLOCA scenario was analyzed earlier. The actual impaired flow scenario falls naturally into two cases: those in which flow is reduced below that required to survive the initiator (this case is modeled in the PRA systems analysis) and those where it is sufficient for long term success, but decidedly less than expected and, perhaps, less than needed to meet design criteria early on. Such a case would involve delayed core reflood (not observable to the operator), possible fuel damage resulting in high fission products in the RCS, and, possibly, delayed switchover to sump cooling. Of these, the only one that is likely to be observed and of concern to the operator would be the high fission product concentration in the coolant. It is difficult to see how this would cause significant problems to the operator other than minor confusion and concern, unless this extra burden intensified the pressure due to other outside EFC.

- *Accumulator dump.* Improper nitrogen pressure on the accumulators would delay or speed up their discharge, with little anticipated impact on the accident progression or, therefore, on operator response. From thermal-hydraulic analyses of LOCAs with and without accumulator discharge, impact of such problems on operator performance seems unlikely.

- *Core reflood rate and timing.* No phenomenological reason for delayed reflood has been identified, other than reduced ECCS flow described above..

- *Clad temperature.* No phenomenological reason for decreased clad temperature has been identified.

When we applied the other negative guide words ("Less," "Late/Never," "Too slow," "Too long," and "Part of"), we found that all lead the analysis to the same result. In this example, "No" is a surrogate for all these other words.

"More" LLOCA Deviation Case. The next guide word to consider is "More" (or "Early," "Too quick," or "Too short"). This requires a break size greater than the DBA (i.e., severing of two or more loops or fracture of the reactor vessel), which is very unlikely except under seismic excitation well beyond design or if PTS occurs to a vulnerable vessel. Plant-specific information for this reactor vessel indicates that it is not particularly vulnerable to PTS rupture. At this time, we believe such an event is so low in frequency as to be negligible with respect to risk. We note, however, that while the PRA assumes core melt is guaranteed under such conditions, it is possible to survive some LLOCAs beyond the DBA if all injection systems work. The plant is designed to survive the DBA with any single active failure, e.g., failure of an RHR (LPI) pump. HRA of such an event (after thermal-hydraulic success criteria have been determined) would be concerned with a shortened time to switchover and a reduced time available for switchover. This scenario would be outside of the operators' training and indications that an event greater than the DBA would probably not be recognized.

"Reversed" LLOCA Deviation Case. The next guide word is "Reversed." The notion appears to be meaningless for the LLOCA.

"As Well As" LLOCA Deviation Case. Finally consider "As well as," which also includes "Repeated" and "Inadvertent." Here the idea that developed is that the initial LLOCA suddenly becomes blocked (e.g., by RCS internals that have come loose). An event of this sort could start a bit confused, but quickly appear to be an SLOCA. The observable parameters are sketched in Figure C.16, where a very unfamiliar pattern is seen. Containment pressure looks like a LLOCA. RCS pressure initially falls like a LLOCA, but quickly begins to recover, which is almost surely an unexplainable time history for the operators. Safety injection (SI) flow begins high, but quickly drops to SLOCA levels, when pressure rises above the shutoff head of the RHR pumps. These early, inconsistent details are likely to be ignored as the reality of the SLOCA sets in. Soon, SI pumps will be stopped and the system stabilized. When the debris vibrate loose, reestablishing the LLOCA, there will be little time to recognize what has happened and reestablish full SI, before core damage occurs. This is certainly an unfamiliar scenario. Fortunately it is very unlikely. Nevertheless, we pursue it further because of its unique and potentially challenging characteristics, until it can be proved to be impossible. We also note that a similar scenario would involve a small LOCA that appears to stabilize and later expands quickly to a near DBA LLOCA. Such a scenario would not be as confusing, lacking the unexplained beginning, but could lead to an identical situation. We will call this deviation case the "Switching" LLOCA, being a special case of "as well as."

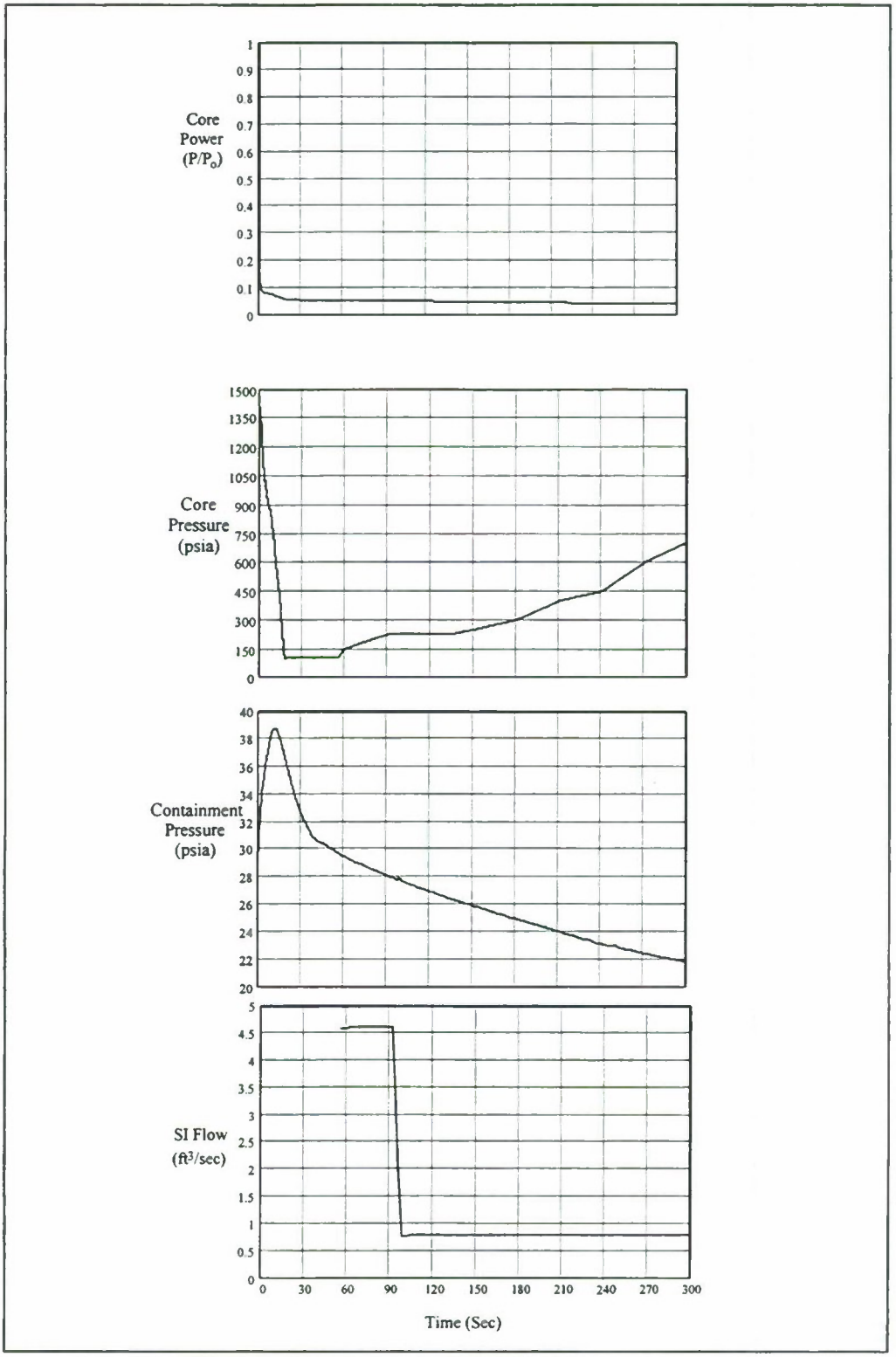


Figure C.16 Observable Parameters during LLOCA "Switching" Deviation Case

Let us take a closer look by tracking the "Switching" LLOCA scenario through the EOPs. Again we begin with the base case LLOCA procedure map of Figure C.13. The early plant response (large drop in pressure and temperature, combined with very high containment pressure) would carry the operators through the initial stages of E-0 with little question. By step 18 some questions and uncertainty could arise. Temperature will be well below 547F and, depending on when they reach this step, it will either be continuing to fall or trending back up. For a LLOCA, temperature would be falling and operators would expect to be securing steam dump. (For an SLOCA they would have expected to need to dump steam and that certainly is not the case.) If they notice the increasing pressure and limited injection flow, they might begin to suspect a steam or feed rupture inside containment. In any case, faith in the diagnostic power of E-0 will still be strong. At step 21, they should find no need to transfer to E-2, the faulted steam generator (SG) isolation procedure, as all SGs should look the same. Even if they choose the wrong path due to a strong belief that a steam break must be the problem, E-2 will send them to E-1, loss of reactor or secondary coolant, with only a slight delay, after isolating the SGs. The loss of secondary heat sink could become a problem later, but not at this time.

In E-1 all should go smoothly initially. At step 14, just before securing the RHR pumps (a different path through the EOP than the base case), the operators are cautioned that "If RCS pressure decreases in uncontrolled manner below 150 psig, RHR pumps must be manually restarted to makeup the RCS." This is an important warning for the "Switching" LLOCA scenario, but we note that there is no other caution or check for this condition other than the critical safety function status tree for core cooling, which looks at the core exit thermocouple readings at irregular intervals. The caution is not on the E-1 foldout sheet, which would be available as a ready reminder. When the LOCA grows sometime later, the crew will be involved in wrapping up the stable and supposedly well understood SLOCA. For now, the crew continues with E-1 until step 18 where, because RCS pressure is above 150 psig, they should transition to procedure ES-1.2, post LOCA cooldown and depressurization. This is the same path followed by the "No" LLOCA case and we can follow the same map of ES-1.2 in Figure C.15.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes, while not a major effect, could add to confusion. The next real trap for the "Switching" LLOCA case comes in step 3.e where, in the first cycle through steps 3-26, the operators are again asked to stop RHR pumps, which will leave the plant with insufficient injection, when the LLOCA begins again. Note that this is not an error. If the pumps are not stopped they will be damaged due to lack of flow. It is, however, an act that leaves the plant vulnerable. Failure to closely monitor pressure, while in a vulnerable state (i.e., until fully depressurized) would be a significant unsafe act.

After step 6, they may not have recovered subcooling, so the EOP path may move on to step 7, rather than step 16, as shown. Next, a warning is provided at depressurization steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing Pzr level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. Nevertheless, if the context becomes sufficiently challenging, old rules can be enabled, such as the "Don't go solid" informal rule. Finally, the SI

pump stop criteria in step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading due to an incorrect action. Transfer to sump recirculation could be delayed because of the belief that transfer to RHR cooling will occur soon. (Furthermore, if the LLOCA reoccurs during step 11.d, the careful focus on the step by step rules in the EOP, especially as conditions are changing, could involve a type of "tunnel vision," delaying recognition that a LLOCA was again in progress.)

The goal of ES-1.2 is to place the RCS on long term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the Emergency Director does not choose to place RHR in service in step 24.c (e.g., because of concerns about residual steam in the RCS binding RHR flow or the odd, unexplained conditions at the beginning of the scenario) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

Once the LLOCA is re-established and, if the operators spot it in time to start the RHR pumps and save the core, it is fair to question how they would use the EOPs. They could jump back to E-0 or E-1. The case is formally included in the EOPs as cautions in E-1, Step 14, and ES-1.2, Step 3. Thus the operators could return to one of those points or carry out the action to start the RHR pumps and continue cycling through ES-1.2, Steps 3-26. The first would naturally take them to sump recirculation cooling in Step 19, if they reach that step in time. The second would simply cycle unsuccessfully hoping to refill the Pzr, when we really should not be in this procedure because we do not meet the >150 psig criterion to enter it. The E-1 foldout, still in effect formally would transfer to ES-1.3 sump recirculation.

From this discussion, it appears that, while the EOP can work for the "Switching" LLOCA deviation case, there may be some rough spots for the crew. Along the way several actions listed as HFEs in ATHEANA Step 4 could be enabled by this deviation scenario:

- Operator removes early makeup from armed/standby status. (Note that this action to disable the RHR pumps is required by the EOP to protect the pumps and is not, therefore, an HFE. It does, however, defeat automatic response of the pumps if they are subsequently needed.)

- Operator fails to properly align containment sump recirculation cooling. (This HFE would be enabled simply by the cyclic structure of ES-1.2, and would be reinforced by the "Switching" LLOCA, because of the differences in timing introduced by a LLOCA occurring after the RWST is partially depleted by the preceding SLOCA.

- Operator fails to manually start RHR pumps, when required. (This is a new HFE, not identified for the base case LLOCA, in ATHEANA Step 4–one that is introduced due to the "Switching" LLOCA deviation scenario.)

Returning to the vulnerabilities summarized in Table C.3, we observe that:

- training and experience do not directly apply; they apply to either the LLOCA or SLOCA base case, but the "Switching" deviation introduces problems in recognition, timing, and EOP ordering

- the operator tendency to reduce injection for overcooling is very unlikely to have any impact

- the history of channel A Pzr pressure problems would be unimportant without failure or erroneous indication on channel B

- the informal rule to protect pumps from damage would reinforce the procedural stopping of RHR pumps and tend to place the focus on protecting the pumps rather than being alert to their future need

At this point, the possible physical deviation is well-defined and appears to be important enough to proceed to the next part of the analysis. It is time to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

The "Switching" LLOCA deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that this case involves at least eight different, potentially troublesome characteristics. This is not surprising; we are involved in a significant deviation from expected plant conditions outside the training and expectations of the crew. This is just the kind of situation implicated in serious accidents in which the operators are "set up" for failure. The identified scenario/parameter characteristics include"

- Large (initial) change in parameter; under the deviation scenario this can affect situation assessment and response planning. In itself, this may have minor impact. The change is well within the range observed in training scenarios.

- Low rate of change in parameter; can affect detection, situation assessment and response planning.

- Relative rate of change in two or more parameters is not what would have been expected; can affect situation assessment.

- Changes in two or more parameters in a short time (following a period of stability); can affect detection and situation assessment.

- Garden path problem; can affect situation assessment.
- Situations that change; can affect situation assessment.
- Multiple lines of reasoning; can affect situation assessment.

These human complications spell difficulty for the operator and support the three HFEs listed above. Although the procedure can guide them through it successfully, there are significant factors that can defeat its success.

Summary of Deviation Cases. Results of the preceding guide word deviation analysis are summarized in Table C.4, where, for each guide word, we summarize the identified possible physical deviations and their significance. We also indicate which of these deviation cases are considered further. The summary analysis is continued in Table C.5, where the scenario/parameter characteristics of the deviation cases from Tables 9.15 and 9.16 are presented. The analysis of these characteristics is extended in the table by identifying the associated error types and error mechanisms from Tables 9.15 and 9.16 that apply to each deviation case.

Consider the "No" LLOCA deviation case. Despite the large number of error types and error mechanisms that could enable the two HFEs

- Operator interrupts early makeup
- Operator fails to properly align containment sump recirculation cooling or RHR

there is substantial time for the operators to respond to the many directions in the EOPs that would restore the scenario to a success path. It appears that the "No" LLOCA deviation case surely requires additional error-forcing context (e.g., instrumentation problems or significant extraneous demands on attention) to become significant. Informal rules described in the text would then become important and could lead to either HFE. The issue addressed in this analysis is to assess if *physical deviations* in the LLOCA initiator and base case scenario can adversely affect the operators in ways that have the potential to transform the DBA into a core damage. Because it appears that additional complications beyond the *physical deviations* in the LLOCA initiator are required for this case to have a reasonable likelihood of leading to the HFEs, the "No" LLOCA deviation case is dropped from further consideration in this analysis.[6]

---

[6]The interested reader will find that a very similar scenario was identified through a less direct process, in a trial of an earlier version of ATHEANA (NUREG-1624). That analysis proceeded by identifying potential HFEs; searching procedures and informal rules for rules that would direct the HFE, if used improperly; and then tried to add on plant and human context that would enable the HFE. There was no direct search for deviations or procedure mapping, so success depended on close familiarity with EOPs by operators on the analysis team and a rather free association of principles from behavioral science with plant conditions and the HFE, to complete the context. The scenario of the previous analysis included an initiating event that is nearly identical to the "No" LOCA deviation case; that analysis also identified significant failures in instruments. The conditional probability of the HFE and failure to recover was quite high (0.8 and 0.1). However, the plant-specific probability of the particular postulated instrument failure was very low, leading to a very small contribution to core damage frequency.

Table C.4 Application of Guide Words to LLOCA Deviation Analysis

Guide Word	Possible Physical Deviation	Significance	Carry Forward? (Explained in Text)
No/not/less/ late/never/too slow/too long / part of	Break size less than DBA	Can change timing, no longer have right conditions at EOP decision points. If the vulnerabilities identified in the text enable associated error mechanisms, operators could interrupt early makeup or fail to properly align sump recirculation cooling or RHR.	Yes
	Power fails to drop (fails to shutdown)	Only possible if pre-existing error violated fuel load/control requirements. Assumed very low probability.	Not evaluated further, at this time
	Reduced ECCS Flow	Reduced flow due to obstruction or impaired pump performance is either too great for success (and is therefore included in ECCS system analysis of the PRA) or impacts timing and RCS radioactivity, which does not appear to have significant impact on human performance.	No, little impact on operator performance
More/ Early/ Too Quick/ Too Short	Break size greater than DBA (i.e., greater than 2 loops or reactor vessel)	Not analyzed because very low in frequency and little impact on operator performance. Either the event is too severe for the ECCS to handle or not. The operator has no direct indication of LOCA size. However, because of redundancy in injection systems, and because full HPI adds significant flow, the plant could survive some such accidents. Can change timing, especially shortening the time to start and to complete switchover.	No, little impact on operator performance
Reversed	None	No physical sense other than inadvertent SI, which is another identified initiating event.	No, N/A
As well as/ repeated/ inadvertent	Switching; starts as near-DBA, plugging by debris, later return to LLOCA	Interim SLOCA leads to disabling LPI and automatic SI actuation, operators fall into a regime where they know what is going on Very low in frequency, but significant impact on operations.	Yes

Table C.5 Results of LLOCA Deviation Analysis

Possible Physical Deviation	Characteristics Potentially Affecting Human Response	Potential Error Types and Mechanisms	Further Analysis and Possible Similar Scenarios
"No" LLOCA Deviation Case: Break size less than DBA	Large change in parameter Low rate of change in parameter Relative rate of change in two or more parameters is not what would have been expected Changes in two or more parameters in a short time Direction of change in parameters over time is not what would be expected	A number of error types and mechanisms relevant to the HFEs (interrupt early makeup and fail to align recirculation) are associated with the characteristics Error types include lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to taking inappropriate action, taking correct action too soon, and failure to take needed action The underlying error mechanisms include over-eagerness, simplifying, preoccupation, tunnel vision, and fixation	The issue addressed in this analysis is to assess if *physical deviations* in the initiator can lead to core damage. This scenario is dropped from further consideration, because it almost surely requires additional context (e.g., instrumentation problems or significant extraneous demands on attention) to become significant.
"Switching" LLOCA Deviation Case: starts as near DBA, plugging by debris, later return to LLOCA	Large change in parameter Low rate of change in parameter, early on Relative rate of change in two or more parameters is not what would have been expected Changes in two or more parameters in a short time (following a period of stability) Garden path problem Situations that change Multiple lines of reasoning	A very large number of error types and mechanisms relevant to one HFE of Step 4 (fail to align recirculation) and a new HFE (fail to manually initiate LPI) are associated with the characteristics Error types include lack of awareness of change, generation of false theories to explain seeming anomalies, delay in response while searching for an explanation, lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to missing a decision point, taking inappropriate action, and failure to take needed action The underlying error mechanisms include incredulity, over-eagerness, simplifying, preoccupation, tunnel vision, fixation, lack of deep technical knowledge, and multiple lines of reasoning are creating conflicting choices	Yes, continue. Similar scenario: Small LOCA that stabilizes and later expands quickly to a near DBA LLOCA; similar scenario, but much more likely

Now consider the "Switching" LLOCA deviation case. This scenario has many nearly overwhelming error mechanisms at work. On top of that, although one can track a success path through the EOPs, there are many opportunities for missing, at least for a short time, necessary pieces of information. All this is combined with unfavorable timing (very short time frame for restarting RHR pumps; a distorted picture of the time until switchover to recirculation, and possibly, for switchover due to the long time under SLOCA conditions). Finally there is disbelief that a LLOCA can actually occur and the early confusion in the event. All together, this is a very strong EFC for the two HFEs under consideration.

C.6.2 Search of Relevant Rules

The EOPs applying to the base case LLOCA were examined in Section 5 and yielded no strong context that would be expected to lead to error without further EFC. In addition, the two more challenging deviation scenarios developed from applying the guide words to the base case LLOCA led to a thorough review of the EOPs applied to these scenarios, under the search of Section C.6.1. This search of the EOPs yielded several challenging conditions.

Because of the strong context already developed, no further search of the rules is needed here.

C.6.3 Search for Support System Dependencies

In some designs, there are large valves in the RCS loops that can be opened under RCS pressure. In addition, there could be some combination of pump seal ruptures that could equal a LLOCA. For such plants, human actions and the effects of support system failures (e.g., seal cooling systems) could induce a LLOCA. However, in this plant no support system induced failures and human actions have been identified that can mimic a LLOCA. There are no large valves that interface with the RCS that can be physically opened under normal RCS pressure. Likewise there are no combinations of pump seals, whose rupture is larger than an SLOCA.

A related issue is dependency among operator actions. It is possible that, if operators identify the need for restarting RHR pumps in time, there could be some dependency between that action and the eventual action to switchover to recirculation cooling. One was identified in the discussion of the "Switching" LLOCA scenario in Section C.6.1. Depending on which procedural anchor the operators use to start the RHR pumps, they can restart E-0, jump to E-1 Step 14, jump to ES-1.2 Step 3, or simply start the pumps and continue their cycle through ES-1.2. The likelihood of being ready for recirculation, when needed, may depend on this decision.

C.6.4 Search for Operator Tendencies and Error Types

This search could develop other potentially significant EFC that could become contributors to core damage frequency. However, it will not be performed, for two reasons:

- As indicated in the process description of Section 9.6.6, this search is a "catch-all" for deviation characteristics that might have been missed in the earlier searches. It is similar to

the open-ended search of earlier versions of ATHEANA, albeit a more structured approach. If significant EFC/UA combinations have been identified by the earlier searches, they are more likely to be important, because they focus on elements known to be represented in serious accidents

- It is outside the scope of the issue for which this ATHEANA analysis is performed. The issue is to determine if *physical characteristics* associated with the progression of the LLOCA can adversely affect the human operators in ways that have the potential to transform the DBA into a core damage accident.

C.6.5 Develop Descriptions of Deviation Scenarios

The description of the "Switching" LLOCA in Section C.6.1 is complete and has not been extended by searches in C.6.2, C.6.3, or C.6.5, because the context was deemed strong enough without further requirements that diminish the frequency of the event. Likewise, while additional complicating factors would make the context even more cognitively demanding, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be added at this time.

It is appropriate, at this point to summarize the key elements of the "Switching" LLOCA scenario; identify those vulnerabilities, error types and potential error mechanisms that we believe are most significant; and identify the associated PSFs. This information is presented in Table C.6.

C.7 Step 7: Identify and Evaluate Complicating Factors and Links to PSFs

This step is addressed in section C.6.5 above.

C.8 Step 8: Evaluate the Potential for Recovery

Because of the short time available for restarting RHR pump, the short time later when switchover to recirculation must begin, and the short time available to complete the switchover, recovery is not considered separately. Definition of the HFEs will include the idea that failure means failure to accomplish the activity, within the time before unrecoverable damage occurs.

C.9 Step 9: Quantification Considerations

Quantification of the "Switching" LLOCA deviation case will focus first on the probability of the unsafe acts (UAs), given the scenario. The reasons for this are explained in more detail in the following section on issue resolution.

Probability of Unsafe Acts. We address the probability of the UAs including non-recovery in an integrated one-step process. Thus we evaluate

Table C.6 "Switching" LLOCA Deviation Scenario

Overall Plant Condition (Scenario)	Key Information Related to HFEs, Error Types, and Error Mechanisms	Most Relevant PSFs
Event starts as near DBA LLOCA. After the initial few second of response, plugging by debris occurs and the event continues as an SLOCA. Later, after the operators have stabilized the SLOCA and are preparing for long term cooling, the debris vibrates free and the LLOCA returns.	Two HFEs of interest (fail to align recirculation) and (fail to manually initiate LPI) Unexpected initial events can lead to false theories to explain seeming anomalies caused by incredulity; this allows the initial information to create early confusion and to become lost later, when it would be helpful As operators settle into the SLOCA track, they become vulnerable to the garden path problem and are susceptible to tunnel vision and fixation, simplifying the scenario by ignoring the initial LLOCA-like trends When RHR pumps are secured, the procedure warns that manual restart would be required. Nevertheless, experience and training reinforce the garden path scenario As they begin to focus on moving out of SI and into RHR cooling, they can become preoccupied with the details of EOP ES-1.2 and developing an over-eagerness to reach the stable end point All these factors permit a lack of awareness of change and of attention to other parameters Now they are set up for failure to recognize a serious situation in time; i.e., they can miss a key decision point, failing to take needed action, when RCS pressure suddenly falls because of the reinitiated LLOCA Even if they should respond in time, restarting the RHR pumps, multiple lines of reasoning about where to branch in the EOPs creates conflicting choices, delaying their attention from preparing for recirculation cooling, which will be needed very soon	Training/practice. Lack of training or practice for off-normal, unexpected accident conditions and problem solving Training/practice. Base case LLOCA and SLOCA used repeatedly in training Procedures. Insufficient warning to be prepared for rapidly increasing LOCA Lack of trending displays allows odd initial parameter tracks to be put aside

$P(UA_1)$ = P(operators fail to restart RHR pumps | EFC), and

$P(UA_2)$ = P(they fail to complete the sump recirculation cooling lineup before the RWST runs dry | they restart RHR pumps $\wedge$ EFC)

Taking into account the deviation scenario, including the associated EFC documented in Table C.6 and the short time available for each action, the analysts have developed a consensus judgment of the likelihood of the crew performing these unsafe acts. Their judgment is based on their experience, their observations of many crews in the plant and in simulators, and their understanding of the context of this event, including the status of procedures and training discussed earlier. Given the difficult context of the scenario our estimates are

$P(UA_1)$ = 0.30; i.e., they are only slightly more likely to restart the pumps than not

$P(UA_2)$ = 0.07; i.e., about 1 in 15 crews would be trapped by the short time, multiple lines of reasoning, and deceptive timing and fail to shift to recirculation in time[7]

Frequency of Error-Forcing Context. To be consistent with the PRA, we estimate the frequency of LLOCA as 1×10^{-4} per year. The conditional probability of the "Switching" LLOCA, given a LLOCA would generally be quite low, we believe, although there is no direct experience with LLOCAs in PWRs to demonstrate that real LLOCA forces in an aged, real plant would not result in unexpected structural failures. For our particular plant, a recent SG internal inspection identified indications in the steel sheet that separates the T_H and T_C plena that were believed to be insignificant, but were scheduled for a detailed examination at the next refueling outage. Under this condition

---

[7]As a sanity check on these estimates, we examine the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10. First we must match our actions and EFC with those in HEART. The following are reasonable matches:

- Restarting the RHR pumps, is, in the words of HEART a "routine, highly practiced, rapid task involving relatively low levels of skill, but EFC is "unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel." The associated probability is no more than 17 * 0.02 or 0.34, with uncertainty of (0.12 to no more than 0.77)

- Switchover to recirculation cooling, is, in the words of HEART almost a "complex task requiring a high level of comprehension or skill." It is tempered by the fact that they did restart the pumps and hardened by the strength of the EFC. If we assume that the positive impact of having restarted the pumps balances the difficult EFC, the associated probability from HEART is 0.16 and ranges from 0.12 to 0.28.

Our estimate for UA_1 is surprisingly consistent with the generic estimates in HEART. Our estimate for UA_2 is lower than HEART by about a factor of 2; i.e., reasonably close.

combined with the forces of the LLOCA, the conditional probability of cracking and displacement of that sheet and later shifting as pumps are started and stopped is judged to be 1 in 10. So the frequency of the "Switching" LLOCA is 1 x 10^{-5} per year, for this particular plant.

Frequency of the Event Leading to Core Damage. Combining the frequency of the EFC and the probability of the HFEs yields an estimate of core damage frequency due to the physical deviation of the "Switching" LLOCA scenario creating an EFC that sets up the operators for failure. To have failure, either the operators fail to restart RHR pumps or they successfully start the pumps and fail to complete the sump recirculation cooling lineup before the RWST runs dry; i.e.,

$$P(UA_1) + \{[1 - P(UA_1)] * P(UA_2)\} = 0.35$$

Combining the frequency of the EFC with the probability that one of the UAs occur yields a core damage frequency of 3.5 x 10^{-6} per year for the "Switching" LLOCA deviation case.

C.10 Issue Resolution

This ATHEANA example analysis was performed to address one specific issue:

> *To determine if physical characteristics associated with the progression of the LLOCA initiator can adversely affect the human operators in ways that have the potential to transform the DBA into a core damage accident.*

The analysis defined several deviation scenarios in Table C.4 that go beyond training and FSAR analysis and could lead to core damage. Two of them are functionally challenging, but would not seem to challenge the operators. One, "Power fails to drop," could be very challenging to the operators, but it would appear to be very unlikely, and was dropped from the analysis without substantial investigation into its plausibility. Of the remaining two, the "No" LLOCA deviation case (< DBA) was shown to involve many possible human error mechanisms, but was believed to require additional complications for the HFEs to have a substantial chance of occurring. It goes, therefore, beyond the issue defined for the analysis and was dropped, but flagged as a case worthy of investigation under other issues.

The remaining case, the "Switching" LLOCA involves many challenging aspects. The probability of an HFE, given the scenario, is quite high. In a generic sense, the frequency of this initiator is very, very low. Nevertheless, there are several reasons to consider the case seriously:

- It is more than frequency. In the spirit of medical diagnosis, it is not simply the probability of a possible diagnosis that is of interest. If some very high consequence *treatable* disease has a low probability of being correct, we hope our physician does not dismiss it, because of its low probability, but investigates further (more research on the characteristics of the

disease, more tests, etc.). We are more willing to play the odds, if the consequences are low. This is not to say that risk is not a suitable criteria for programmatic decision making, but that in diagnostics, it is worthwhile digging deeper and being better prepared for high consequence events.

- The frequency might not be correct. There may be failure modes not yet evidenced that can occur under specific conditions, including aging. Even if generically the chance of the "Switching" LLOCA may be very low, specific plants with specific designs, operating histories, maintenance histories, and vulnerabilities could have a much higher frequency for such events.

- Similar events. As identified in Table C.5, an SLOCA that stabilizes and later expands could have similar consequences, but higher frequency. Other possibilities include a smaller, more likely LLOCA combined with:

  – one RHR pump out of service and a second that was allowed to run "too long" in the operators' view such that they believe it is damaged.

  – Channel B Pzr pressure instrument out of service and the operators disbelieve Ch. A

Thus the issue resolution process may demand that the analysis be extended or that, because of the broad range of possibilities, some precautions in training or practice be instituted to ensure, if an unlikely or unforseen condition arises, the operators are well prepared to deal with it.

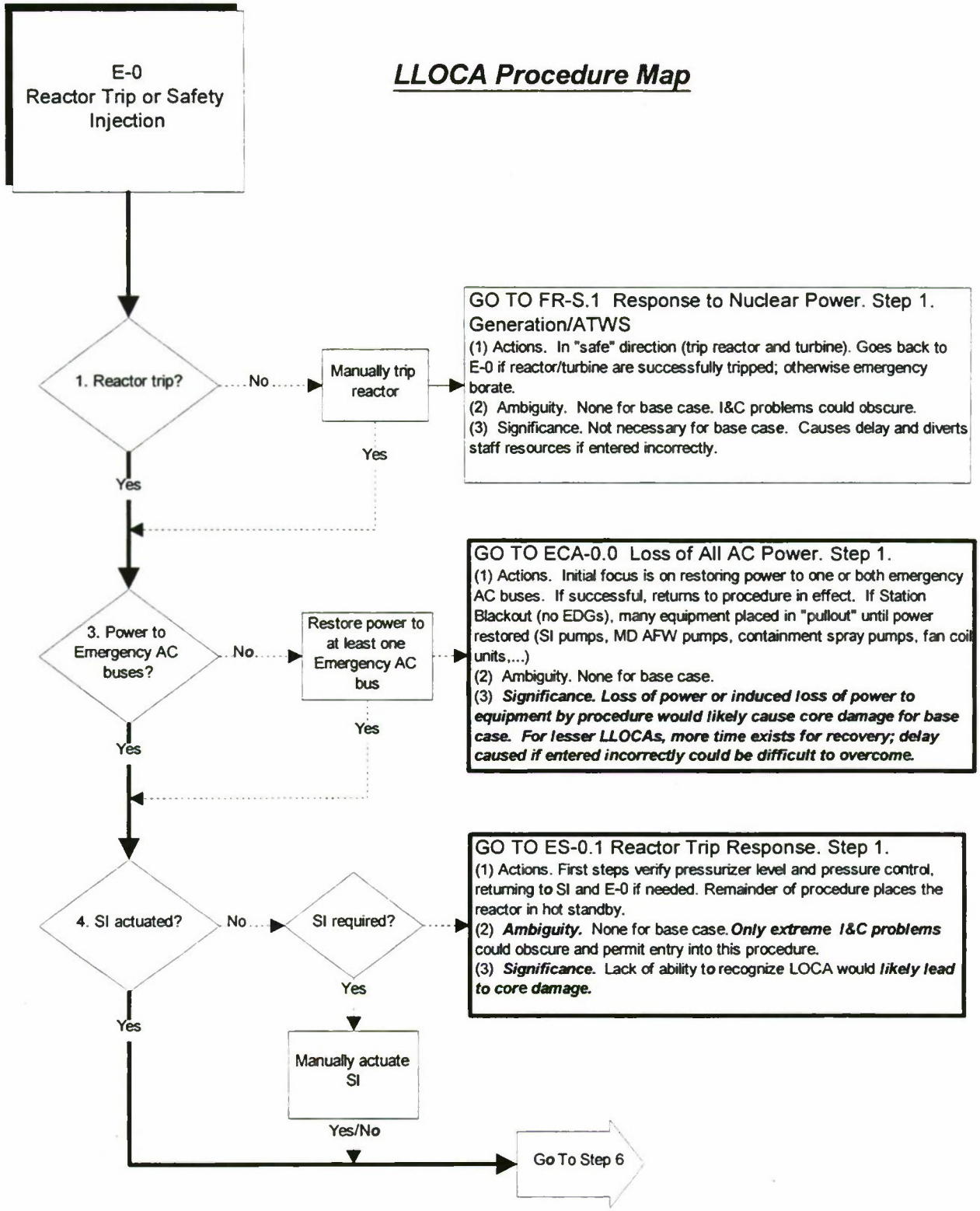


Figure C.13 EOP Map for Base Case LLOCA (Sheet 1)

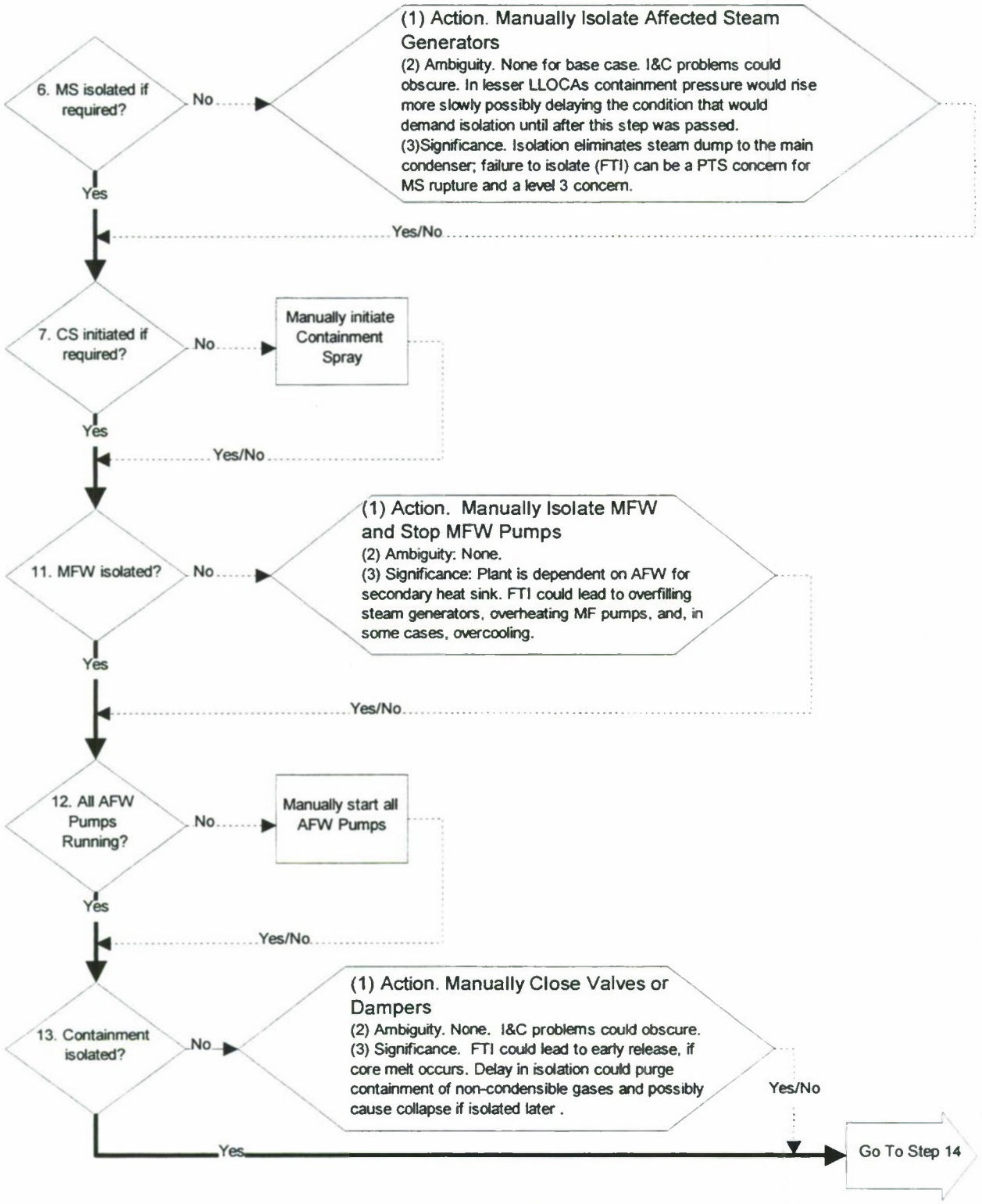


Figure C.13 EOP Map for Base Case LLOCA (Sheet 2)

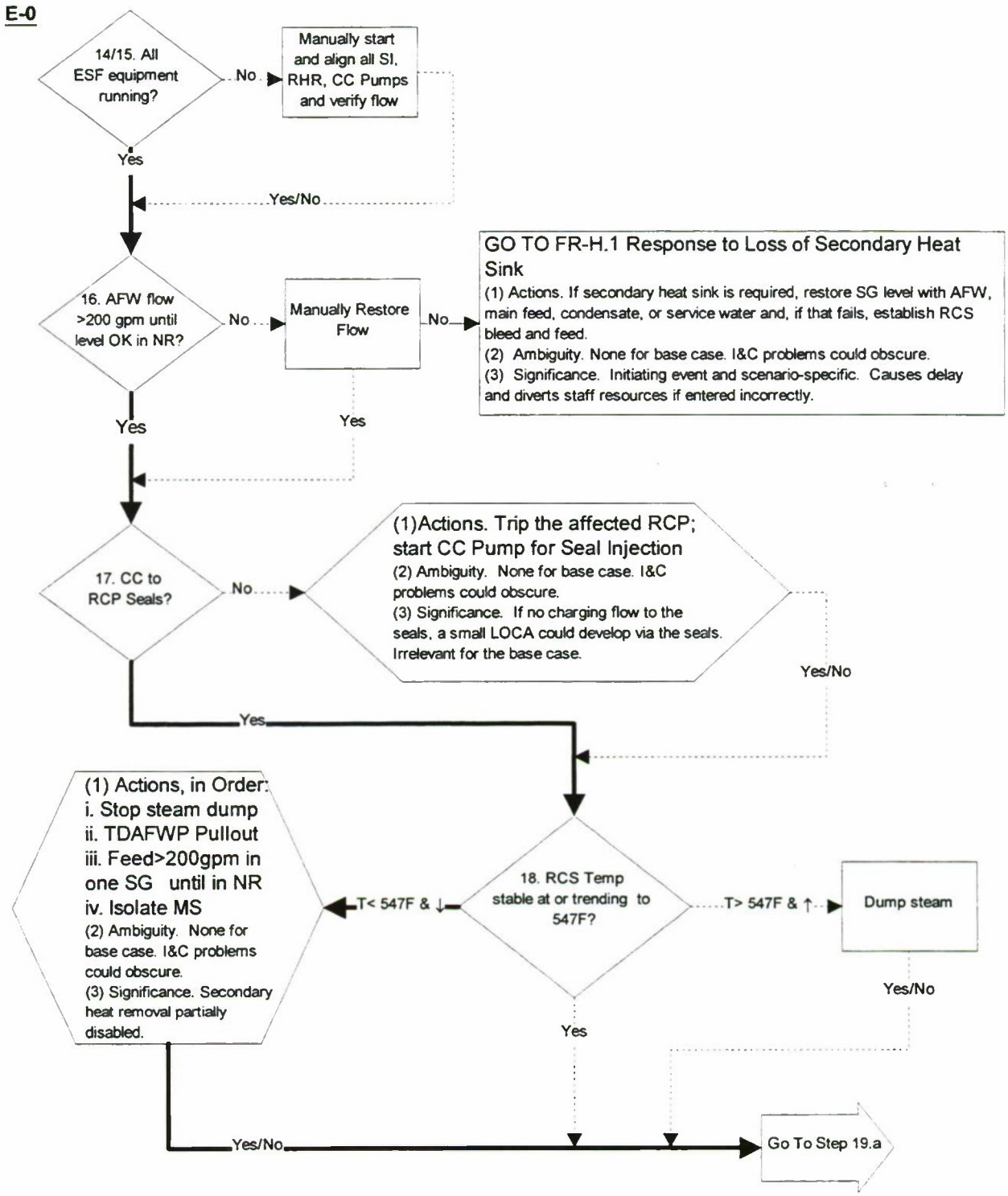


Figure C.13 EOP Map for Base Case LLOCA (Sheet 3)

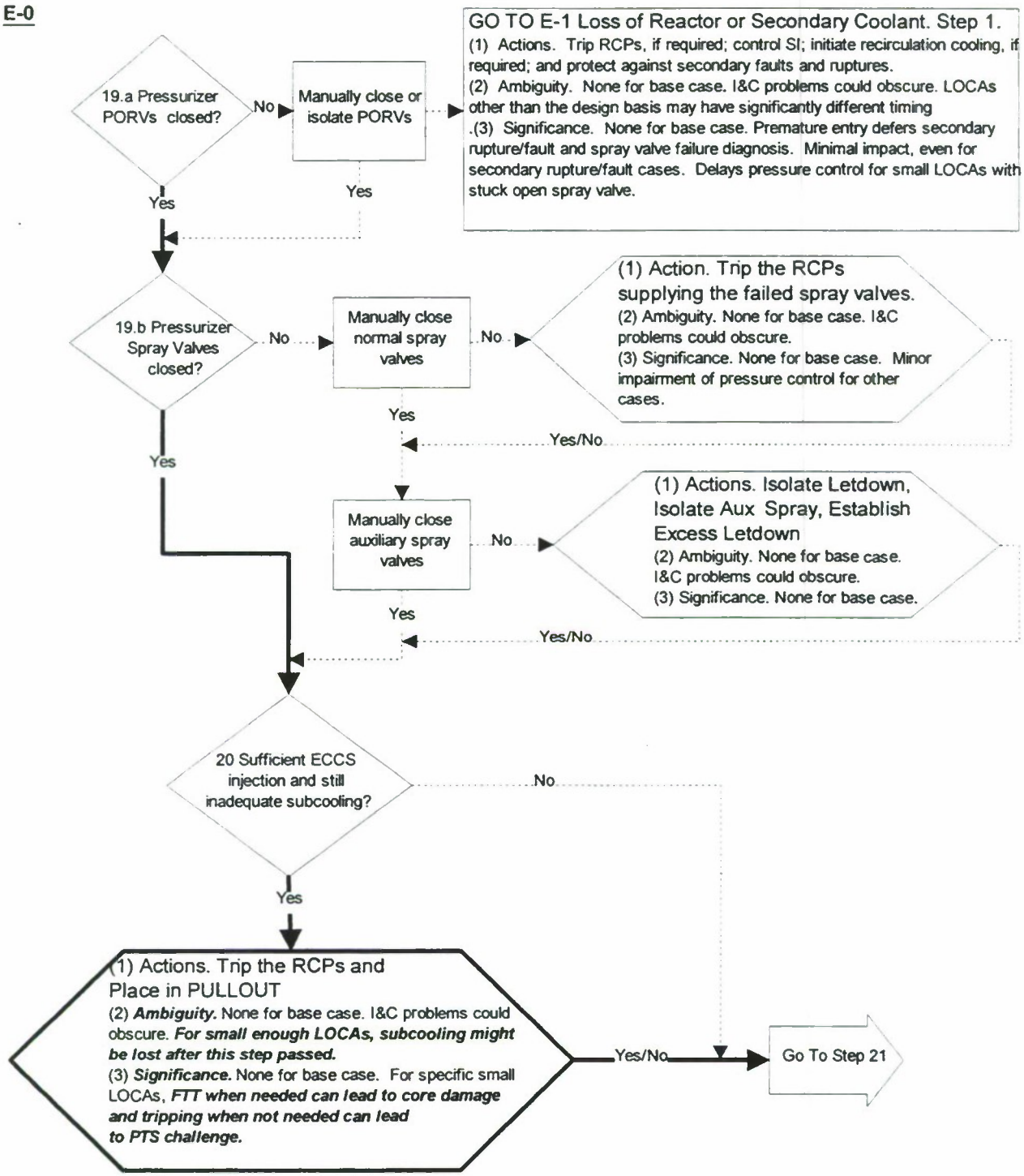


Figure C.13 EOP Map for Base Case LLOCA (Sheet 4)

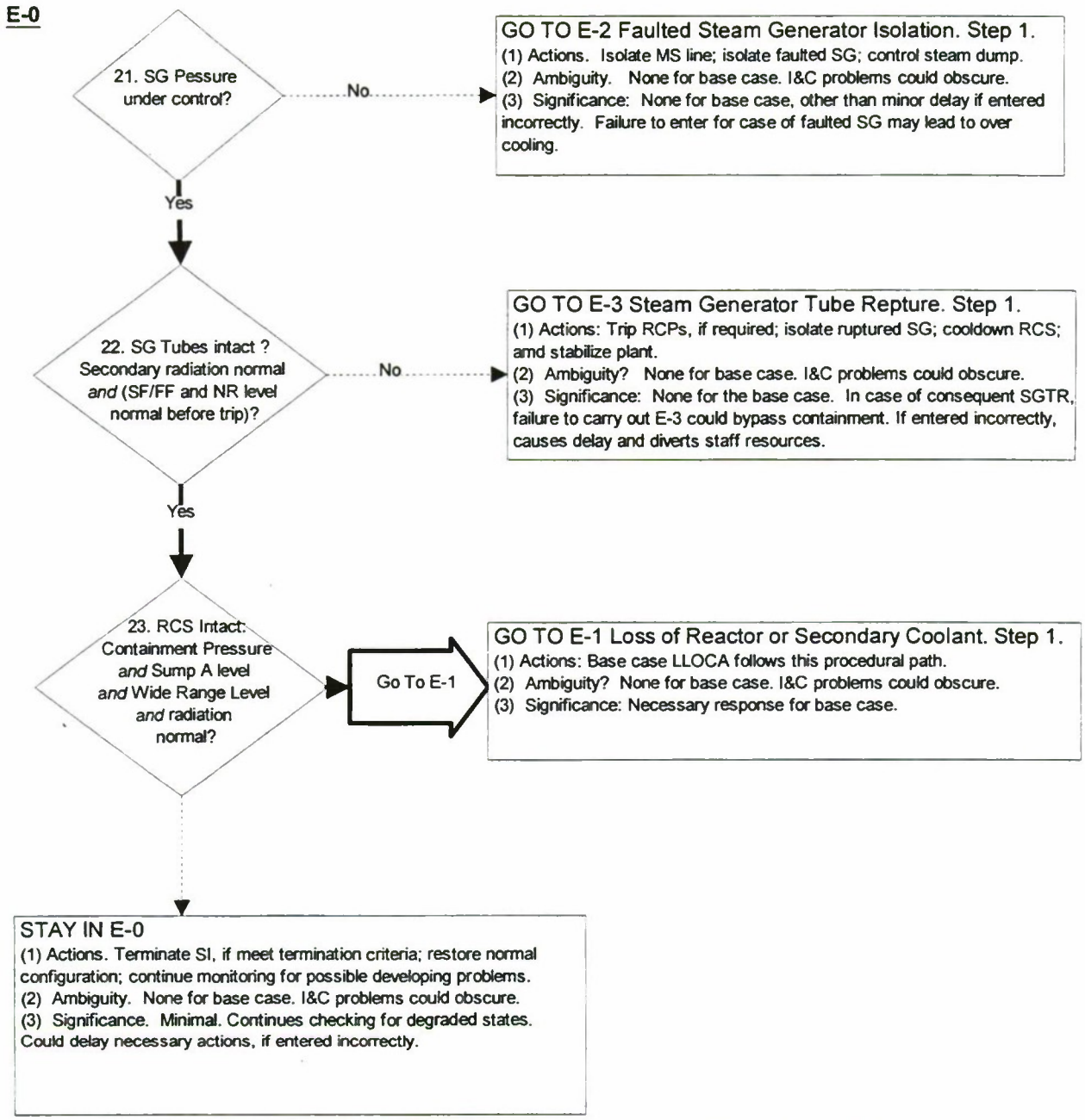


Figure C.13 EOP Map for Base Case LLOCA (Sheet 5)

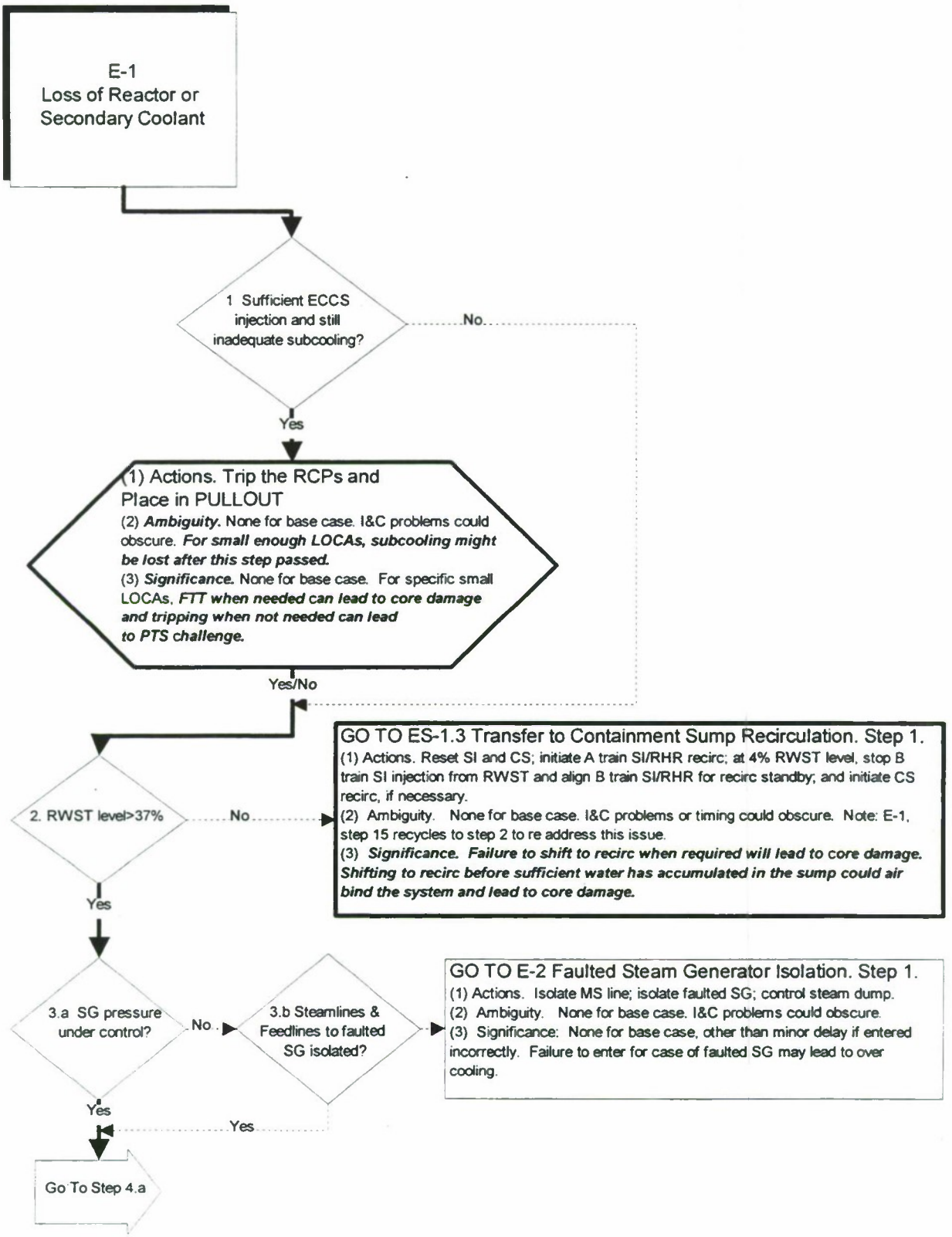


Figure C.13 EOP Map for Base Case LLOCA (Sheet 6)

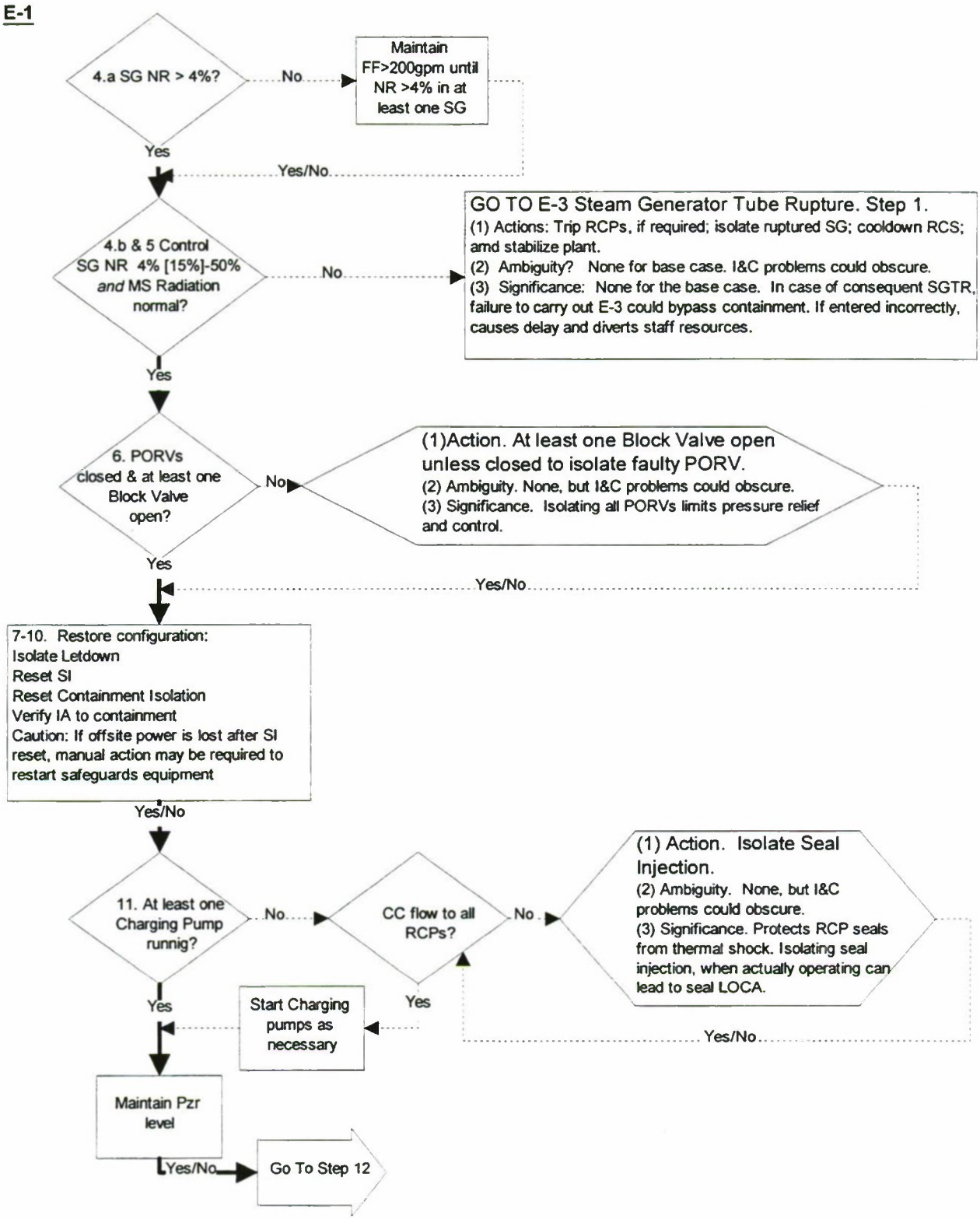


Figure C.13 EOP Map for Base Case LLOCA (Sheet 7)

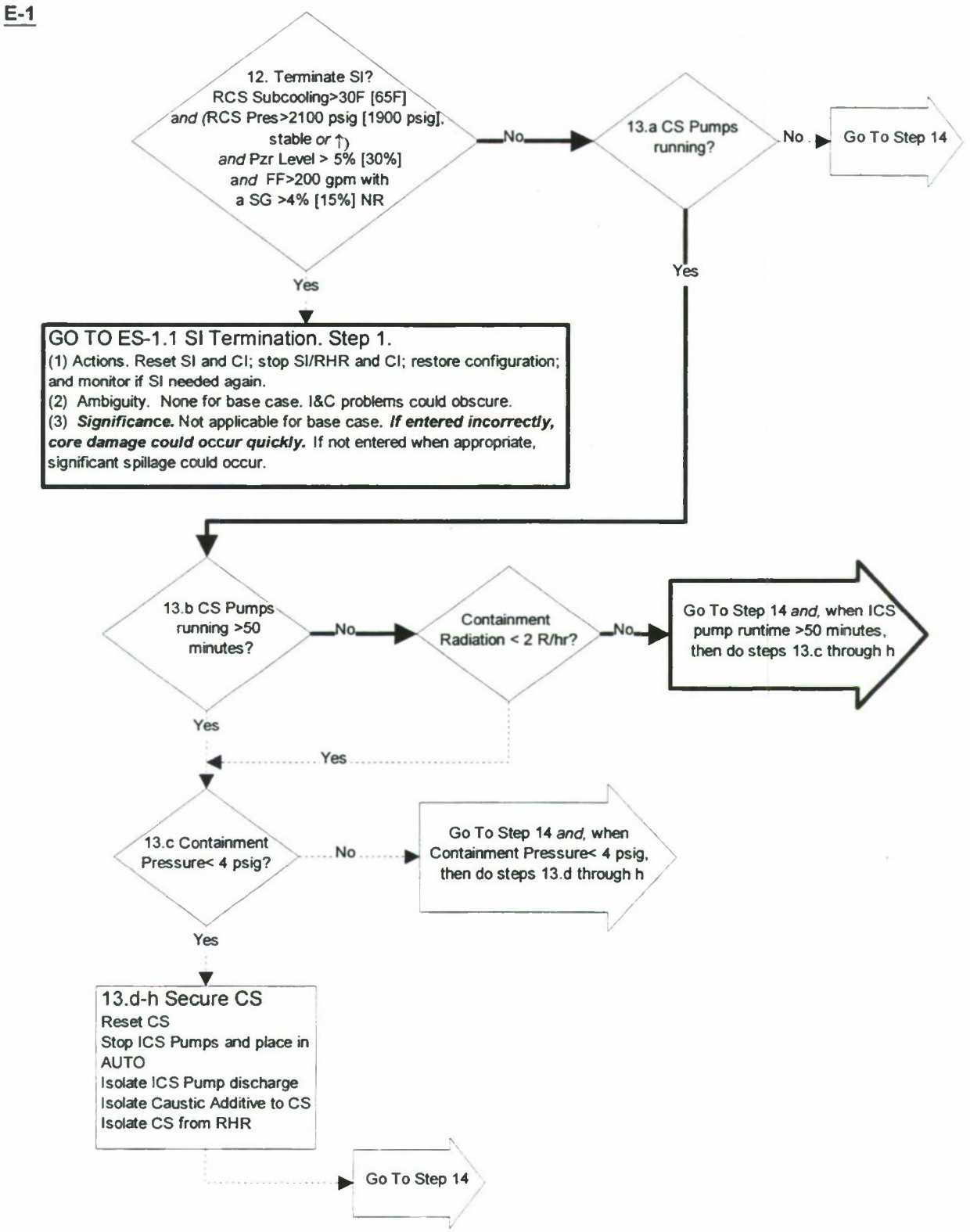


Figure C.13 EOP Map for Base Case LLOCA (Sheet 8)

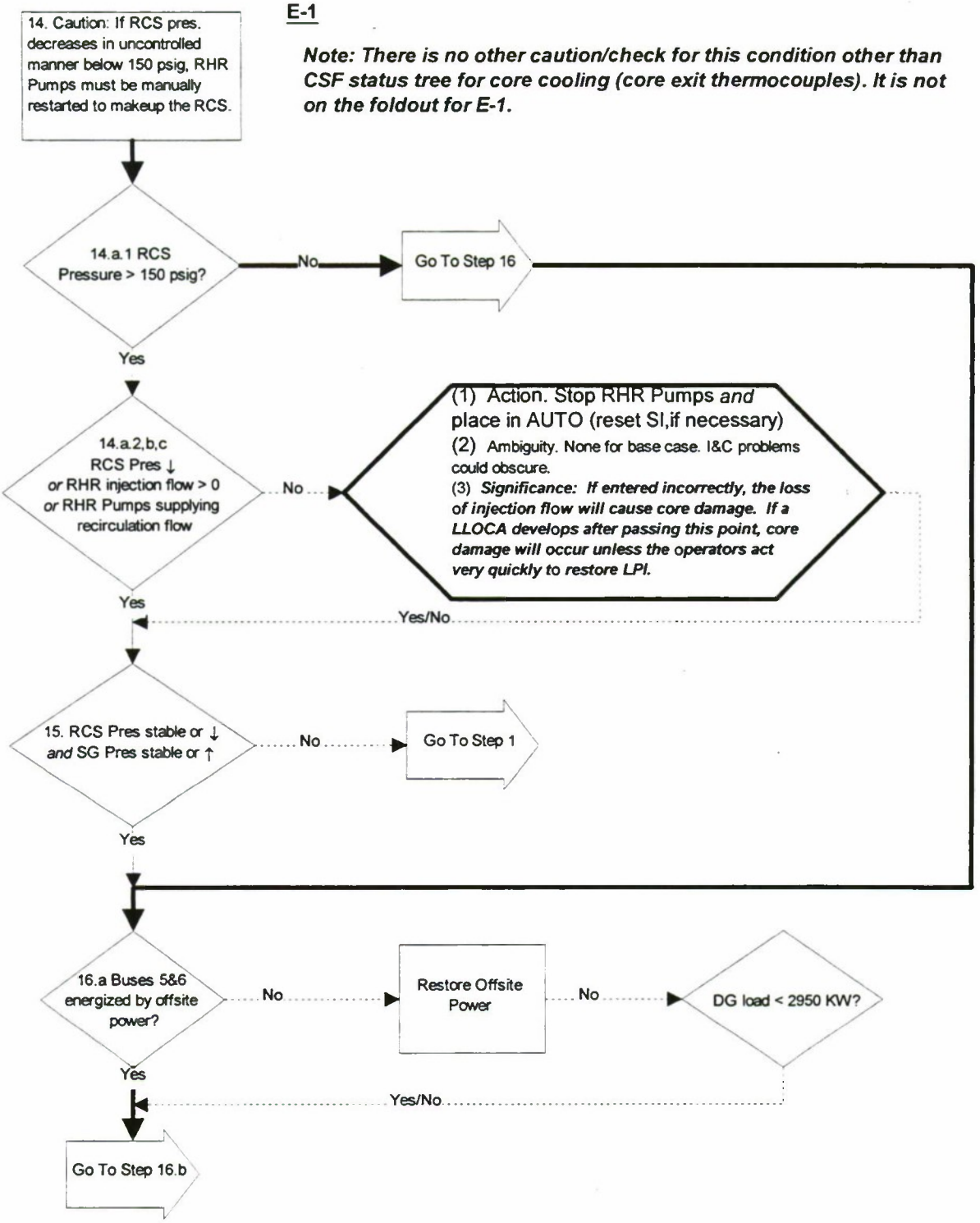


Figure C.13 EOP Map for Base Case LLOCA (Sheet 9)

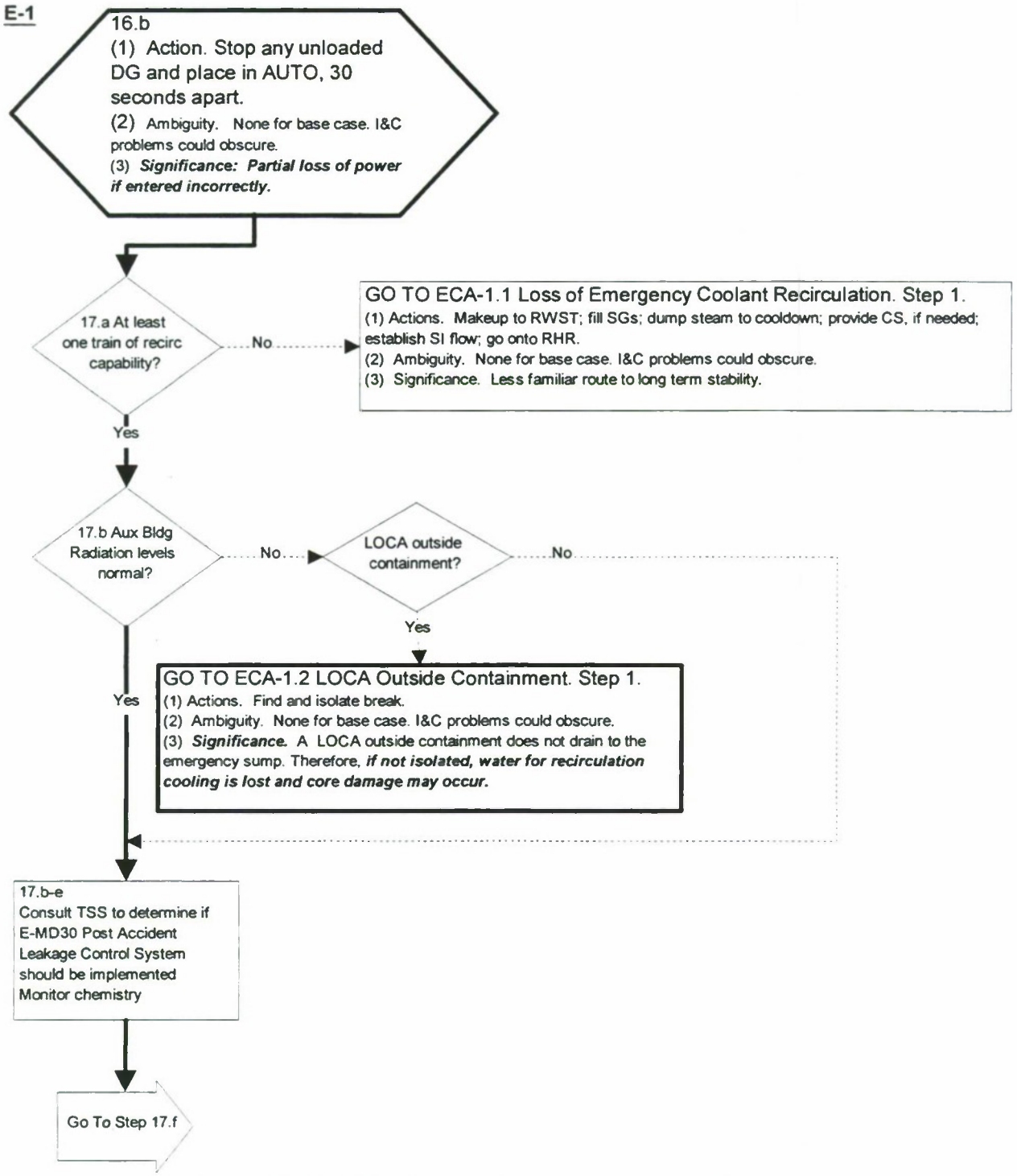


Figure C.13 EOP Map for Base Case LLOCA (Sheet 10)

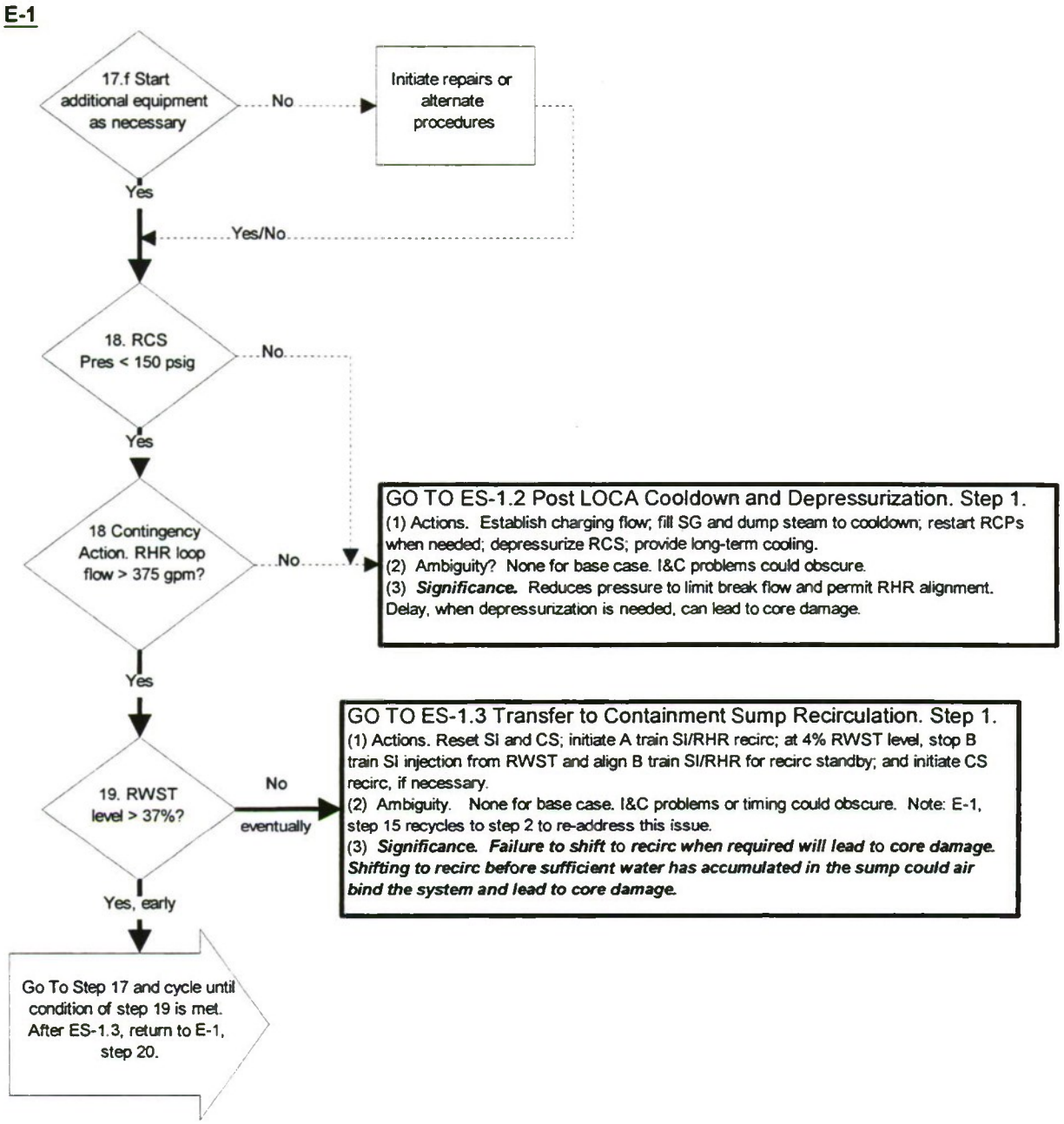


Figure C.13 EOP Map for Base Case LLOCA (Sheet 11)

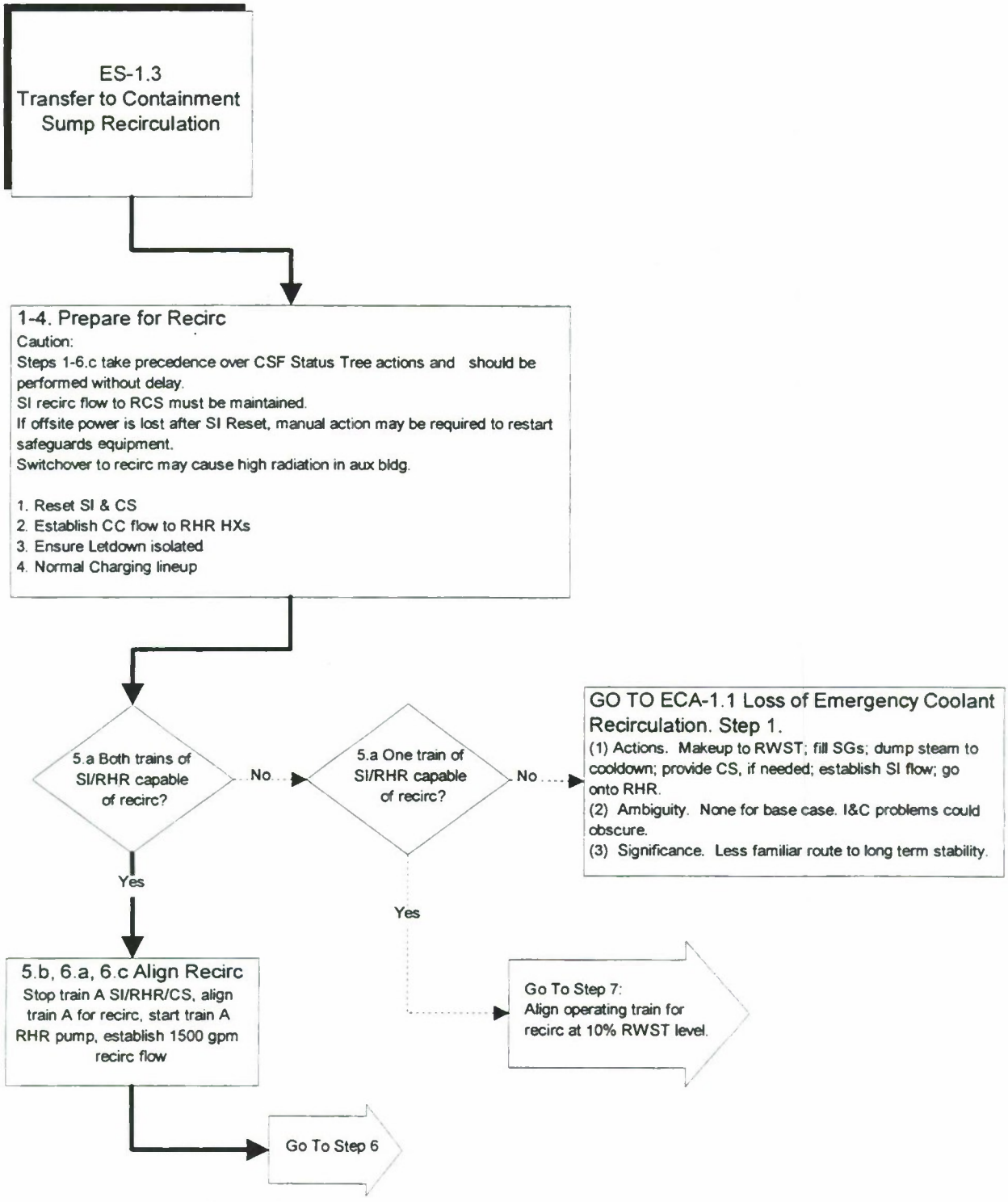


Figure C.13 EOP Map for Base Case LLOCA (Sheet 12)

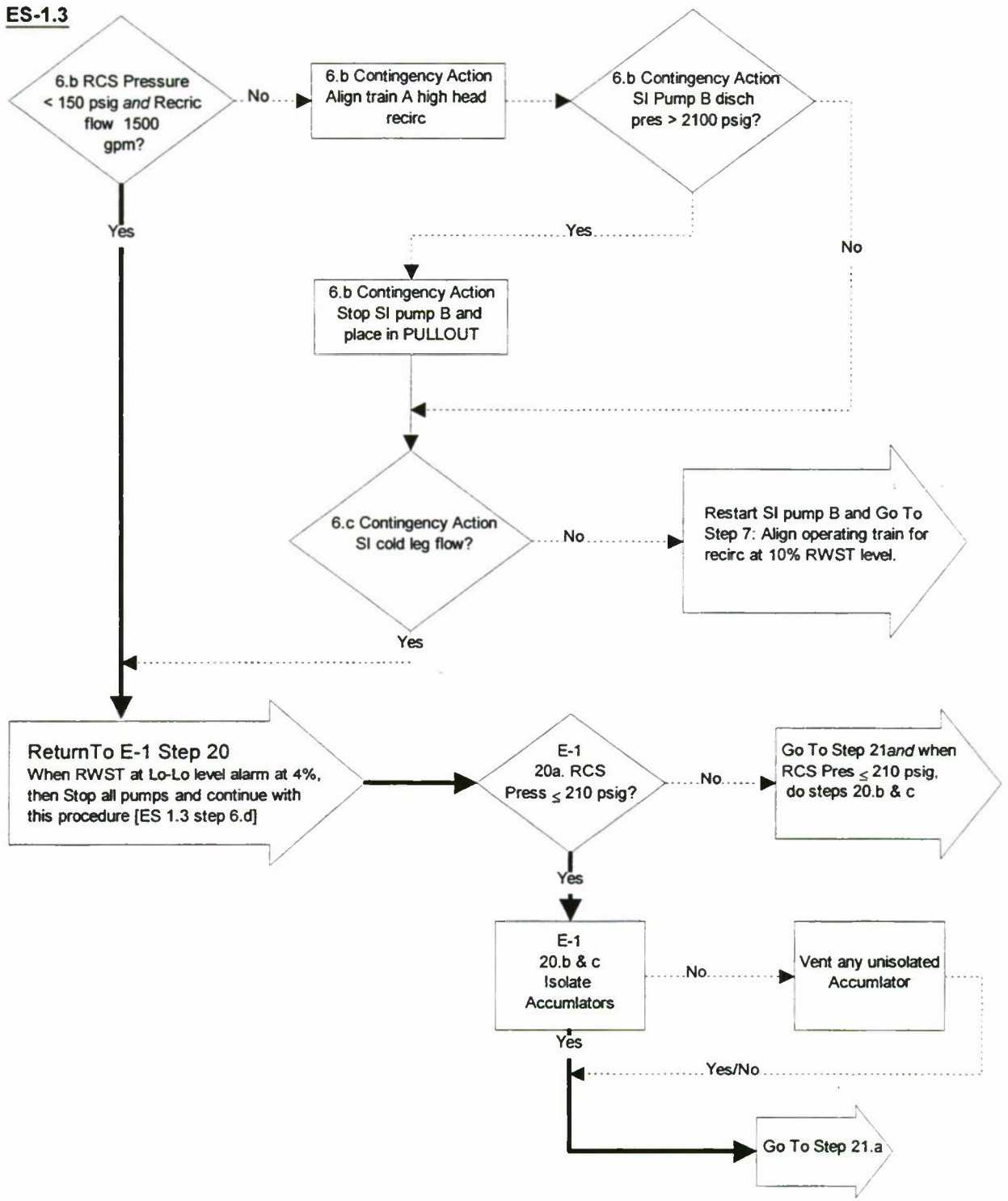


Figure C.13 EOP Map for Base Case LLOCA (Sheet 13)

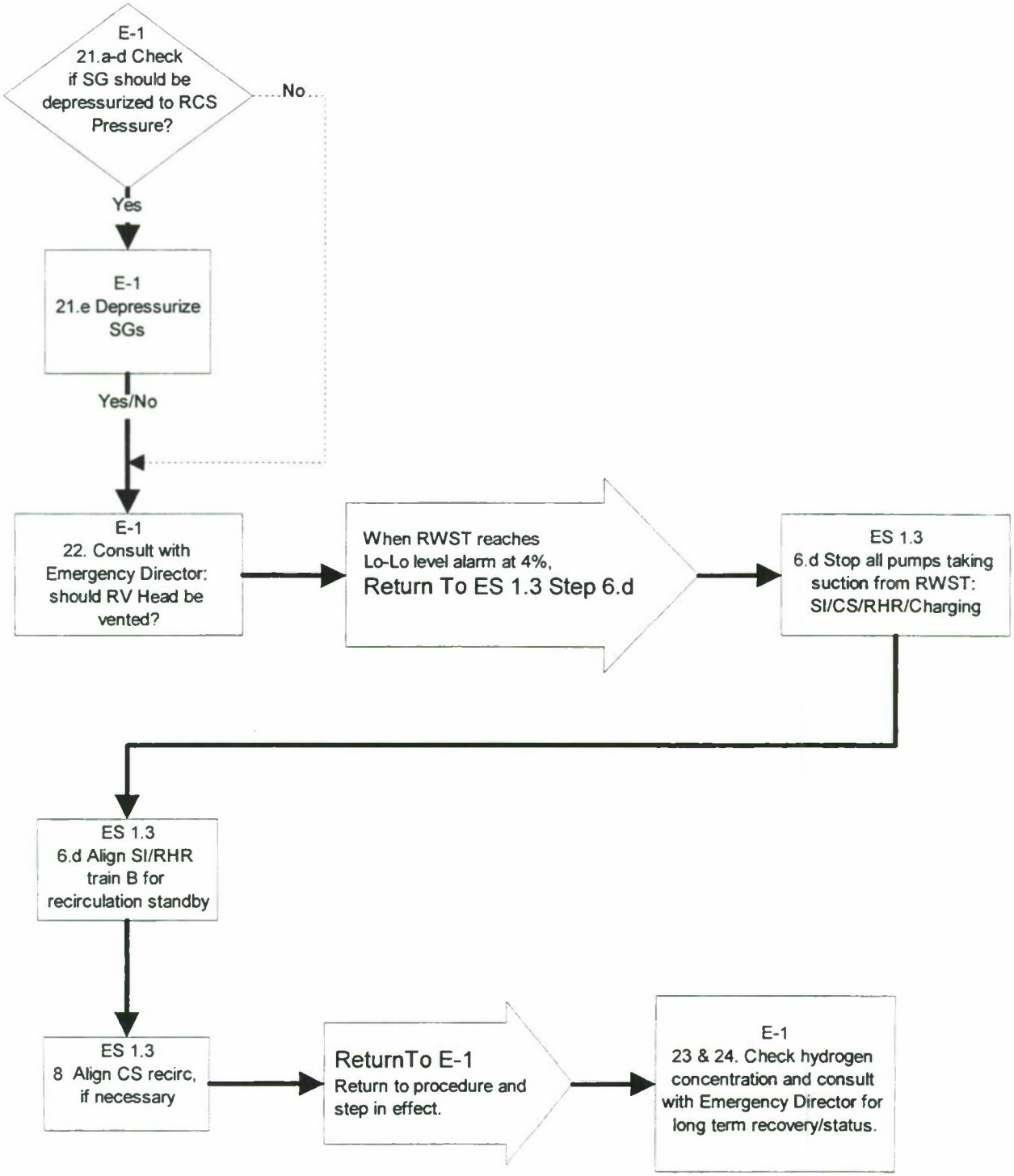


Figure C.13 EOP Map for Base Case LLOCA (Sheet 14)

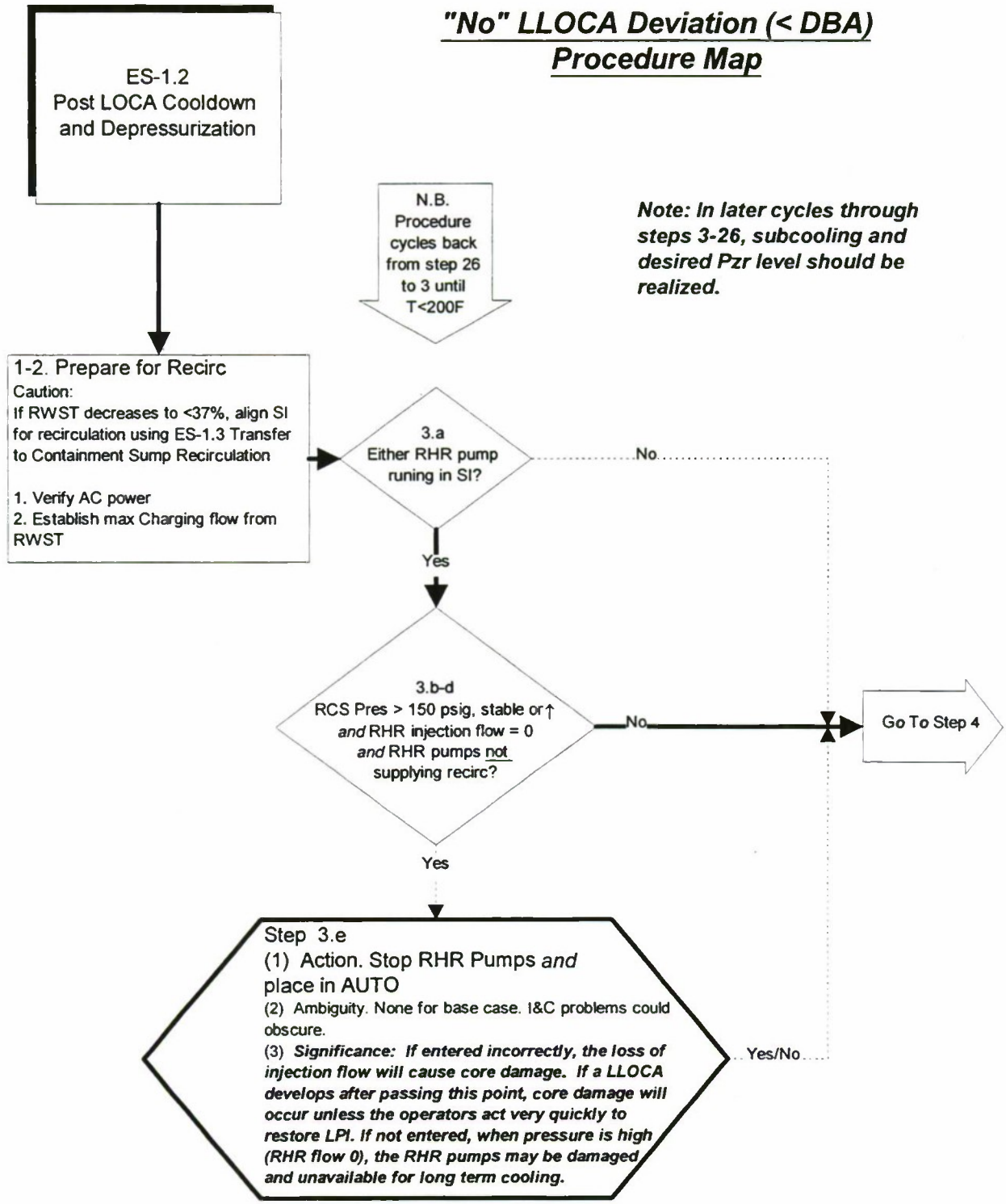


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 1)

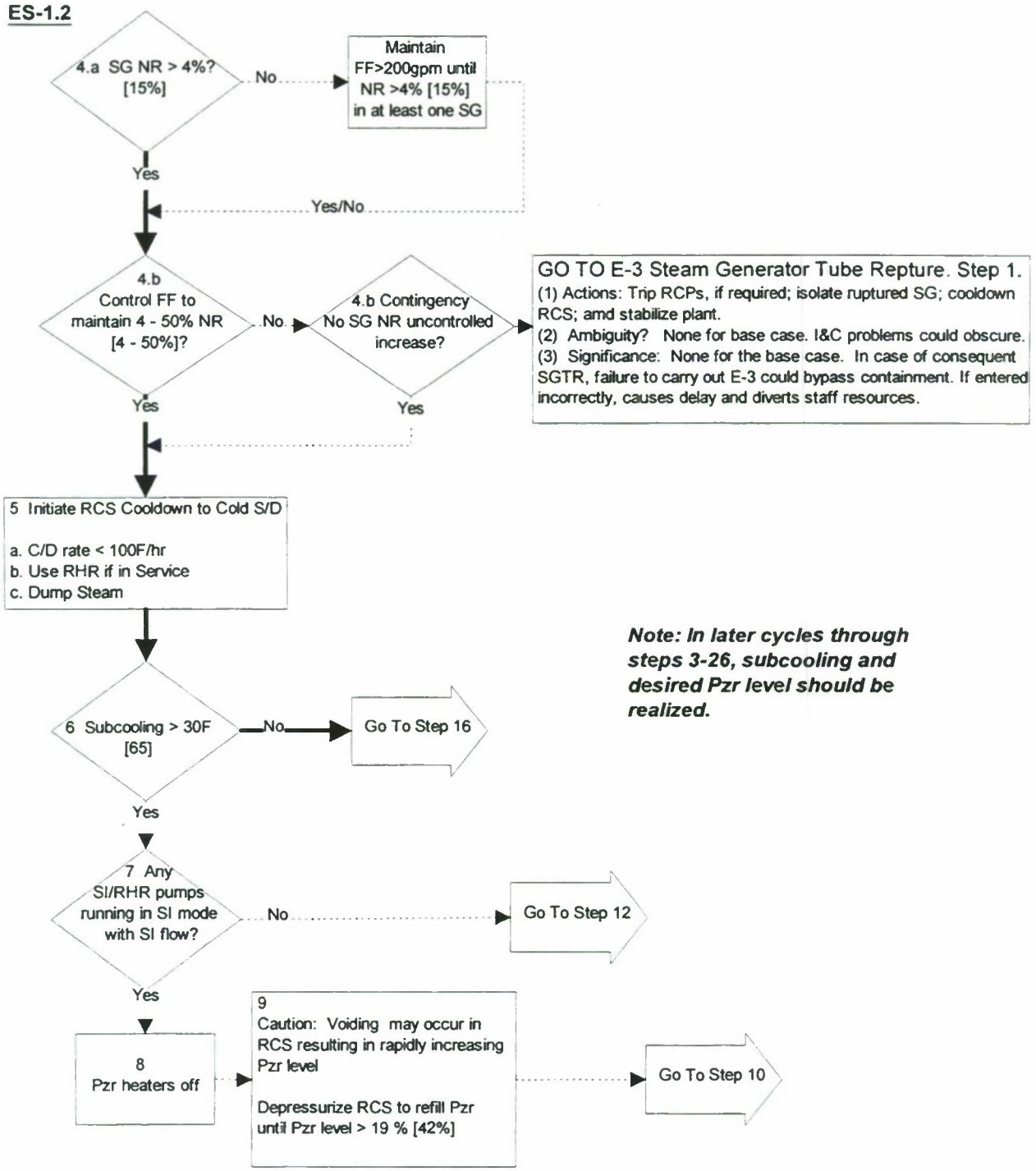


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 2)

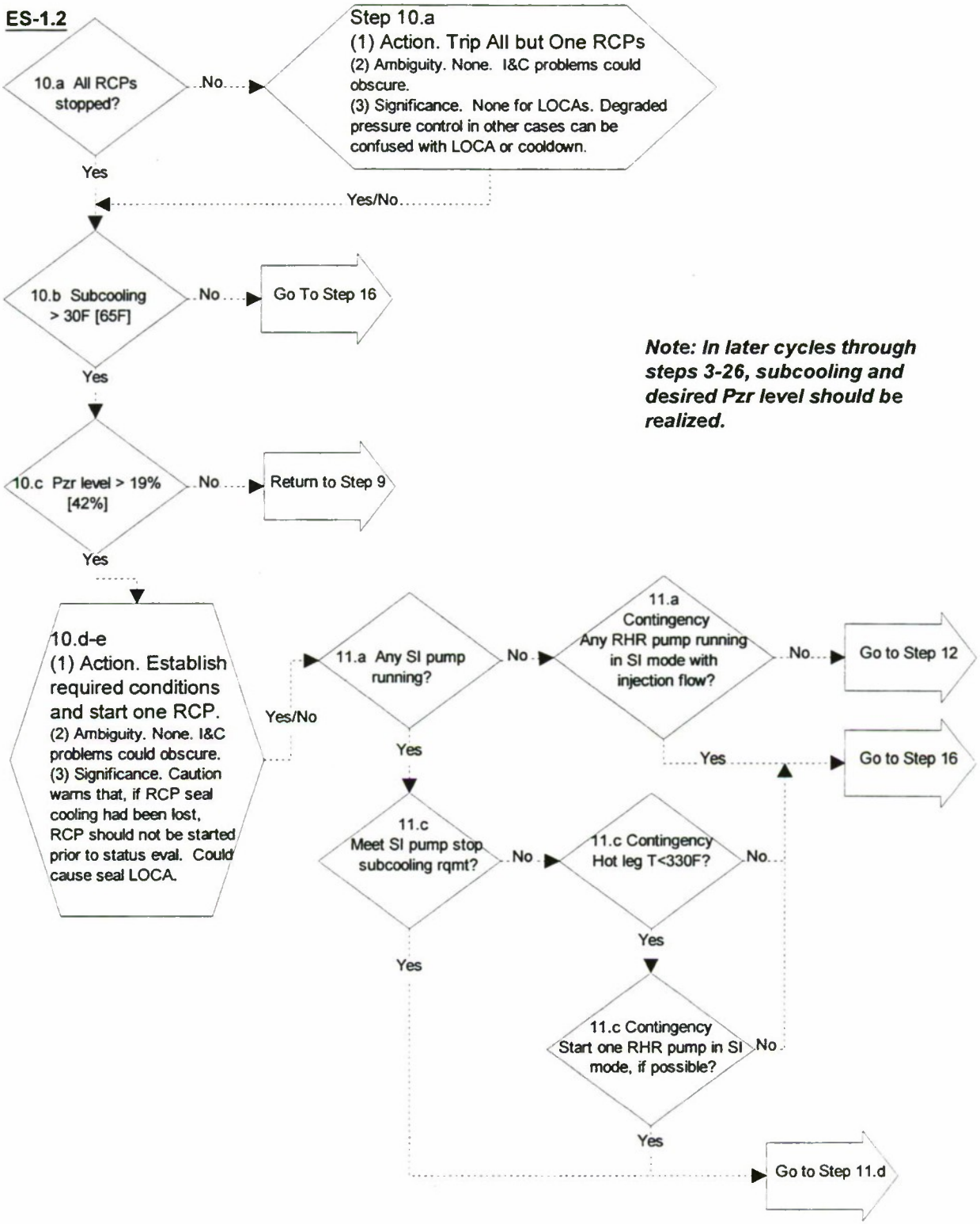


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 3)

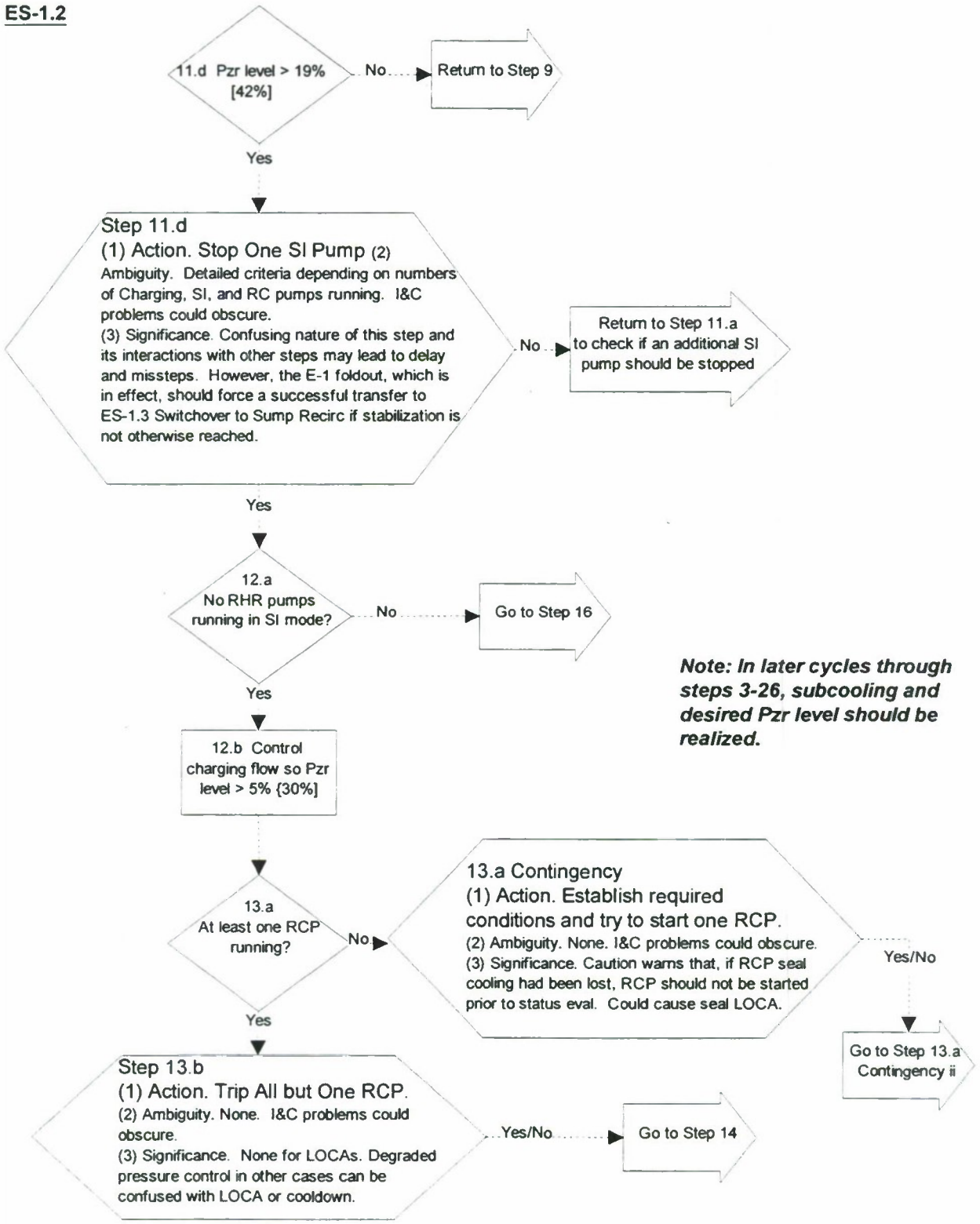


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 4)

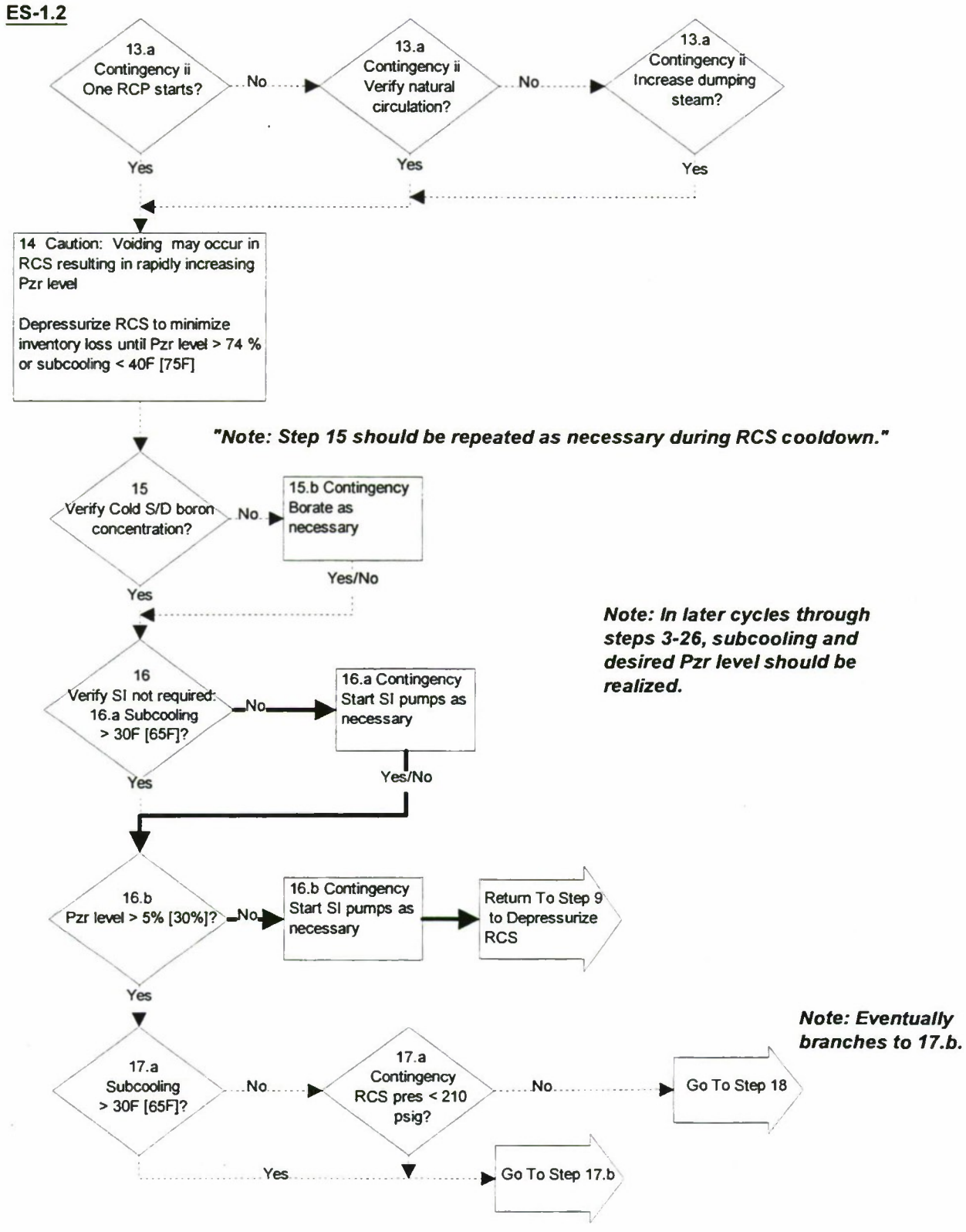
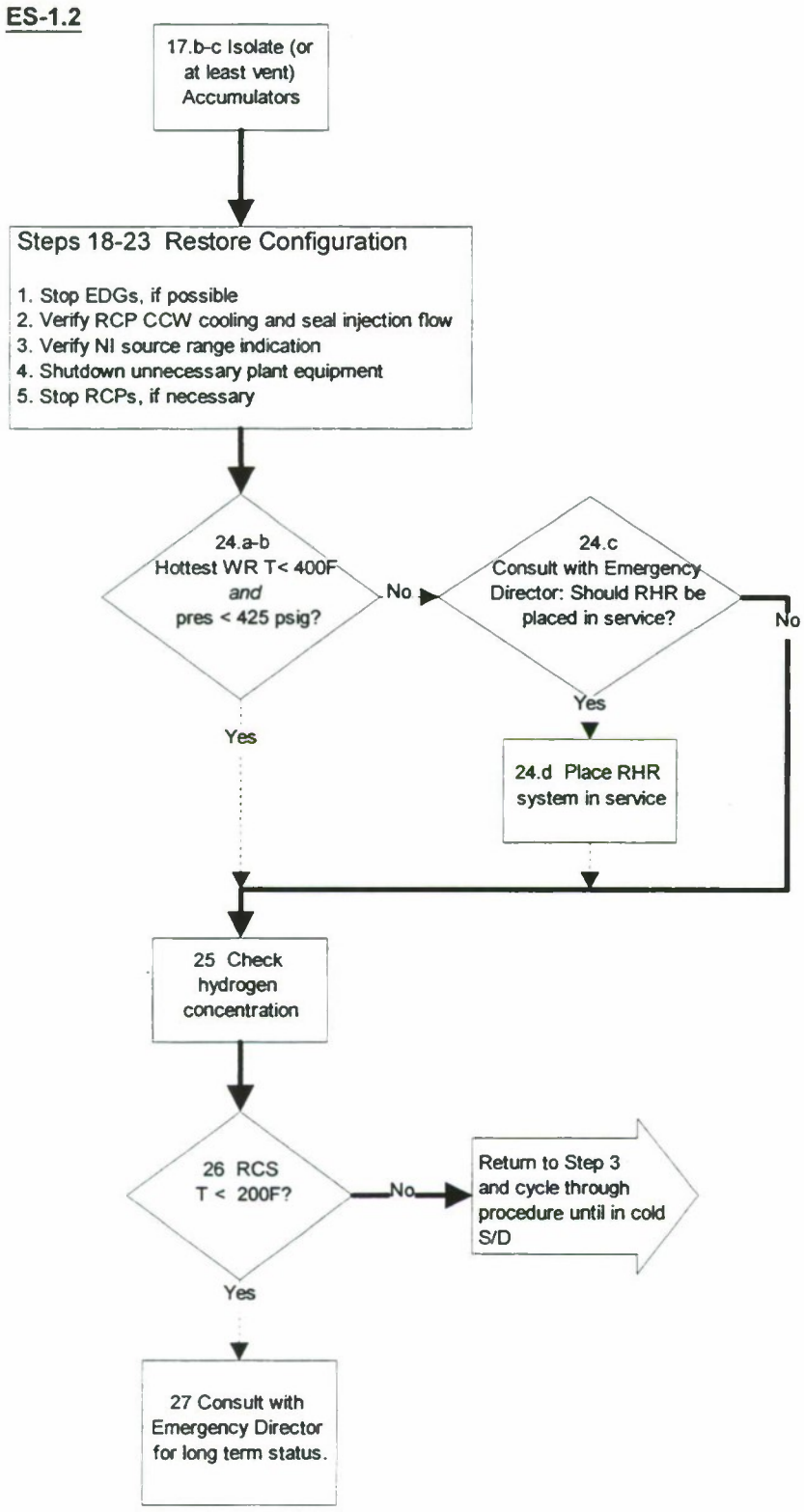


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 5)



N.B. If RWST level cannot be maintained, the system must eventually be placed on RHR or the E-1 foldout will require going to ES-1.3 Transfer to Containment Sump Recirculation, Step 1

Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 6)

APPENDIX D
ATHEANA EXAMPLE -
LOSS OF SERVICE WATER EVENT

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that would degrade the plant response in a boiling water reactor (BWR) during a total loss of service water. In particular, the objective is to identify whether there are any improvements that would better prepare operating crews to properly respond to a prolonged loss of heat sink. Service water provides the ultimate heat sink in this BWR-6 design and without it, plant equipment will fail over time and the plant status will continue to degrade, potentially leading to core damage if the heat sink is not eventually restored. Thus actions that operators can take to "buy time" and maintain safety functions until the heat sink is restored are vital to the success of mitigating such an event. This illustration of the use of ATHEANA serves to identify those circumstances (contexts) that might induce human actions that would inappropriately worsen the plant response to the event, even though the operating crew is attempting to perform the appropriate responses. Put another way, the purpose of this analysis is to identify the more likely circumstances and the resulting errors that might be performed that would worsen the plant response in a loss of service water event.

While this is a plant-specific example, however, the plant analyzed is a composite BWR, not exactly matching any particular installation. The example is realistic in that all specific design, procedures, training and operating and maintenance practice information used in the analysis have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate a similar issue at their plant. The example follows the steps discussed in the ATHEANA process in Section 9 of this document.

D.1 Step 1: Define and Interpret the Issue

In this example, the issue being analyzed is the following:

> A prolonged loss of service water event at a BWR, while relatively unlikely compared with many other types of transients, represents a severe challenge to the plant. It is also an event that provides a significant challenge to the operating crew since they need to continually take actions to deal with the progressively deteriorating nature of this accident. If service water is not eventually restored, damage to plant equipment and potentially the core are possible. This event most likely involves multiple active failures or unlikely passive failures and is therefore beyond the design basis of the plant. Thus, procedures and training are limited, as are investigations into the complexities of operator response.
>
> The objective of the analysis is to identify whether there are any improvements that would better prepare operating crews to properly respond to a prolonged loss of ultimate heat sink. To do this, the analysis will identify (a) the possible conditions that might induce the operating crew to inappropriately respond to a prolonged loss of service water event and (b) the more likely errors by the operating crew that might occur as a result of these conditions. The results of the analysis are to be used to make any improvements (procedure changes, training changes, human–machine interface changes) that would better prepare the operating crews to properly respond to such a severe event.

D.2 Step 2: Define the Scope of the Analysis

The scope of this analysis has been largely based on the description of the issue provided in Step 1 where the initiating event is defined as a prolonged loss of service water. In addition, the scope is purposely limited to a scenario that does not include additional, random failures since the event itself already provides for progressive degradation of equipment in the plant over time. In fact, a review of Table 9.2 in Section 9 shows that this event by itself has the characteristics of a high-priority initiator. With the exception of "short time to damage" and "high frequency event," the loss of service water contains all the other characteristics presented in that table, even without other equipment failures.

The plant's probabilistic risk assessment (PRA) already covers the loss of service water initiating event and estimates a resulting core damage frequency of approximately 2E-7/year. This assessment is largely based on equipment failures and does not address potential operator actions other than some key errors of omission, such as failing to use firewater as an injection source (to buy time) and failing to restore service water. The PRA does not address possible errors of commission that might occur and make things worse, as a result of responding to the conditions in the plant as they develop. This ATHEANA analysis examines the potential contexts and the likelihood of the operating crew carrying out unsafe acts due to those contexts during their response to the event. Acts of concern include those that would make conditions worse, thereby lessening the time available to restore the ultimate heat sink.

D.3 Step 3: Describe the Base Case Scenario

D.3.1 Introduction

This step of the analysis process defines a base case scenario for the loss of service water event from which to develop scenario contexts that may challenge the operating crew in ways that may be error forcing. As stated earlier, this analysis will not pursue additional random failures during the scenario, but will examine likely deviations as a direct result of the event itself. Ideally, the base case scenario has the characteristics shown in the first row of Table D.1; i.e., the scenario description represents a consensus of the expected plant response by most operators, it is well defined operationally, there are well-defined physics descriptions and adequate documentation of the plant response, and the scenario is realistic. The base case scenario for this analysis has the characteristics shown in the second row of Table D.1.

As indicated in Table D.1, there is no consensus operator model or safety analysis report-based (SAR) reference case for this event. Nevertheless, information summarized in the next subsection provides the essentials for understanding the loss of service water event based on the plant design, existing procedural guidance and related operator expectations, and the PRA. From this information, a realistic base case scenario is derived using additional judgment on the part of the analysis team.

Table D.1 Base Case Scenario Characteristics

Base Case	Consensus Operator Model	Well Defined Operationally	Well-Defined Physics	Well Documented	Realistic
Ideal	Exists	Yes	Yes	Yes	Yes
Loss of service water scenario	No single model exists although some general expectations do exist for the short term.	No, since the specific effects on equipment and the timing are not well known.	No, detailed analyses have not been performed to address a prolonged event. Limited calculations to support the PRA are available.	No, this is a beyond design basis event and so is not covered in the SAR. Limited information available in the PRA.	Will attempt to derive a realistic scenario based on limited operator expectations and information from PRA.

D.3.2 Understanding the Loss of Service Water Event

Plant Design

This BWR plant, as with many BWRs, has four service water systems that are relevant to this event. These are:

(1) A normally running closed component cooling water (CCW) system that cools recirculation pumps, reactor water cleanup coolers and heat exchangers, fuel pool heat exchangers, and the control rod drive (CRD) pump oil coolers.

(2) A normally running turbine building closed cooling water (TBCCW) system that cools most loads associated with balance-of-plant equipment, including various heater drain pumps, condensate and condensate booster pumps, main feedwater (MFW) pumps, main turbine lubrication oil and other coolers, generator primary water coolers, isophase bus and exciter coolers, hydrogen coolers, and service and instrument air compressors.

(3) A normally running plant service water (PSW) system, which serves as the normal ultimate heat sink and cools CCW, TBCCW, mechanical vacuum pump and steam jet air ejector coolers, drywell chillers, emergency safeguards (ESF) electrical switchgear room coolers, and various other plant chillers, among other equipment. It can back up most of the loads served by the standby service water (SSW) system (see below).

(4) A SSW system, which is designed to be the ultimate heat sink for loads during a loss-of-coolant accident (LOCA) or offsite power loss (which if lost, causes loss of the other three systems above). These include diesel generators, ESF electrical switchgear room coolers (backup to PSW), all emergency core cooling system (ECCS) room coolers, reactor core

injection cooling (RCIC) system room cooler, residual heat removal (RHR) pumps and heat exchangers and room coolers, control room cooling units, fuel pool heat exchangers (backup to CCW), CCW, drywell chillers (backup to PSW), and the service and instrument air compressors (backup to TBCCW).

While the specific ways to lose all service water will not be investigated in this step, it is observed that a loss of offsite power coincident with a common mode or other catastrophic failure of SSW provides one logical way that a total loss of the ultimate heat sink is possible. By virtue of the loads involved, the following represents a summary of the key potential effects of such a loss if it is not recovered following a prolonged period of time:

- loss of the balance-of-plant, including its isolation (i.e., main steam isolation valve closure on loss of condenser) with concurrent reactor trip
- eventual heatup of all the mitigating loads that are used to provide continuous core cooling and other mitigating functions (e.g., power, pumps, heat exchangers)
- various room and other area heatups such as the fuel pool, control room, drywell (containment), and the suppression pool
- loss of service and instrument air pressure throughout the plant
- may induce recirculation pump seal LOCAs due to the inability to cool the seals, resulting in a primary system makeup demand (albeit probably a small demand).

In summary, from the plant design standpoint, the dependencies on service water are great and a total and prolonged loss of the ultimate heat sink is a particularly challenging event.

Procedural Guidance and Related Operator Expectations

Besides the emergency operating procedures (EOPs), which will be discussed later, there are four procedures (which will also be discussed later) that specifically address individual losses of any one of the four service water systems (for SSW, the procedure addresses only losses of any one of the three SSW loops). The operators are trained periodically in the use of these procedures for short-term simulated losses and hence this training and the actions specified by these procedures largely define the expectations of the operating crew. In a total loss of ultimate heat sink, the operators would be carrying out, not only these procedures, but also the EOPs in parallel once the plant is tripped, in an effort to ensure that all plant critical functions (reactor power, reactor vessel level, containment conditions, etc.) are maintained.

The four procedures provide the symptoms (alarms and indications) used to recognize the loss, and can generally be described as requiring the operators to shut down or trip unnecessary loads and use alternative equipment or trains if possible, including alternately running equipment to extend its operation. More on these procedures and the EOPs can be found in Section D.5.4.

PRA Information

The PRA is among the best information sources available to gain insights as to a likely scenario progression. The base case scenario described in the next subsection is largely based on the PRA information and so that information will not be repeated here. However, two key elements from the PRA are particularly worth noting:

(1) The mitigating equipment for this event, with the exception of the diesel generators, heat exchangers, and similar devices (e.g., RHR heat exchangers for shutdown cooling, room air units), will operate continuously for at least a short period of time (at least 1/4 to 1/2 hour or longer) once it is started, depending on the size of the load and how continuously it and other service water-shared loads are needed. In other words, few components will fail almost immediately after they are started as a result of the loss of service water. This fact allows, for instance, for pumps to be run for a few minutes and then shut down, thereby performing an important function for a short period of time such as maintaining reactor pressure vessel (RPV) level. The diesel generators, however, are a counter example to this because they will fail in a potentially irreparable manner in just a few minutes without service water cooling.

(2) It is estimated that in about 4 hours, most areas of the plant (as a result of loss of room cooling) as well as the equipment throughout the plant (e.g., that requiring direct cooling such as pump seals) will be operating in temperatures that put the continued functioning of the equipment in serious jeopardy.

D.3.3 The Base Case Scenario

The possible scenarios in a prolonged loss of ultimate heat sink are dependent on a variety of factors not least of which are the specific operator actions regarding what equipment is used and for how long, as well as what equipment is secured during various times throughout the event. The following, however, highlights what is believed to be a reasonable chain of events which at a general level is a sufficient description of a base case and realistic plant and operator responses to a prolonged loss of service water. This summary and the accompanying representations of the key parameter indications observable to the operators shown in Figures D.1 through D.6 provide the expected "signature" of the event and indicate what the operators are likely to need to do as the scenario progresses. This progression does not include additional complexities (i.e., deviations) beyond those directly caused by the event.

- Initial Condition: The plant is operating at full power when a loss or degradation of service water occurs. This could happen abruptly due to events such as a loss of offsite power followed by complete failure of SSW. Degradation of service water over time could occur due to events such as valve or pump malfunctions or a breach in the PSW system, followed by a failure in SSW due to ice buildup in the intake structure or traveling screens (which could serve as a common mode failure for both PSW and SSW). Depending on the specific nature of the event, initial cues of multiple problems in the service water system (in CCW, TBCCW, PSW, SSW) may include low header pressure, signs of automatic starts of backup service water pump trains, and low surge tank levels, among others. Alternatively, the first

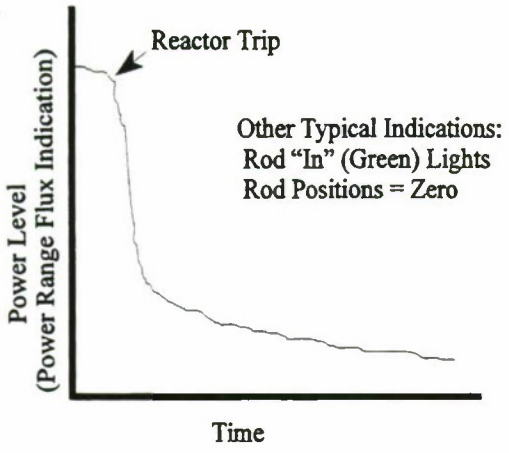


Figure D.1 Power Level vs. Time

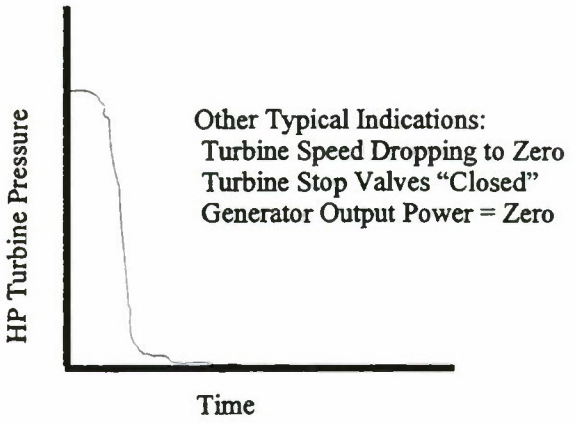


Figure D.2 Turbine Pressure vs. Time

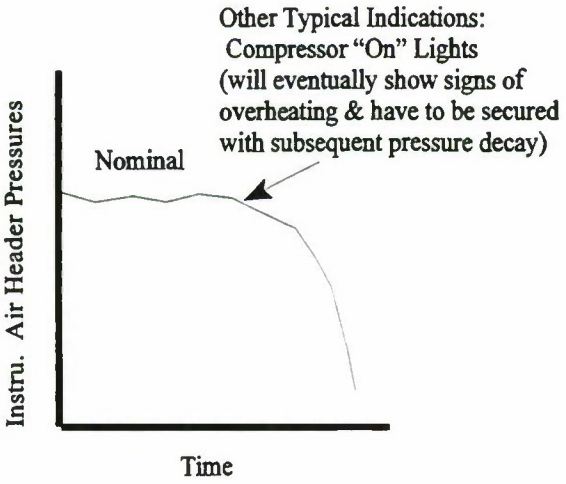


Figure D.3 Instrument Air Pressure vs. Time

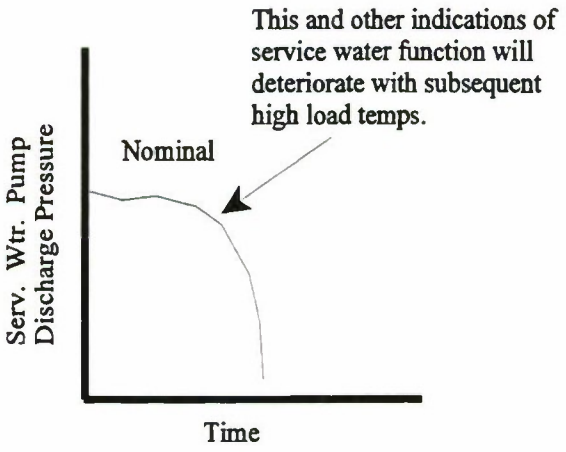


Figure D.4 Service Water Pressure vs. Time

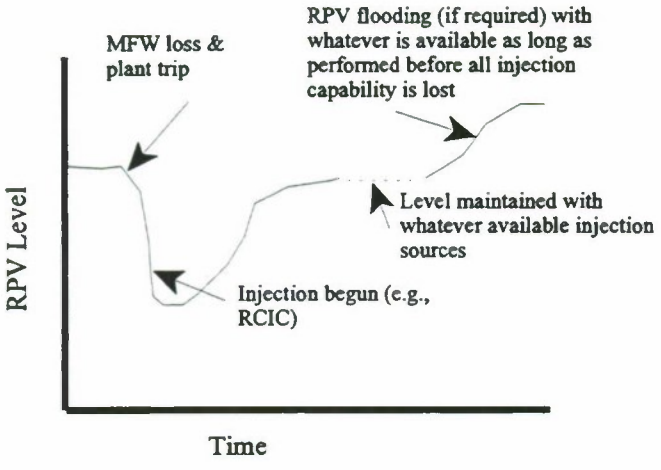


Figure D.5 RPV Level vs. Time

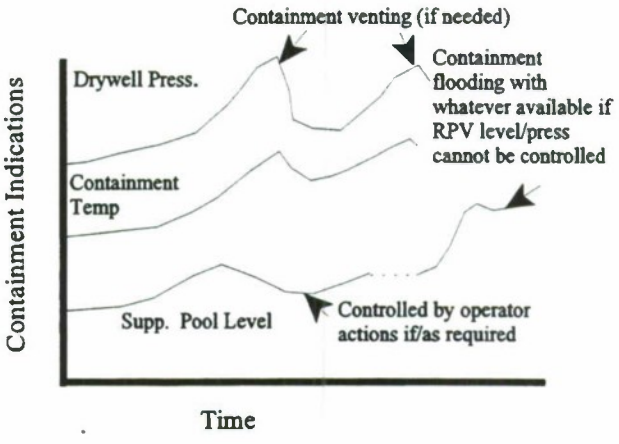


Figure D.6 Containment Conditions vs. Time

cues may be high-temperature alarms on the larger instrumented loads (e.g., recirculation pumps), as well as isolation alarms such as reactor water cleanup isolation or fuel pool heat exchanger isolation. The specific sequence of events cannot be predicted beforehand because it largely depends on the specific faults leading to the total loss of service water. However, and especially in a slowly degrading type of event, the operators will start hearing alarms and seeing indicators of various equipment problems that at first may not seem related or directly attributable to loss of service water. Some degradation of functioning equipment may occur before a plant trip finally results, either automatically or manually by the operating crew.

- Depending on what symptoms appear before the plant trip, the operating crew may already have begun following the steps in one or more of the four procedures for abnormal service water, including securing affected equipment, beginning to troubleshoot the nature and possible sources of the trouble, and eventually manually scramming the plant if required and if an automatic trip has not yet occurred. By the time of the trip, the operators may or may not have yet associated all the symptoms with the common problem of service water cooling.

- The larger loads and the associated service water systems that serve them are likely to develop the initial signs of degradation that finally require equipment shutdown and cause a corresponding plant trip. These are the recirculation pumps as well as all the many loads associated with the balance-of-plant and cooled by the PSW/TBCCW systems. For the base case scenario, the balance-of-plant is isolated either automatically or manually (main steam isolation valves (MSIVs) close) very early in the event (i.e., at or shortly after the plant trip) and all subsequent plant response is based on responding to an isolation-type transient with safety relief valve discharge to the suppression pool serving as the initial heat sink path for core decay heat.

- With plant trip, the operators enter EOP EP-2, RPV control, and by following EP-2 and other automatic and trained responses, they watch for and respond to, as necessary, the following plant conditions (not necessarily in order of priority) as the scenario progresses:

  (1) Reactor power decreases nominally following the reactor trip, as evidenced by the typical indicators and power (flux) time history shown in Figure D.1.

  (2) The turbine trips and the generator load is dropped, as evidenced by the typical indicators and turbine pressure time history shown in Figure D.2.

  (3) One possibility is that all electric buses continue to operate (including required bus transfers) and appear normal, based on breakers indicating "closed," available bus voltages and related indicators that are nominal; and expected operating loads operating as evidenced by current, flow, and similar readings. If the nature of the event has caused an automatic diesel start and there is evidence of lack of cooling to the diesel such as that due to lack of SSW operation, the diesels are supposed to be shut down quickly to protect them. Alternatively, loss of normal power could be a contributing factor to the total loss of service water. In this case, normal bus voltages and currents will drop until and if an attempt is made to run the diesels to restore power. Running the diesels without cooling presents a problem to be discussed later.

  (4) Instrument air, a support system, should be available for a short time, as evidenced by no change in header pressures shown in Figure D.3 and appropriate compressor "on" lights. This is because the compressors should only need to operate intermittently and the heatup of the TBCCW will require a little time to overcome thermal inertia. However, without compressor cooling, compressor failure or shutdown is expected and air pressure will degrade at a rate dependent on the leakages in the system and the demands for air.

  (5) As already alluded to above, service water systems are checked for signs of proper functioning, e.g., pump lights are "on," pump discharge pressures remain nominal over time, and service water load temperatures are nominal. These systems are likely to be already showing signs of trouble as discussed above and illustrated by Figure D.4. Some equipment may have already been secured by the operators. These indicators will continue to show signs of degradation as the scenario proceeds.

  (6) RPV level goes through a time history response typical of that shown in Figure D.5. This history is indicative of a loss and isolation of the balance-of-plant, including failure or shutdown of feedwater with early automatic or manual vessel level restoration via RCIC and/or the high pressure coolant system (HPCS). If a loss of offsite power is part of the event, HPCS operation will likely need to be interrupted or prevented due to a lack of cooling to the HPCS diesel. Safety relief valve (SRV) demands will occur to relieve pressure in the RPV, and pressure and level will be manually controlled by the operator as necessary.

(7) Containment conditions soon react to the loss of drywell cooling and the ineffectiveness of any attempts to cool the suppression pool via RHR due to the degrading service water conditions (see Figure D.6). Injection to the reactor vessel causes, through SRV operation, a rise in the suppression pool level and temperature. These containment conditions cause the operating crew to enter another EOP EP-3, containment control, in an attempt to keep these parameters within acceptable ranges. In the long term, this will not be possible and manual emergency depressurization of the primary system is called for. If or as conditions deteriorate, and once the containment pressure exceeds 20 psig, containment venting is to be performed.

(8) Low-pressure injection systems as well as high-pressure systems are used as necessary to maintain RPV level or flood the RPV if called for, as shown in Figure D.5. Each, however, is subject to failure eventually because of many conditions, depending on the specific system. These include rising suppression pool temperature, rising containment temperature and pressure, high room temperatures (including switchgear equipment), etc.

(9) Depending on the ability of the operating crew to alternate injection trains and extend their usefulness without damage, alternative injection systems may also have to be used to maintain RPV level or flood the RPV as shown in Figure D.5. Firewater lineup into the RPV, which requires local action over about an hour, can be particularly useful because it is independent of the loss of service water. However, without the ability to maintain service and instrument air compressors and with the eventual rise in containment pressure, maintaining SRV operation to keep the RPV pressure low for firewater and other low-pressure injection is jeopardized.

(10) Should the accident progress to the point that the ability to maintain RPV level and/or SRV operation is in serious doubt, containment flooding is started with whatever injection sources may be available (see Figure D.6).

(11) No radiation indicators or alarms are present, at least early in the scenario.

(12) Operators will be noting adverse indicators or alarms associated with ventilation problems and high temperatures in various rooms as well as the fuel pool.

- All the while, ultimate heat sink restoration will be being attempted.
- The technical support staff will likely be convened and the emergency plan enacted.
- At any time when the ultimate heat sink is restored and plant conditions can be restabilized, continued cooldown of the plant and shutdown of unnecessary equipment occurs.

Note that in the base case scenario, operating crew decisions and actions take place on a continuous basis in an attempt to deal with the deteriorating conditions. Some actions may be required

immediately, such as shutting down diesel generators before they are damaged. Most occur over time as decisions are made regarding what equipment to use and for how long. This is a "balancing act" between maintaining adequate core and containment conditions for as long as possible vs. shutting down or securing equipment to avoid its being damaged (perhaps irreparably).

D.4 Step 4: Define Human Failure Events (HFEs) / Unsafe Actions (UAs)

Based on the issue as defined in Step 1, part of the purpose of this analysis is to identify what the more likely HFEs/UAs may be in light of the changing plant conditions during the scenario progression. Hence, the HFEs/UAs cannot be defined a priori, but instead will be a product of this analysis. However, in general, the potential HFEs/UAs of interest all involve potential failures of the operating crew to "control" individual equipment items in a way that preserves their functionality for as long as possible and makes the best use of limited water, power, and compressed air resources so that the necessary safety functions can be maintained for as long as necessary. Actions such as securing systems from automatic control, manually initiating or backing up necessary automatic functions, stopping running equipment when considered necessary, operating equipment in unusual configurations, etc., are among the many examples of operator actions that may need to be performed if the loss of heat sink exists for hours. For example, operators may need to shut down diesel generators, start/stop/swap various injection trains to avoid serious overheating, disable undesired system starts, manually perform functions such as emergency depressurization, bypass automatic reconfiguration of equipment such as HPCS to the suppression pool (to avoid this "hot" injection source of water), etc.

A review of Tables 9.6 and 9.7 reveals that every functional failure mode category and example HFE may be applicable to the required operator actions in this scenario. This analysis serves to identify which HFEs/UAs appear to be more likely and under what circumstances their likelihoods appear to be the highest.

D.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

Given the already challenging nature of the scenario described, this step is the first involving the identification of those complexities associated with the base case scenario that introduce contexts that can make HFEs/UAs likely. While some deviations from the base case scenario may be examined as a result of uncertainties in the specific accident progression, deviations as a result of random equipment failures will not be addressed in this analysis. Consideration of characteristics of the scenario, formal rules and procedures, informal rules, operator tendencies and biases, potential procedural difficulties, and potential timing and workload are among the issues involved in identifying such complexities and deviations. This step reviews potential vulnerabilities with regard to these issues that may make HFEs/UAs likely.

D.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

Examination of Table 9.10, which addresses event types and related potential operator vulnerabilities, results in the following observations relevant to this analysis for this plant.

- The loss of service water event fits a class of events that are rare and not even anticipated during the life of the plant (i.e., beyond design basis). While there have been precursor events at a few plants where service water became severely degraded or even lost, it was recovered before a serious event ensued. Therefore, training is performed infrequently and only involves partial losses of individual service water systems. In addition, the simulated scenarios typically only cover the first half-hour or less in the accident progression to ensure that the symptoms are properly identified and diagnosed, and that the early required actions are performed. Attention is not spent on training for a prolonged and total loss of the ultimate heat sink, which would also be a difficult event to simulate due to simulator limitations. There are therefore only limited expectations by the operating crew as to what such a scenario looks like and the expected response of plant equipment and indicators. As such, the scenario represents a mismatch between expectations on the part of the crews and the existence of the scenario itself.

- Based on information presented in Table 9.10 as applicable to a loss of service water scenario, potential vulnerabilities could include:

  - unfamiliarity as to what to expect and therefore how to plan ahead in such a scenario
  - places where the procedures and other rules may not be appropriate or adequate
  - limited guidance on how to decide among alternative actions
  - the potential to have to coordinate among people in multiple locations

Based on the above observations, it should be the focus of the next step (Step 6) to identify scenario complexities and characteristics that test the potential vulnerabilities to determine whether HFEs/UAs are likely to occur because of these vulnerabilities.

D.5.2 Time Frames of Interest

As a further insight into the potential for HFEs/UAs to occur, four time periods in the scenario can be identified relative to potential operator influences. These are summarized in Table D.2.

The above summary illustrates that throughout the scenario (even pre-initiator), operators are continually involved in an attempt to first identify and isolate the problem and prevent a trip, and then to respond to degrading conditions throughout the scenario progression. They must also coordinate attempts to identify the source of the loss of heat sink and recover from it. If the event is not recovered quickly, more staff are likely to be called in, including the technical support staff. Emergency plan actions may begin. Environmental conditions will degrade as room areas heat up as a result of the loss of cooling. All of this is likely to result in increasing stress with resources potentially stretched to deal with the varied set of problems. Consideration of these observations about the scenario should be included in the next step (Step 6).

Table D.2 Relevant Time Frames for the Loss of Service Water Scenario

Time Frame	Major Occurrences	Potential Operator Influence
Pre-initiator	Alarms or indicators begin to show signs of trouble due to service water degradation Some equipment malfunctions may begin	Begin troubleshooting problem, attempting to find and address source of problem. Operators begin shutting down seriously affected equipment immediately.
Initiator	Loss of MFW and balance-of-plant Reactor scram or turbine trip MSIV closure now or soon after	The plant trip may occur automatically or the operators may trip the plant, depending on their observations regarding the equipment being affected.
0 - 10 minutes	Auto equipment responses occur (e.g., RCIC, HPCS start to restore level) Diesels may start if high drywell pressure present Containment isolation may occur now or soon	Operators verify or back up initial plant responses (particularly those that are automatic, such as lowering power level) per EOPs. If operators are aware of equipment high temperature or service water problems, they may need to quickly shut down or secure or even prevent some equipment starts.
>10 minutes	Equipment degradation occurs over time, room areas heat up, degrading containment conditions develop, etc.; critical safety functions are maintained for as long as possible by operators. If or when heat sink restored, restabilization and cooldown of plant occurs	Operators deal with equipment and plant degradation issues by alternating equipment operation, securing some equipment, using alternative systems, and performing many other actions necessary to respond to the event. Key core and containment cooling actions include maintaining RPV level and flooding it if necessary, emergency depressurizing if and when necessary, attempting to cool containment and venting it if and when are required. All the while, attempts are coordinated to restore service water. Technical support staff is convened and emergency plan commenced if recovery is not quick.

D.5.3 Operator Tendencies and Informal Rules

Many of the operator action tendencies summarized in Table 9.12b apply in this scenario because they describe what the operators will be attempting to do in response to parameter indications. Those actions that are most relevant as the situation continues to degrade, include:

- attempting to restore or augment loss of cooling water
- maintaining RPV level and not letting it decrease too fast or get too low by using various injection systems
- pressure maintaining low with SRVs, vessel vents, etc., especially after emergency depressurization

- attempting to prevent containment conditions from getting "too high" via the action tendencies shown

- preventing irreversible equipment damage by shutting down/securing/alternating operation whenever possible.

Using examples from the Table 9.13, at this plant a particularly relevant informal rule is that there is a strong tendency to follow and "believe in" the procedures. Experience has shown them to be capable of handling at most any situation, even though this scenario has not been trained for or simulated.

These tendencies, while good, do provide somewhat conflicting directions as to how the operators are to proceed. In particular, for this scenario, the last tendency listed above (prevent irreversible damage to equipment) is somewhat in conflict with the other tendencies to use the equipment to maintain safety functions. Specifically, while the four procedures for abnormal service water generally direct equipment to be shut down, the EOPs direct the use of mitigating equipment to the extent possible. These procedural and tendency differences could create so-called "double-binds" where the operators must choose among undesirable alternatives. Resolution of these issues as they arise is a potential vulnerability since the event will test the understanding of the crew as to the status of the plant and equipment; they will have to rely significantly on their cognitive skills rather than the skills involved in simply following procedures. In this case, the procedures conflict somewhat.

D.5.4 Evaluation of Formal Rules and Emergency Operating Procedures (EOPs)

This evaluation looks for vulnerabilities associated with ways the emergency operating procedures (EOPs) and other formal rules may lead operators to HFEs/UAs. In this case, the EOPs and the four procedures provide the primary inputs that will guide the operators' actions when responding to a loss of service water event. This examination is developed by tracking those portions of these procedures that are most germane to the scenario.

Figures D.7 through D.9 display in very simplified flowcharts the major actions called out by the various procedures once the scenario progresses past the initial power reduction, which is assumed to be successful. Note that these flowcharts are not meant to duplicate the procedures. However, they do highlight the most significant cues called out by the procedures and the actions to be taken. In particular, the hexagon shapes represent places where equipment is terminated. These and other places in the procedures represent possible vulnerabilities where it may be more likely for the HFEs of interest to occur, thereby jeopardizing the scenario outcome.

Review of the above procedures for potential vulnerabilities that might lead to HFEs/UAs suggests the following observations:

- From an overall perspective, and as already mentioned in Section D.5.3, some potential conflicts are set-up among the procedures. The abnormal service water procedures call for shutting down equipment, while the EOPs require equipment to be used to maintain safety functions.

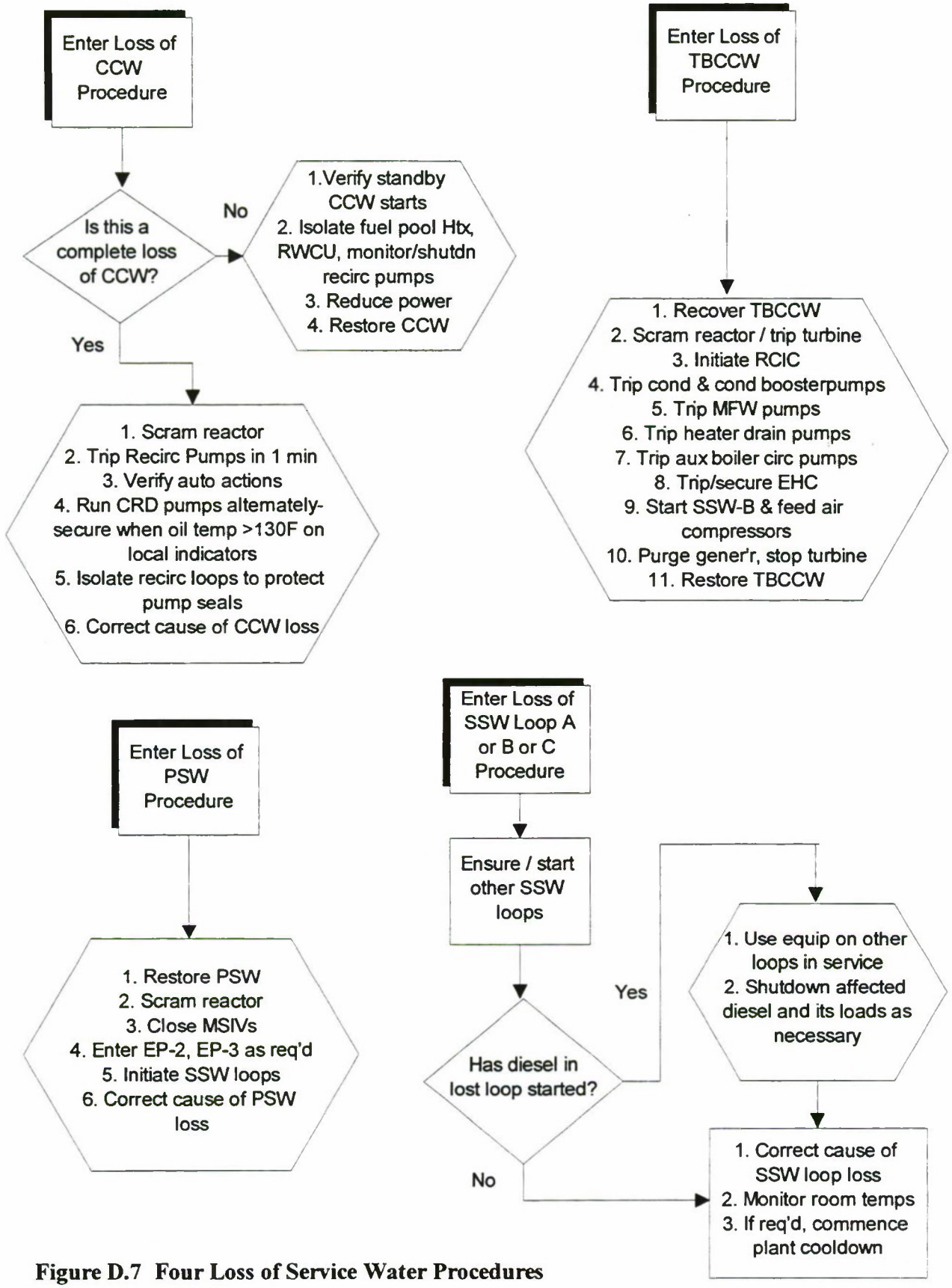


Figure D.7 Four Loss of Service Water Procedures

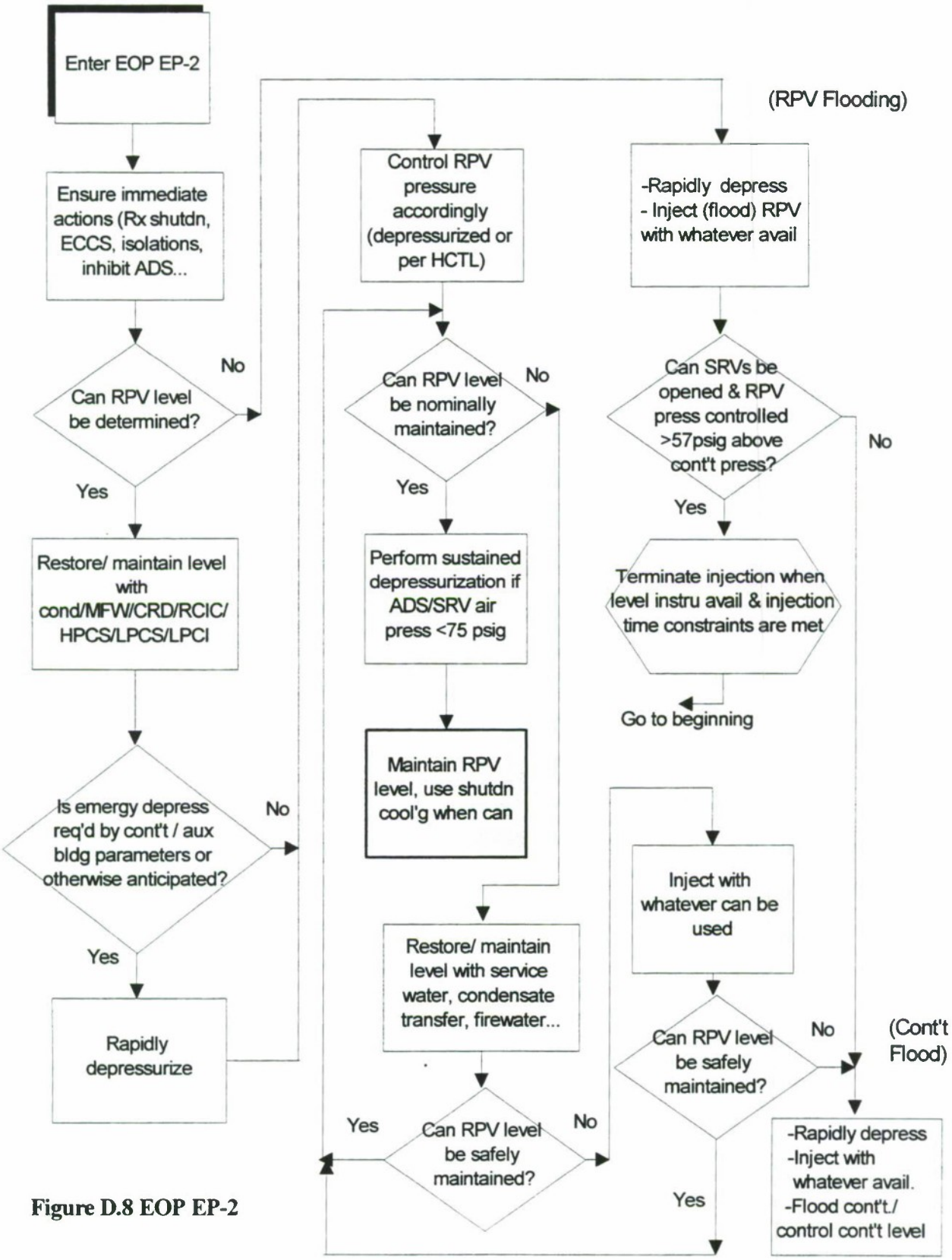


Figure D.8 EOP EP-2

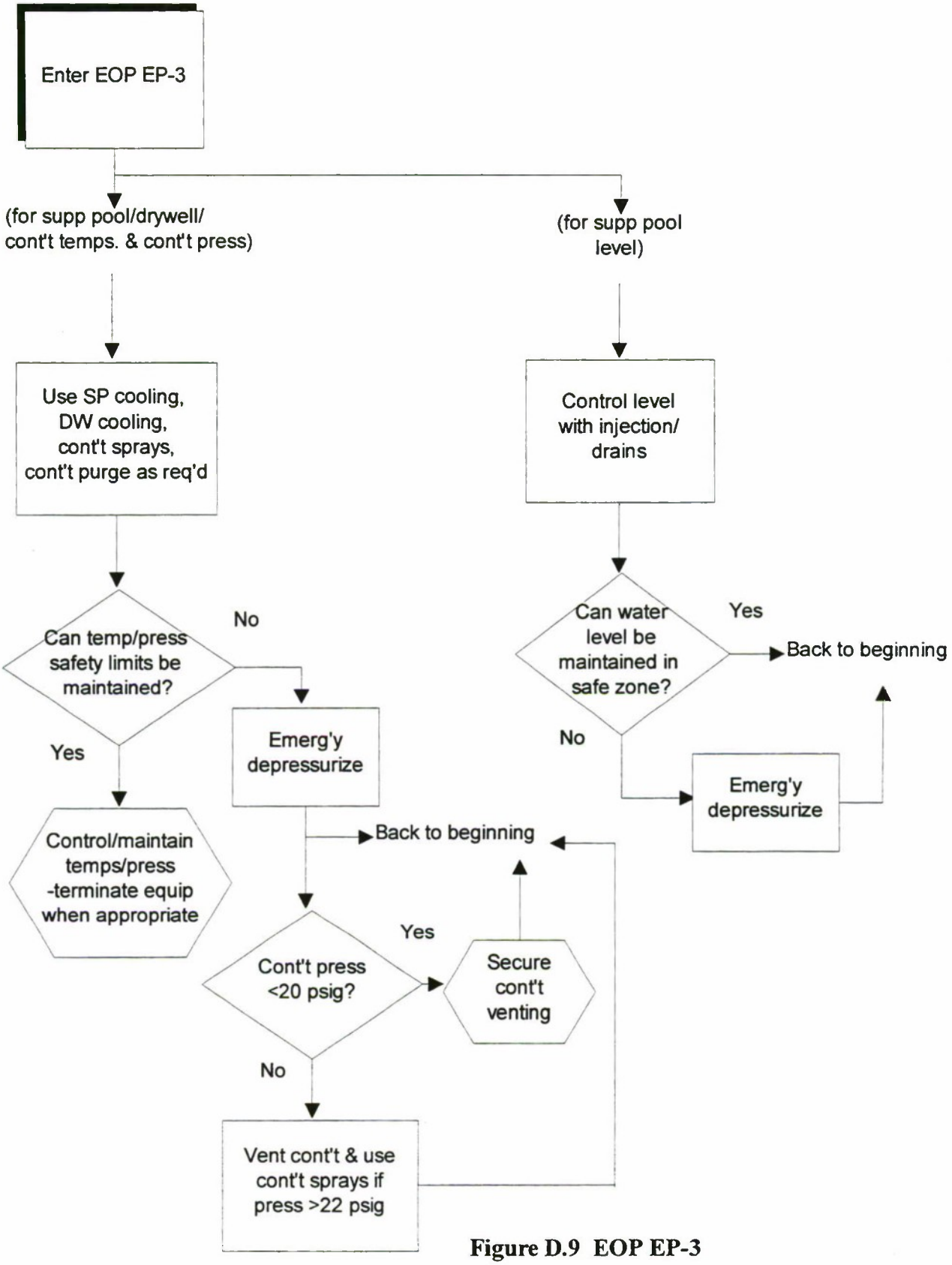


Figure D.9 EOP EP-3

- No specific procedure exists for loss of all three loops of SSW; thus the operators will have to cognitively extend the use of the Loss of SSW abnormal procedure, while also attempting to follow the EOPs.

- If a loss of offsite power were involved and SSW were to completely fail, operators would be presented with the choice of shutting down diesels to protect them and forcing a station blackout, or running one or more diesels to power equipment (preferred actions are not indicated in procedures).

- If diesels start (e.g., from high drywell pressure) with offsite power available, diesel shutdown should be performed but must be done quickly to avoid irreparable damage.

- Failure to shut down or, if appropriate, extensively cut back the use of running or automatically started equipment during the initial and later phases of the accident could damage the equipment so that its later use cannot be relied upon. Indications of impending equipment damage may occur late or not at all, creating ambiguous criteria as to when to start or restart equipment, how long to run it, and when to shut it down.

- Restoring or maintaining RPV level will be the likely first safety function challenge for the operating crew and will require quick decisions and unambiguous communication among the crew, as to which equipment to start and let run (and for how long), and which equipment to shut down or secure, even if automatically started. Failure to maintain this function could lead directly to core damage.

- Responding to higher containment temperatures and pressures will also be an early challenge for the operating crew and will also require unambiguous communication among the crew as to which equipment to start, when, and for how long; and which equipment to shut down or secure even if it was automatically started. Whether systems that can cool either the core or containment (e.g., RHR), depending on the alignment, should be preferably used for core cooling or containment cooling may also be an issue for which no procedural guidance is provided.

- Air pressure will likely deteriorate if the compressors are not or cannot be run by the operators periodically. This could severely hamper the ability to emergency depressurize and maintain depressurization, especially if SRV operation is not managed so as to avoid using up any backup or bottled air sources. Operators will need to be aware of this issue because loss of the ability to depressurize and maintain pressure control could lead to core damage.

- Failure to defeat unwanted or undesirable alignments such as RCIC switching to the suppression pool for suction (pool temperature will get high due to lack of RHR-SSW cooling) could result in equipment damage and the inability to operate the equipment, if needed later.

- Failure to take other desirable measures such as using portable room cooling, refilling the condensate storage tank if needed, dropping unnecessary electrical loads, and arranging a temporary means for cooling water to vital loads could cause losses of air, water, and power (consumables) needed to respond to the event.

- As a final and general observation, having performed this review, it appears that many of the characteristics of the scenario are similar to a station blackout (SBO) for which this plant has a procedure; by carrying it out, the plant can supposedly cope for up to at least 4 hours. However, in this case, some or all of the power may be available and so the operator needs to be more involved with shutting down equipment to "save it for later" if needed. In many ways, it seems the SBO procedure would be applicable, but with modification. As of now, no specific guidance is available as to equipment priorities, timing of desirable actions, other unusual actions to take, etc.

D.5.5 Summary of Potential Vulnerabilities

Based on the information from this step, Table D.3 summarizes potential vulnerabilities that may make HFEs/UAs by the operating crew plausible. These are addressed further in Step 6.

D.6 Step 6: Search for Deviations from the Base Case Scenario

The scenario being analyzed already represents a significant deviation from operating crew expectations; in fact if it were to occur, disbelief could be an initial natural reaction. Without additional complexities, such a scenario is already quite challenging and in light of the identified vulnerabilities, offers a number of instances for the crew to perform unsafe acts. Because of this, deviations from the base case scenario considered in this step will generally not include such issues as random equipment faults or indicator failures because it does not seem these would be necessary to make the scenario sufficiently error forcing. However, potential deviations of the scenario itself and how it might progress will be considered in the following searches to see if certain circumstances can lead to strong error-forcing contexts.

D.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

The search for possible scenario deviations is begun by first considering deviations in the initiating event itself as well as in the scenario as a whole. In this case, a useful approach is to apply guide words typical of hazard and operability analyses to investigate differences in the way the initiator or scenario might proceed.

Table D.4 demonstrates the possible deviations that have been considered in this search. The types of initiator or scenario deviations that seem to have the most potential for inducing HFEs/UAs involve a somewhat slowly degrading type of initiator that may provide diagnosis problems at first, while at full power with the highest heat loads. The possibility of a demanded SRV sticking open, thus, quickening the necessary responses and placing a greater demand on RPV injection, is also of particular interest. The combination of these characteristics may make for the most challenging event and it is this combination that is reviewed further in Table D.5.

Table D.3 Summary of Potential Vulnerabilities for Loss of Service Water

Consideration	Observation	Vulnerability/implication
Training, experience, expectations	Has never happened (though some precursors at other plants); seems impossible	Disbelief (mismatch from expectations)
	Limited training on lesser losses of water cooling systems individually. No training on prolonged total loss (beyond design basis accident)	Unfamiliarity Limited procedural and other guidance Multiple location coordination required
Timing considerations	Signs of trouble and equipment malfunctions may occur for a time before trip	Failure to diagnose cause early could affect future decisions Failure to shut down affected equipment could cause additional problems
	Diesels may start	If need emergency power, there is no specific guidance as to shutdown vs. operate any of them
	Equipment and room areas will degrade over time	Need to intervene considerably; trying to maintain safety functions with limited equipment use and no specific procedural guidance
Tendencies or informal rules	Tendencies exist to recover and maintain safety functions and prevent irreversible equipment damage	For this scenario, tendencies oppose each other, requiring careful balance
	Crews follow procedures	Abnormal procedures tend to oppose needs of EOPs. Clear procedural guidance not available
Formal rules/procedures/EOPs (for observations not covered above)	Involves a total loss of service water, including all SSW	No specific procedural guidance for loss of all SSW
	Decisions as to what equipment to run, stop, when, and how long	No specific guidance. Will require strong coordination and communication
	Consumables (air, water, power) in jeopardy long term	Must manage and anticipate without specific guidance
	Need to take other desirable actions and prevent undesirable equipment alignments or starts	Limited guidance
	Some similarities with SBO	SBO procedure maybe helpful, but needs modification "on the fly"

Table D.4 Loss of Service Water Initiating Event / Scenario Deviation Considerations

Guide Word	Possible Physical Deviation	Significance	Carry Forward in the Analysis?
No/not/never	Initiator - N/A Scenario - N/A	Relative to the initiator or scenario, "no" loss of service water eliminates the initiator and so there is no scenario. Use of this guide word is not applicable.	No.
More/early/ quicker/ shorter	Initiator - abrupt loss Scenario - coincident LOCA requires quicker responses	The base case scenario did not give the specifics of the initiator. The loss could be total and abrupt. It is not clear that such a loss changes the time or nature of the response significantly enough to be a concern, with the exception of requiring a quick shutdown of the diesels. A total abrupt loss may be easily identified based on the numerous alarms that would all come in at once. The demands on the plant and operator response will be the quickest if the pre-initiator plant condition is full power with greatest heat loads. A simultaneous LOCA or similar event would also "quicken" the scenario, but the coincident probabilities are considered too low, with the possible exception of a stuck-open SRV or RCP seal LOCA.	See below. Also, significant RCP seal LOCA not likely and should be isolated by procedure, anyway. Stuck-open SRV adds an additional challenge for earlier and more continuous injection.
Less/slower/ longer/late/ partial	Initiator - Service water is not totally and abruptly lost initially, but is only partially or slowly lost over time Scenario - low power level and heat loads	For the initiator, this is a possible situation in which it may be harder to detect and identify the source as well as the extent and nature of the problem. Such a situation might delay diagnosis of the problem and responses to the effects. The scenario and related degradation could occur slower, especially at low power levels and corresponding heat loads.	Combination of slower or harder to detect initiator while at full power seems to provide the most challenging event.
Reversed/ repeated/as well as	Initiator - Service water is apparently restored, but it is still not sufficient or is lost again (repeated) Scenario - N/A	For the initiator, this is a possible situation that could add confusion as to the extent and nature of the recovery. Such a situation might enhance the chances of operating more equipment simultaneously, only to have to respond again to the repeated service water loss.	No. Probabilistically too less likely overall than above.

Table D.5 Results of the Loss of Service Water Initiating Event/Scenario Deviation Analysis

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Service water is not totally and abruptly lost initially, but is only partially or slowly lost over time while plant at full power. Recovery is not forthcoming, requiring operators to decide on what equipment to run when, etc. as the situation continues to degrade. A stuck-open SRV during the event places a greater early and continuous demand for injection.	No or smaller change in parameters than expected. (No indication or slower or smaller than expected changes in plant parameters occur at first due to slowly degrading situation.) Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. [Starts as partial loss of service water (expected) but could degrade and become a total loss and hence more severe] Familiarity and simple expectations about the event need to be overcome if the situation changes. (Situation could start as partial loss and become total loss, perhaps unexpectedly, requiring the situation assessment and response change.) Scenario contains dilemmas and response contains double-binds. (Undesirable alternatives such as stop equipment to "save it" vs. operate equipment to maintain safety functions, both per procedures, may setup delays in the response, reluctance or cautiousness, anxiety and stress.) Scenario has many side effects that take time to develop. (There could be fixation on immediate problems and insufficient planning for what is to come.) Delays in changes of parameters may cause events to be a surprise as there is limited knowledge as to what to expect and when. (Equipment degradation may not be indicated and alarmed right away but be delayed.) Scenario may require high tempo/multiple tasks at times adding to anxiety and stress. (Potential for simultaneously indicating problems and some necessary quick responses such as shutting down diesels could add to anxiety and stress.)	May take no action or delayed action to prevent further degradation of service water or respond to its effects due to lack of awareness, at first, as to nature of problem. Could believe situation has stabilized with some service water flow and thus be caught off guard when total loss occurs; potentially missing some necessary immediate actions such as shutting down diesels or loads. Wrong or inappropriate actions could be taken or needed actions could be taken too late, regarding which equipment to operate or shut down, when to do it, for how long. Could result in unnecessary equipment damage or safety function degradation. Note that the overall strategy decision as to how to respond could be an important and potential error (e.g. fill vessel and depressurize early vs. maintaining status and waiting for procedural cues). Insufficient planning may exist as to what may happen next, as well as in the longer term, so that best response and use of resources (equipment, consumables, staff) is not achieved. Anxiety and stress, should scenario seriously degrade, could disrupt coordination efforts and challenge communication among staff so that actions are taken by individuals without full knowledge of entire crew.	Yes. Should carry forward. Many error mechanisms are potentially triggered by this possible scenario.

Table D.5 summarizes more specifically how the above combination might trigger relevant cognitive processes, error mechanisms, and related error types based on a review of Tables 9.15a and b as well as 9.16a and b, in ways that might induce HFEs/UAs of concern. For the possible physical deviations being considered, the contents of Tables 9.15a and b and 9.16a and b that are the most relevant are shown in the second column of Table D.5. The third column of Table D.5 summarizes the potential errors (HFEs or UAs) that could occur given the general error types provided in those tables.

D.6.2 Search of Relevant Rules

This portion of the analysis examines whether unsafe acts could be induced as a result of deviations from the base case scenario so that incorrect procedural guidance or other rules are followed, or the prescribed actions can be applied in ways that would cause HFEs/UAs. Note that while possible deviations could be examined as to the *specific* sequence of events, these are likely to be dependent on the operator actions and may be too numerous to investigate efficiently. So this examination is made considering the overall scenario and not the timing and sequence of specific events and how they might deviate from one another. Besides, the observations made below are generally applicable anyway.

Step 5 resulted in the identification of a number of vulnerabilities that could induce unsafe acts for the scenario as postulated. The vulnerabilities that may directly or indirectly relate to the procedural or other rules followed by the operators can be summarized as:

- there is no specific procedural guidance for loss of all service water
- the four abnormal procedures, the EOPs, and other rules which tend to be followed by the operators potentially set-up conflicts with regard to shutting down equipment vs. operating equipment to maintain safety functions
- operating crews at this plant have a strong belief in the procedures and tend to follow them with little discretion, further setting up a potential conflict as to what extent to follow the abnormal procedures vs. the EOPs.

The scenario itself is considered sufficiently challenging and these vulnerabilities are considered to be sufficiently strong that investigation of further deviations from the base case scenario do not appear warranted, with the exception of the stuck-open SRV, which was identified earlier. Such a deviation quickens the need for injection and may cause a more continuous demand for injection over longer periods of time. This places a greater demand on proper operator response.

Furthermore, the decisions with regard to overall strategies (call them "rules" here) for responding to this event could be critical with regard to how the scenario proceeds. For example, in EOP EP-2, the decision about whether emergency depressurization is anticipated (even though strict requirements are not yet met) could lead to an early transfer of energy from the core to the suppression pool, or a later transfer. Whether to simply control RPV level within certain limits vs.

purposely overfilling the vessel (but which will require longer sustained injection) could lead to very different demands on system operations and hence their potential for damage. Whether to shut down diesels in certain situations provides another case where a strategy decision will have to be made, perhaps quickly. The existing potential ambiguity as to which "rules" (strategies) to follow could significantly affect the scenario progression and outcome.

A review of Table D.5 and the potentially triggered error mechanisms and resulting error types relevant to the scenario listed in that table suggests that these apparent problems with the existing "rules" serve to further support the existence of those error mechanisms and types. The rule problems do not necessarily introduce new error types of their own; they simply make the error types identified in Table D.5 (which are fairly general) more likely. This is an important consideration later in the analysis when consideration is given to the likelihood of making unsafe acts.

D.6.3 Search for Support System Dependencies

This search focuses on ways that deviations as a result of support system failures could further add to the error-forcing context of the scenario. In this case, the event itself already involves the complete failure of a major support system of the plant. Further, the potential effects on other support systems, including air and power, have already been considered in the scenario complexities along with the possible ramifications. These include the potential inability to depressurize and/or control RPV pressure, as well as the diesel start issue and the potential for station blackout.

Other possible deviations (but not simply random independent failures of equipment) involving electrical power could include a loss of offsite power as a contributor to the event as well as temperature-driven failures of electrical switchgear, etc. Such deviations would, in the context of this scenario, simply serve as yet other ways that equipment may fail so that it cannot be used. While loss of offsite power would likely cause more of an abrupt loss of the normally running water systems (CCW, TBCCW, PSW), SSW could still degrade over time, depending on the failure mode(s) and therefore the initiator could still be a slowly developing event. In addition, loss of offsite power will further limit the available equipment choices for the operators, depending on which buses are lost and when.

Furthermore, the loss of efficiency in chiller/heating, ventilating, and air conditioning/unit coolers will result in rising room temperatures. This effect will make the environment in the main control room and other areas of the plant less comfortable. This adverse environment could add to the anxiety and stress of the staff as well as potentially increase the chances of making poor judgments in assessing the situation and carrying out tasks. Some temperature-sensitive electronics, indicators, etc. could also be eventually affected, further hampering operator response in the long term.

As with the relevant rule search, it does not appear that the loss of power or induced loss of room cooling would necessarily create new error types from those already identified in Table D.5, which are defined as sufficiently general (although adverse environmental conditions could be considered to introduce new error mechanisms such as tiring and lack of focus). However, the potential for power losses to more severely limit equipment choices, the additional workload and attention issues

created by losing power and the resulting efforts to get power back, and the adverse environmental conditions are likely to make the generally defined unsafe acts even more likely.

D.6.4 Search for Operator Tendencies and Error Types

This search focuses on the tendencies of the operators and the potential error types as a result of those tendencies. Like the search above for relevant rules, note that while possible deviations could be examined as to the *specific* sequence of events and what the operators would tend to do in those specific circumstances, these are likely to be too numerous to investigate efficiently. So this examination is made considering the overall scenario and not the timing and sequence of specific events and how they might deviate from one another. Besides, in a general sense, the two strongest applicable tendencies will likely govern the operators' overall response regardless of the specific situation; these are the potential conflict of the tendency to want to shut down equipment to avoid damage vs. operating the equipment to ensure safety functions. These tendencies are supported by the operators' tendency to follow procedures which for this scenario, call for response to an unfamiliar event for which they have little training and potential procedural conflicts and lack of specific guidance.

Based on these observations, and keeping the search general in scope, it does not appear that these operator tendencies would create error types different than those already identified in Table D.5, which are defined as sufficiently general.

D.6.5 Develop Descriptions of Deviation Scenarios

Because of the nature of the scenario being examined and the already challenging nature of the event, the above searches have not investigated specific deviations from the base case scenario described in Section D.3. For instance, random independent failures of equipment have generally not been considered during the search process. The searches have, however, considered overall scenario deviations resulting primarily from likely cascading effects of the loss of service water event and provided a better understanding as to the potentially triggered error mechanisms and possible error types (defined in a general sense) that may more likely occur. During these searches, it was found that a stuck-open SRV during the event and the possibility of power losses either as part of the initiator or much later in the scenario would be additional deviations that could increase the need for definitive responses and limit the available equipment that could be used.

Therefore, for purposes of this analysis, a scenario will be examined that is considered to follow that generally described in Section D.3 for the base case, but that includes an early stuck-open SRV. The possibility of losing power at some time in the event (i.e., initially or subsequently due to high room temperatures) will be considered.

For this scenario, a summary of what appear to be the more relevant general types of error mechanisms and types is presented in Table D.6, which is largely duplicative of Table D.5. Based on the information in the table, a list follows summarizing the seemingly most relevant scenario-related HFEs/UAs that might be induced and their general impact on the scenario progression.

Table D.6 Loss of Service Water Scenario Summary

Overall Plant Condition (Scenario)	Potential Error Mechanisms Affecting Human Response	Potential Error Types (HFEs/UAs)
Service water is not totally and abruptly lost initially, but is only partially or slowly lost over time while plant is at full power. Recovery is not forthcoming, requiring operators to decide on what equipment to run when, etc. as the situation continues to degrade. A stuck-open SRV early in the event places a greater early and continuous demand for injection. Offsite power may be lost initially or electrical buses may begin to gradually have problems and load disruptions occur due to high room temperatures in electrical bus rooms.	No or smaller change in parameters than expected. (No indication or slower or smaller than expected changes in plant parameters occur at first due to slowly degrading situation.) Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. [Starts as partial loss of service water (expected) but could degrade and become a total loss and hence more severe] Familiarity and simple expectations about the event need to be overcome if the situation changes. (Situation could start as partial loss and become total loss, perhaps unexpectedly, requiring the situation assessment and response change.) Scenario contains dilemmas and response contains double-binds. (Undesirable alternatives such as stop equipment to "save it" vs. operate equipment to maintain safety functions, both per procedures, may setup delays in the response, reluctance or cautiousness, anxiety and stress.) Scenario has many side effects that take time to develop. (There could be fixation on immediate problems and insufficient planning for what is to come.) Delays in changes of parameters may cause events to be a surprise as there is limited knowledge as to what to expect and when. (Equipment degradation may not be indicated and alarmed right away but be delayed.) Scenario may require high tempo/multiple tasks at times adding to anxiety and stress. (Potential for simultaneously indicating problems and some necessary quick responses such as shutting down diesels could add to anxiety and stress.)	May take no action or delayed action to prevent further degradation of service water or respond to its effects due to lack of awareness, at first, as to nature of problem. Could believe situation has stabilized with some service water flow and thus be caught off guard when total loss occurs; potentially missing some necessary immediate actions such as shutting down diesels or loads. Wrong or inappropriate actions could be taken or needed actions could be taken too late, regarding which equipment to operate or shut down, when to do it, for how long. Could result in unnecessary equipment damage or safety function degradation. Note that the overall strategy decision as to how to respond could be an important and potential error (e.g. fill vessel and depressurize early vs. maintaining status and waiting for procedural cues). Insufficient planning may exist as to what may happen next, as well as in the longer term, so that best response and use of resources (equipment, consumables, staff) is not achieved. Anxiety and stress, should scenario seriously degrade, could disrupt coordination efforts and challenge communication among staff so that actions are taken by individuals without full knowledge of entire crew.

Based on the above information, scenario-related "general" HFEs/UAs more likely to be potentially induced include the seven listed below.

The following are potential HFEs/UAs related to *certain actions of the crew*:

(1) *Diagnose initiator. Failure to diagnose source and full scope of the initiating event early.*
Unawareness or misdiagnosis of the source (loss of service water) and scope (eventual total failure) of the event could result in operators not shutting down unnecessary loads or swapping or alternating equipment, at least at first, as the EOPs are followed. This could result in irreparable damage to equipment items, making them unavailable for later use and thereby more severely limiting the equipment options later in the scenario. If the diesels were involved and not shut down quickly, the plant could experience a station blackout depending on the condition of offsite power. If too much equipment becomes failed, safety functions may not be able to be maintained and core or containment damage may result.

(2) *Diesel management. Failure to properly respond to diesel generator starts initially or later in the scenario.*
It is not clear ahead of time as to the appropriate response because it likely depends on the condition of other power sources, which loads are needed and when and for how long, etc. As stated above, the possibility of entering a station blackout, loss of safety functions, or irreparable damage to the diesels could result.

(3) *Equipment management. Shut down or secure equipment to protect it at an inappropriate time when it is vitally needed, fail to prevent startup of equipment (or manually start it) when it is not needed, fail to shut it down before damage occurs to the equipment, or fail to prevent undesirable alignments that may increase damage to the equipment.*
This is a potential issue throughout the scenario and requires cognizance of the status of overall plant conditions and individual equipment throughout the scenario. Depending on the overall strategy of the operating crew, maintaining a level of redundancy of mitigating equipment for all safety functions would be most desirable. Inappropriate responses of this nature could cause the loss of equipment needed to mitigate the event and jeopardize the safety functions.

(4) *Consumables management. Use equipment in ways that cause the loss of consumable resources.*
Water for injection, compressed air, and electrical power are resources needed to mitigate the event. For example, operating compressors until they fail or using SRVs too many times with backup air or nitrogen could lessen the chance of successfully depressurizing and controlling pressure when required. External water sources will be cooler than the suppression pool as a suction source and thus actions taken to preserve or replace their contents may be desirable. Nonrecognition of the desire to drop unnecessary electrical loads and use portable room cooling for electrical bus rooms could result in later problems with electrical power. If not used and protected wisely, loss of these consumables could lead to the inability to use mitigating equipment at a vital time, thereby causing loss of safety functions.

The following are potential HFEs/UAs that can affect the *overall response of the crew* and thereby contribute to or lessen the chances of the HFEs/UAs listed above:

(5) *Adopt an overall poor strategy or plan at the beginning of the scenario.*
The overall crew strategy or plan as to how to respond to the event should be decided early and consider the best way to save equipment and consumables while meeting the needs of the safety functions. For instance, overfilling the RPV early will allow more time for later responses (it will take longer for the vessel level to drop to undesirable limits), but will require more continuous use of equipment early in the scenario. A poor strategy (probably one involving too much maintenance the status quo and not anticipating later needs) or lack of planning could result in eventual loss of ability to mitigate the event.

(6) *Improperly communicate or coordinate control room and other plant area efforts.*
These types of failures could result in plant equipment alignments being made without full knowledge of the crew, potentially causing confusion/anxiety/stress that may further complicate the response and cause loss of safety functions or vital equipment.

(7) *Improper use of personnel for the circumstances or high room temperatures*
If the event is particularly prolonged for many hours, the use of staff resources should consider the adverse environment (high temperatures) within the plant and allow for breaks, turnovers, etc. so as to not overly tire individuals. Otherwise, poor judgments and actions may result.

D.7 Step 7: Identify and Evaluate Complicating Factors and Links to Performance Shaping Factors (PSFs)

While additional complicating factors such as random failures of equipment or indicators or alarms may make the context even more error forcing, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be addressed at this time.

Also, the most relevant PSFs have already been identified through the previous steps. These include such factors as unfamiliarity with the event, including a tendency to disbelieve it, little training and procedural guidance, adverse environment, conflicting goals, time pressure at times (e.g., shutting down diesels), limited resources, and potentially high attentional and work loads. These have already been accounted for as potentially contributing to the types of errors that could be made.

D.8 Step 8: Evaluate the Potential for Recovery

Even if the scenario occurs and is a prolonged loss of the ultimate heat sink, and if the operators were to make the types of HFEs/UAs listed in section D.6.5, there is a chance that the operators will recover from their past faults and still prevent severe core or containment damage. In order to address the recovery issue, it is necessary to understand the relationship among the HFEs/UAs listed above and the possible recovery actions that may influence the scenario outcome. To do that, an event tree is constructed and shown in Figure D.10.

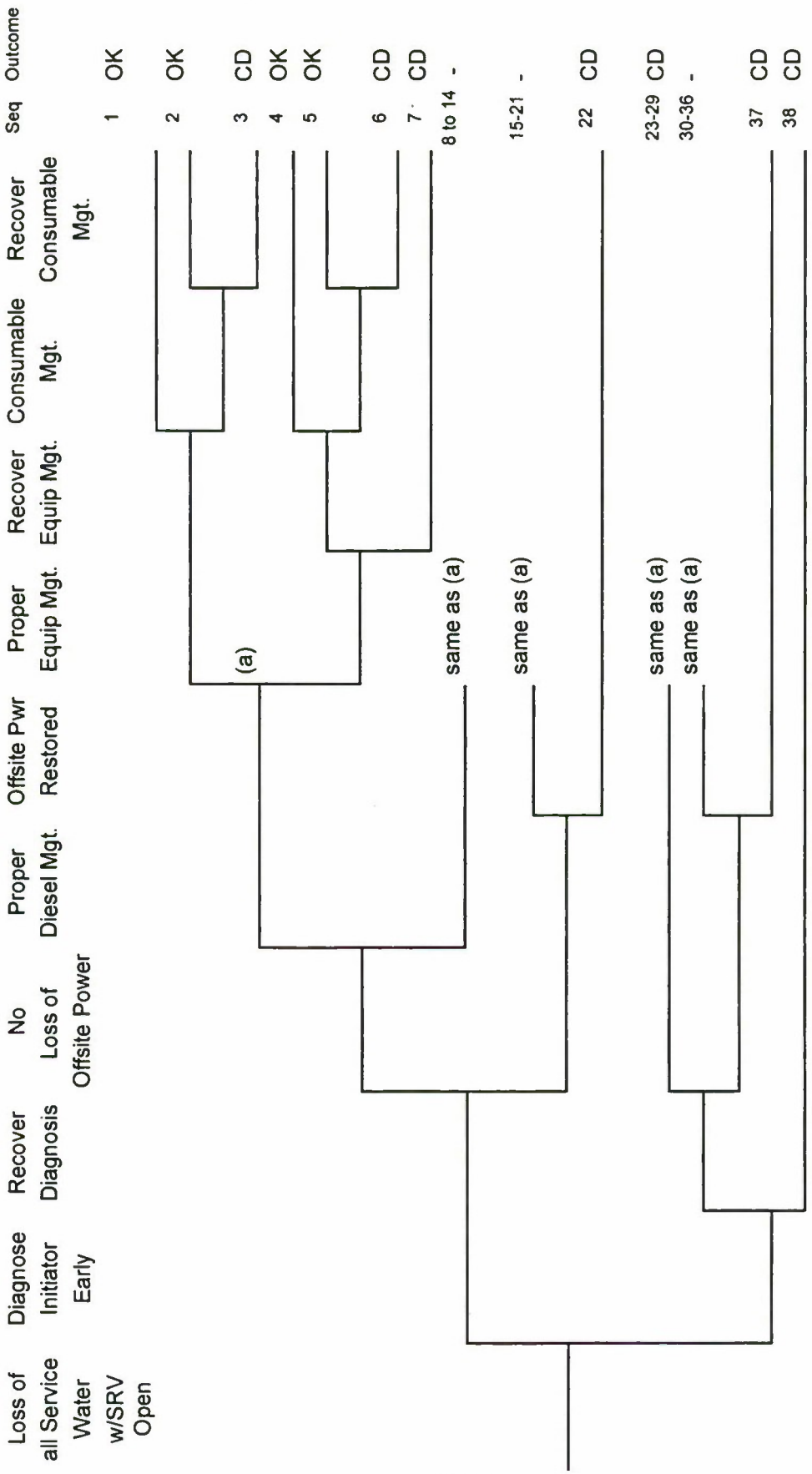


Figure D.10 Loss of Service Water Event Tree

The event tree displays the logic among the first four possible HFEs/UAs listed and their potential to lead to core damage. Also shown are the logical chances for recovering from each HFE/UA except for the diesel management failure. So little time is available to recover from a wrong decision about protecting the diesels that no chance for recovery is credited. In addition, whether offsite power is available and is recovered (if unavailable) reasonably quickly during the event can have a significant impact on the scenario outcome and so is also included in the tree structure. Note that in cases where there is a loss of normal power and it is not recovered fairly quickly, the outcome is assumed to lead to core damage (may be conservative) since it is also assumed that the diesels cannot be operated for more than a few minutes, and thus a blackout condition with loss of heat sink will soon lead to failure of the only injection system available, RCIC.

For cases where the source and extent of the initiator are not diagnosed early, it is considered that the diesels, which are apt to get a start signal, will likely not be shut down quickly enough and thus will be lost even if the extent of the initiator is eventually understood (recovered). If the initiator and its effects are not diagnosed or understood properly (the last sequence in the tree), it is assumed that the other HFEs/UAs, and therefore core damage, are likely.

The latter three HFEs/UAs listed in Section D.6.5 (numbers 5, 6, and 7) are really underlying factors that affect the likelihoods of especially HFEs/UAs, numbers 3 and 4 above. If strategy development, coordination and communication, or management of manpower resources is poor, there is a greater chance of taking the actions discussed in items 3 and 4.

The specific cues (indicator readings, alarms) and their timing related to the three recoveries in the event tree for initiator diagnosis unsafe acts, equipment management unsafe acts, or consumables management unsafe acts, cannot be explicitly delineated nor can the specific sequence of events.

This would require some additional study and thermal-hydraulic analyses not included here at this time. However, enough is known about the general nature of the cues that may induce the recovery actions that they are briefly discussed below.

Recover Initially Inadequate Diagnosis

If the operating crew has initially failed to understand the source and extent of the initiator, including its effects, many cues will become available so that the operators may correctly interpret the nature of the event and its potential ramifications. This needs to be done before damage has occurred to numerous pieces of mitigating equipment by allowing the equipment to run too long without recognition of inadequate cooling. Otherwise, there may be insufficient redundancy left to ensure maintaining the critical safety functions. As the ultimate heat sink degrades, a series of alarms and other indications will become available, which if taken together, should present a clearer means to diagnose the event. These include (for example):

- recirculation pump motor high temperature alarms
- reactor water cleanup and fuel pool heat exchanger isolations on high temperature
- CCW discharge header pressure low-low alarm
- erratic CRD pump current indications

- TBCCW header pressure indicator reads "low" or TBCCW header pressure low-low alarm
- TBCCW pump trip alarms
- TBCCW surge tank level high/low alarm
- PSW header pressure low alarm
- decreasing condenser vacuum
- auto trips of drywell and plant chillers
- SSW pump discharge pressure low alarms
- SSW pump overload and/or pump trip alarms
- HPCS SSW system trouble light lit
- various indications of trouble (erratic current, vibration, temperature, flow readings to the extent they exist) on affected equipment over time (main turbine, generator, feed pumps, ECCS pumps, room areas).

The extent of the alarms would seem to indicate that even if the initiator were to occur slowly over time so that the initial understanding of the event is not clear, the potential to understand the full nature and impact of the loss (i.e., recover the diagnosis) seems high based on the number and diversity of these indications. Hence, it is the opinion of the analysts that the likelihood of continuing to misdiagnose the event seems quite low. However, it is agreed that full understanding could come after some mitigating equipment (diesels, ECCS pumps) has been overheated or even damaged.

Recover from Poor Equipment Management

The operating crew could mis-operate mitigating equipment needed to attempt to maintain safety functions; especially if HFE/UAs numbers 5, 6, and 7 are also being made. Mis-operation could involve, for instance, letting equipment operate that is not needed or letting needed equipment operate too long and thus overheating it, or even damaging and thereby preventing its use later on. Signs of this mismanagement of the equipment will occur based on indicator readings of erratic current or flow readings where available (such cues do not exist on many pieces of equipment), low discharge pressure readings, pump trip alarms, or even signs of loss of safety functions (such as lowering RPV level). Since clear indications of overheating equipment are not often available until the equipment is already beginning to suffer degraded performance, the potential for overheating or even damaging some equipment during the scenario is judged to be high. However, the above signs of this mismanagement might make the operating crew more cautious and conservative about operating equipment as the scenario proceeds, with greater emphasis on keeping some equipment in reserve. Thus, the operating crew may become more keenly aware of needing to properly manage the use of equipment, especially if they have suffered the loss of some equipment early in the scenario. On the contrary, the demand for maintaining safety functions will be great and there will be a strong desire to operate whatever equipment is needed to do that. Hence, the extent to which the crew will learn from any initial losses of equipment due to mismanagment of equipment resources, and prevent or lessen the chances of such losses continuing to occur, is judged to be uncertain in light of this double-bind situation.

Recover from Poor Use of "Consumables"

The operating crew could mis-operate equipment in ways that quickly consume air, water, or power; especially if HFE/UAs numbers 5, 6, and 7 are also being made. Mis-operation could involve, for instance, not alternating compressor use or using compressor too often, thereby failing them; cycling SRV operation too often, using up available air and nitrogen; not dropping unnecessary electrical loads to lessen the switchgear heatup; not using portable cooling; failing to plan for water replenishment, etc. Signs of this mismanagement of the equipment will occur based on indicator readings of low air pressure, quickly falling tank levels, and room temperature alarms, among others. Since clear indications of problems may not often be discernible until the degraded conditions already exist, the potential for too quickly using up these consumables, at least at first, is judged to be high. However, as these signs do become available and with sufficient forethought about the demands on these resources, the crew could become more cautious and conservative about protecting these consumables as the scenario proceeds. On the contrary, the demand for maintaining safety functions will be great and there will be a strong desire to operate whatever equipment is needed to do that. Hence, the extent to which the crew will learn from any initial mis-managment of these consumables and prevent or lessen the chances of such mismanagement continuing to occur, is judged to be uncertain in light of this double-bind situation.

General Observations

As a whole, it can be said that cues, some direct and some indirect, will present themselves as the scenario proceeds. They will indicate the extent of the initiator and the need to better manage equipment and consumable resources. However, the cues will often be delayed and in some cases may not occur until considerable degradation of conditions has already occurred. Without a pre-thought-out plan of preferred actions, the operating crew may need to respond to events as they happen and learn (i.e., recover from previous poor judgments or actual unsafe acts) as they go, based on their observations of equipment and plant conditions that are dynamic. Hence, recovery where needed is possible; but clearly, recovering past mistakes as they happen and attempting to continue to satisfy safety function demands while avoiding equipment damage is a more difficult task without prior analyses, explicit procedural guidance, and training.

D.9 Quantification Considerations

A rough approximation is derived as to the likelihood of the event and its leading to core damage as a result of the above contributing human failures and/or unsafe acts. From Section 10, it is seen that such an assessment requires estimating the frequency of the error-forcing context (made up of the frequency of the plant condition × the probability of relevant PSFs), the probability the crew will perform the unsafe act(s), and the probability that they will not recover their original mistakes before serious plant damage occurs. Each is discussed below.

Frequency of Error-Forcing Context

The plant condition is postulated as an eventual and prolonged total failure of the ultimate heat sink, along with a stuck-open SRV during the early and numerous demands which are occurring when the balance-of-plant is isolated and subsequent pressure is controlled by the operator. The existing plant

PRA provides information to approximate this likelihood. Based on the modeled ways to lose all service water, the PRA provides an estimate of approximately 1E-5/year for the frequency of losing the ultimate heat sink for more than just a few minutes if loss of offsite power is a contributor to the event. With offsite power available, the PRA value is approximately 1E-6/year. Hence the chance of the initiator is considered to be in the E-5/year range. Considering an estimated number of SRV demands for this event (approximately a dozen or more) and the stuck-open probability per demand of about 1E-2, a likelihood of a stuck-open SRV in this event is estimated to be about 0.1 or a little greater. Combining these two values provides a frequency for the initial plant condition in the low-to-mid E-6/year range. Accounting for the need for this event to last at least in the range of 2-4 hours or more to be particularly challenging, PRA estimates for failing to recover service water or offsite power (if lost) are approximately 0.1. Hence, the likelihood of the plant condition existing for about 2-4 hours or longer is on the order of low-to-mid E-7/year.

The likelihood of the PSFs contributing to the overall frequency of the error-forcing context is considered high enough to be approximated as 1.0 since all the PSFs summarized in Section D.7 are considered by the analysts to be present and strongly influencing the performance of the operating crew given the plant condition. Hence, the estimated frequency of the error-forcing context for the postulated event is in the range of low-to-mid E-7/year.

Probability of Unsafe Act(s) and Nonrecoveries

Rather than attempting to estimate and combine the individual HFE/UA and nonrecovery probabilities, for purposes of this analysis it has been decided that a gross estimate will suffice of the crew incorrectly responding to the dynamics of the situation and performing unsafe acts that contribute to a core damage accident. Taking into account all the opportunities of the various HFEs/UAs that have been discussed and the uncertainty about the ability to recover, the analysts have worked out a consensus judgment about the likelihood of the plant staff performing unsafe acts that either directly cause or significantly contribute to core damage. This judgment is based on their experience, their understanding regarding the dynamic nature of this event, the status of procedural and training guidance, consideration of technical support staff assistance after about 1-2 hours following the trip, and factoring in the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10 of this report. All of these considerations collectively suggest a value of between 0.05 to about 0.5 for this estimate.

Frequency of the Event Leading to Core Damage

Combining the frequency of the error-forcing context and the probability above yields an estimate of this event progressing to core damage largely because of unsafe human interactions to be in the low E-8/year to mid E-7/year range. This is comparable to the existing core damage frequency for this initiator in the PRA of 2E-7/year.

D.10 Step 10: Issue Resolution

This analysis indicates that the likelihood of this event progressing to core damage in large part due to unsafe acts by operators is comparable to or may even be slightly greater than that already calculated in the PRA for a loss of service water initiator.

In addition, and more important, a number of lessons learned have resulted from this analysis that indicate there are improvements that could better prepare operating crews to respond properly to a prolonged loss of ultimate heat sink. The utility staff is considering the following:

- discussing with operating, maintenance, and management staff the results of this analysis and the potential contexts of concern

- performing engineering analyses and simulator runs to better understand possible sequences of events following loss of the ultimate heat sink and the identification and timing of cues indicating developing problems

- developing more explicit procedural guidance for both the operating staff and the technical support staff regarding preferred actions to be taken upon discovery of the loss of heat sink as well as ways to minimize equipment damage and use of resources during the response to such an event (where possible, utilizing guidance available in existing SBO procedures)

- developing training exercises and talk-throughs for this event that approximate various anticipated phases to the extent practicable, to familiarize the staff with its dynamics and what to expect during a prolonged loss of heat sink

APPENDIX E
ATHEANA EXAMPLE -
SMALL LOSS OF COOLANT ACCIDENT (SLOCA)
A "DIRECT INITIATOR SCENARIO"

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that could seriously degrade plant response to a small loss of coolant accident (SLOCA) direct initiating event. More specifically, it is an illustration of the use of ATHEANA to identify and quantify those conditions (error-forcing contexts) that may induce human unsafe acts.

This is a plant-specific example, as all fruitful examinations of context must be. However, the plant analyzed is a composite pressurized water reactor (PWR), not exactly matching any particular operating plant. The example is realistic in that all specific design, procedures, training, and operating and maintenance practice information used in the analysis have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate similar issues in their plants.

The illustration follows the steps discussed in the ATHEANA process in Section 9 of this document.

E.1 Step 1: Define and Interpret the Issue

The Emergency Operating Procedures (EOPs) applicable to SLOCA scenarios have been successfully tested in many plant simulators, with many crews. However, in a number of cases, crews have had difficulties–getting lost in inappropriate branches of the EOPS or running out of time–often because trainers running the simulations have failed large numbers of safety components and subtly related equipment.

The issue to be addressed in this application of ATHEANA is: Can reasonable variations on the SLOCA scenario be identified, such that progress through the EOPs is significantly more difficult than for the SLOCA of the Final Safety Analysis Report (FSAR) safety analysis?

It is useful to discuss the idea of "reasonable" variations, before proceeding with the analysis. The plant probabilistic risk assessment (PRA) identifies the functional failures that lead to core damage. For the SLOCA, the PRA calculates the frequency of scenarios that involve an SLOCA (frequency of SLOCA initiator) and combinations of component functional failure (probability of hardware failure and human failure to carry out expected and necessary tasks) that cause the plant functional failures that lead to core damage. From the ATHEANA point of view, there is a larger class of equipment failure, mal-alignment, and unexpected modes of operation, not currently modeled in the PRA, that, while not directly causing hardware functional failures associated with core damage, create cognitively challenging situations for the operators (error-forcing context, EFC) that can set up the operators to carry out unsafe acts (UAs) that make up human failure events (HFEs), thereby defeating functional success. The fact that a much larger set of components can affect human operator response than can directly affect hardware controlled plant functions sets up the PRA/HRA (Human Reliability Analysis) analyst to underestimate the probability of such conditions.

To the PRA/HRA analyst and, indeed, to most engineers (and even operators, if asked the question directly), the chance that additional components are failed is always lower than the chance that they are not. Such a view is supported by calculations of scenarios for which additional independent

failures are postulated. But there is something of a fallacy at work here; let's call it the fallacy of zero failures. If you pose the question to operators in a different way, you get a very different answer. If you ask an operator: when a reactor trip occurs, would you be surprised to encounter problems (i.e., failures) somewhere in the plant? The answer almost invariably will be "Not at all! There is always some valve, some controller that doesn't work just right. We just find a way around it and check it out later." Note that we are not talking about dependent, common cause failures here, but what appear to be random, independent failures. The reason that the expectation of zero additional failures is fallacious can be demonstrated by a simplified analysis.

Suppose we have several systems composed of a number of two-state components (successful or failed) with identical failure rates. Say that the failure probability of each component is "p," where p = 0.001. If the number of components in a system is "n," then the probability that k out of the n components are failed follows the usual binomial distribution:

$$P(k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$$

Now we can directly address the likelihood of zero failures (or, if a scenario has "r" failures, the chance that they are actually one, two, or more additional failures). We look at four cases where the systems have 100, 1,000, 10,000, and 100,000 components respectively (Table E.1).

Table E.1 Probability of k Failures in Systems of Various Size (p=0.001)

k	n=100	k	n=1,000	k	n=10,000	k	n=100,000
0	0.90	0	0.37	0	4×10^{-5}	0	4×10^{-44}
1	0.09	1	0.37	1	5×10^{-4}	1-64	7×10^{-5}
2	0.004	2	0.18	2	2×10^{-3}	65-74	4×10^{-3}
3-100	2×10^{-4}	3	0.06	3	8×10^{-3}	75-84	0.05
		4	0.02	4	0.02	85-94	0.23
		5	3×10^{-3}	5	0.04	95-104	0.365
		6-1000	1×10^{-3}	6	0.06	105-114	0.23
				7	0.09	115-124	0.06
				8	0.11	125-100,000	0.06
				9	0.12		
				10	0.12		
				11	0.11		
				12	0.09		

Table E.1 Probability of k Failures in Systems of Various Size (p=0.001) (Cont.)

k	n=100	k	n=1,000	k	n=10,000	k	n=100,000
				13	0.07		
				14	0.05		
				15	0.03		
				16	0.02		
				17	0.01		
				18	7×10^{-3}		
				19-33	7×10^{-3}		
				34-10,000	$< 5 \times 10^{-5}$		

We have provided more detail in the calculations than required for our purposes, but feel that the detail may be helpful for some readers. The point is that, for a system with 100 components, our intuition is quite good: the chance that there are zero failures at any randomly selected time is 90%; the chance of one failure is almost 10%; the chance of two failures is only 0.5%; and the chance of more than two failures is minuscule.

However, this situation changes quite dramatically as the number of components in the system goes up. For a plant with 1,000 components, the chances of zero or one failures are equal (37%) and the chance of two failures is about half of that (18%). There is nearly a 10% chance that three to five failures have occurred, and a very small chance that more than five are failed. If there are 10,000 components, there is almost no chance that none or only one component is failed; it is most likely that 7 to 12 are failed (64%); and there is a small chance that more than 20 have failed. Finally, if the system has 100,000 components, there is almost no chance that fewer than 65 are failed; it is most likely that 85 to 115 are failed (> 80%); and there is a small chance that more than 125 are failed.

What does this mean to a nuclear plant PRA and an ATHEANA analysis? Although actual component demand failure rates vary roughly from 1×10^{-4} to 1×10^{-2}, with a few above and below that range, the use of 1×10^{-3} in the example is not unreasonable. There are about 100 component types modeled in a typical PRA, representing about 500 to 1,000 components. So, among those components modeled in the PRA, it is likely that there are 0 to 2 failures at any particular time. As discussed above, many other components–especially instrument and control (I&C) systems, but also balance of plant components and others not modeled in the PRA–compete for the operators' attention and affect their situation assessment, workload, etc. There are typically more than 100,000 components on a plant Q-list, but not all of these have a high potential to directly affect the operators. We suspect that all told there may be 2,000 to 5,000 components among safety systems, support systems, I&C equipment (including alarms), balance of plant, and radwaste systems that

have a potential claim on the operators' attention. Therefore, while from a strictly PRA component list point of view there may be little chance that more failures exist than those identified in the PRA sequences or cut sets, from the EFC viewpoint relevant to ATHEANA, it is almost certain that several additional failures are present. Various groups of these failures form classes of EFC that may be relevant to ATHEANA analysts.

E.2 Step 2: Define the Scope of the Analysis

In this case, the scope of the initiator type is limited by the issue to SLOCA. Characteristics of the SLOCA that are challenging include the fact that inventory is being lost and, if makeup water is not supplied in short order, extensive voiding in the reactor coolant system (RCS) will occur that impedes reflood and pressure control (especially because reactor coolant pumps (RCPs) are stopped by procedure, early in the event). In addition, while there is significant heat removal via the rupture, it is not sufficient to maintain temperature or support cooldown. However, this blowdown heat removal, when combined with steam dump following turbine trip, can lead to concerns about overcooling. After a short time, no steam dump is required at all. Some time into the accident, the operators must manually switch cooling from safety injection (SI) to closed loop residual heat removal (RHR) cooling or containment sump recirculation cooling.

We anticipate that some setting of priorities among potential contextual elements may be needed to narrow the analysis to an affordable scope. Therefore, we consider additional sources of information. From a review of the events in Appendix A, we find that many serious events involve an incorrect situation assessment resulting from a combination of factors:

- a significant physical deviation in the initiator or scenario (a strongly influencing mismatch between training and plant physics in the scenario) and an instrument problem (a moderately influencing mismatch between actual conditions and indicated conditions)

- a significant bias about the initiator or scenario (a strongly influencing mismatch between training and plant physics in the scenario) and an instrument problem (a moderately influencing mismatch between actual conditions and indicated conditions, due to an instrument).

Both cases involve operators not understanding the physics of the situation combined with an instrument problem that can disrupt clear thinking about the situation.

From the examination of Appendix A and Table 9.2 in the report, we infer that physical deviations are most likely to contribute to strong EFC. Next would be crew factors such as distractions that separate the control room team, permitting a single operator to act independently. Finally, we will focus on multiple, conflicting priorities.

E.3 Step 3: Describe the Base Case Scenario

The ideal base case, as described in Step 3 of the process description in Section 9 and illustrated in the first row of Table E.2, corresponds with a consensus operator model (COM) of the event; i.e., a mental model of the event that operators have developed through training and experience, and that is consistently understood among most operators. Furthermore, it is well defined in both an operational sense and an engineering sense (thorough neutronics and thermal-hydraulics analysis support the scenario). Finally, it is well documented and realistic. Note that Table E.2 also previews the results of the SLOCA base case development that will be presented in the following paragraphs. For the SLOCA, the base case is very near the ideal case. It will be used as the stepping off point for the deviation analysis. Because the COM is a result of required training based on the FSAR, the COM is not presented separately but is discussed during the description of the reference case and the base case.

Table E.2 Characteristics of the Base Case Scenario

Type of Base Case	Consensus Operator Model	Well-Defined Operationally	Reference Analysis		Realistic
			Well-Defined Physics	Well-Documented	
Ideal	Exists	Yes	Matches COM	Yes, Public	Yes
SLOCA Base Case	Yes; the FSAR safety analysis case is well known	Yes. Annual training scenario	FSAR safety analysis case closely matches the COM, but the analysis ends, after stabilization, but before the long-term scenario is complete	Yes; FSAR	Reasonably realistic

E.3.1 The Reference Case SLOCA Scenario

The reference case SLOCA scenario is the plant FSAR analysis, "Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes which Actuates Emergency Core Cooling System," FSAR Chapter 14 Safety Analysis, Section 14.3.1 pages 14.3-2 to 14.3-7 plus associated Figures 14.3-1 to 14.3-7 and Table 14.3-1.

The FSAR SLOCA is a Condition III infrequent fault, i.e., "faults which may happen very infrequently during the life of the plant. They will be accommodated with the failure of only a small fraction of the fuel rods although sufficient fuel damage might occur to preclude resumption of the operation for a considerable outage time. The release of radioactivity will not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius. A Condition III fault will

not, by itself...result in a consequential loss of function of the Reactor Coolant System or of containment barriers."

As specified by 10 CFR 50 Appendix K, "ECCS Evaluation Models," the FSAR analysis is conservative in many of its details[1], but the predicted time progression of the major plant parameters is a reasonable representation of the progression of the event. The primary impact of the conservative assumptions is to overestimate the possibility of minor core damage. A number of more realistic analyses exist,[2] but are not available in the open literature. Therefore the FSAR case has been selected to define the "reference" case for the analysis.

The FSAR analysis defines a LOCA and describes the SLOCA analysis, as follows:

> *A loss-of-coolant accident is defined as a rupture of the Reactor Coolant System piping or of any line connected to the system...Ruptures of small cross sections will cause expulsion of the coolant at a rate which can be accommodated by the charging pumps which would maintain an operational water level in the pressurizer permitting the operator to execute an orderly shutdown. The coolant which would be released to the containment contains the fission products existing in it.*
>
> *Should a larger break occur, depressurization of the Reactor Coolant System causes fluid to flow to the Reactor Coolant System from the pressurizer resulting in a pressure and level decrease in the pressurizer.[3] Reactor trip occurs when the pressurizer low-pressure trip setpoint is reached. The Safety Injection System is actuated when the appropriate setpoint is reached. The consequences of the accident are limited in two ways:*
>
> *(1) Reactor trip and borated water injection complement void formation in causing rapid reduction of nuclear power to a residual level corresponding to the delayed fission and fission product decay,*
>
> *(2) Injection of borated water ensures sufficient flooding of the core to prevent excessive clad temperature.*

---

[1]Conservatisms include break size and location, assumed loss of one train of the emergency core cooling system (ECCS), degraded SI pump head, limiting core power distributions, maximum allowable deviation (drift and error) in actuation setpoints, delay in actuation of safety injection, minimum allowable volumes, minimum heat transfer, maximum initial power, maximum fission product inventory, minimum fuel/clad temperature limits, etc.

[2]Other analyses include the backup document for the Westinghouse Emergency Response Guidelines and various proprietary WCAP thermal-hydraulic reports.

[3]If the LOCA should be in the pressurizer, flow is into the pressurizer from the RCS. If it is in the pressurizer steam space (or when the level drops below the break location), level may rise even though mass is being lost. (Steam space pressure will be lower in the pressurizer than elsewhere in the RCS.)

Before the break occurs the plant is in an equilibrium condition, i.e., the heat generated in the core is being removed via the secondary system. During blowdown, heat from decay, hot internals and the vessel continues to be transferred to the Reactor Coolant System. The heat transfer between the Reactor Coolant System and the secondary system may be in either direction depending on the relative temperatures. In the case of continued heat addition to the secondary side, system pressure increases and steam dump may occur. Makeup to the secondary side is automatically provided by the auxiliary feedwater pumps. The safety injection signal stops normal feedwater flow by closing the main feedwater line isolation valves and initiates emergency feedwater flow by starting auxiliary feedwater pumps. The secondary flow aids in the reduction of Reactor Coolant System pressure. When the RCS depressurizes to 700 psia, the accumulators begin to inject water into the reactor coolant loops. The reactor coolant pumps are assumed to be tripped at the initialization of the accident and effects of pump coastdown are included in the blowdown analyses...

The postulated small break LOCA is predominately a gravity dominated accident in which the slow draining of the RCS is accompanied by the formation of distinct mixture levels throughout the RCS. These mixture levels vary with time and are dependent upon the transient two-phase transport of mass and energy, which takes place within the RCS during the course of the accident. Consequently, the degree of accuracy with which a system model is capable of simulating the RCS's response to a small break LOCA is dependent upon the model's capability to accurately model the RCS's transient mass and energy distribution...

Results

...results of the limiting break size [are presented] in terms of highest peak clad temperature. The worst break size (small break) is a 3-inch diameter break. [The 3-inch break analysis is the most thorough of the SLOCA FSAR analyses and is selected as the SLOCA reference case for the ATHEANA analysis. Note that, in the PRA, small and medium LOCAs are considered separately, because the SI systems required to successfully respond are different. The FSAR analysis considers these both as small LOCAs and seeks the limiting case in terms of nearness to critical heat flux and possibly extensive core damage.] The depressurization transient for this break is shown in Figure [E.1, with the associated flow rate to RCS given in Figure E.2]. The extent to which the core is uncovered is shown in Figure [E.3].

During the earlier part of the small break transient, the effect of the break flow is not strong enough to overcome the flow maintained by the reactor coolant pumps through the core as they are coasting down following reactor trip. Therefore, upward flow through the core is maintained. The resultant heat transfer cools the fuel rod and clad to very near the coolant temperatures as long as the core remains covered by a two-phase mixture.

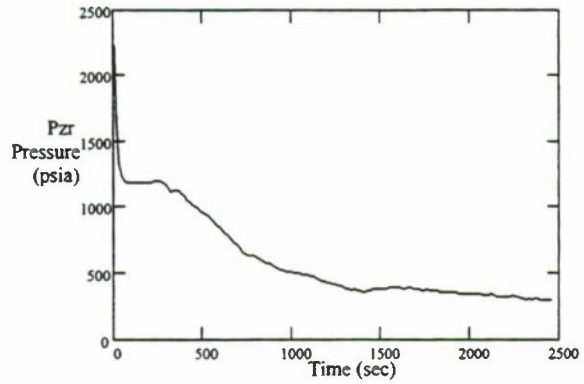


Figure E.1 RCS Depressurization Transient during 3-inch SLOCA Reference Case

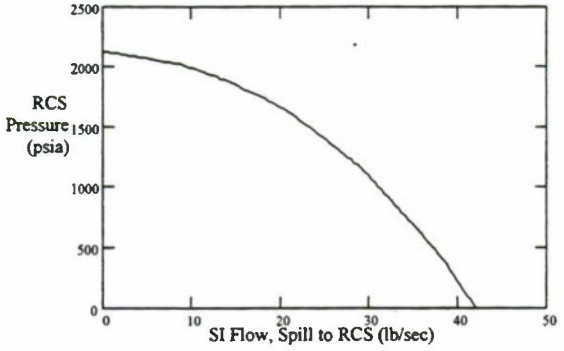


Figure E.2 Pumped Safety Injection Flow during 3-inch SLOCA Reference Case

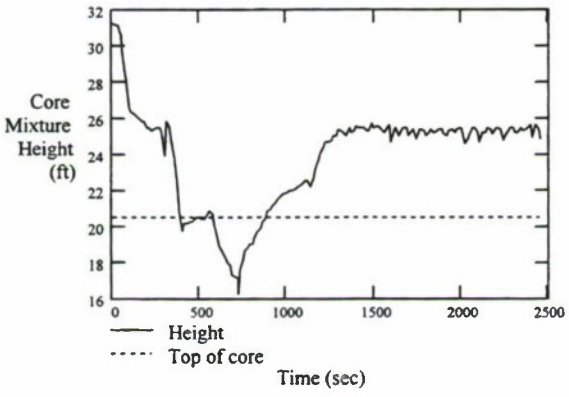


Figure E.3 Core Mixture Height during 3-inch SLOCA Reference Case

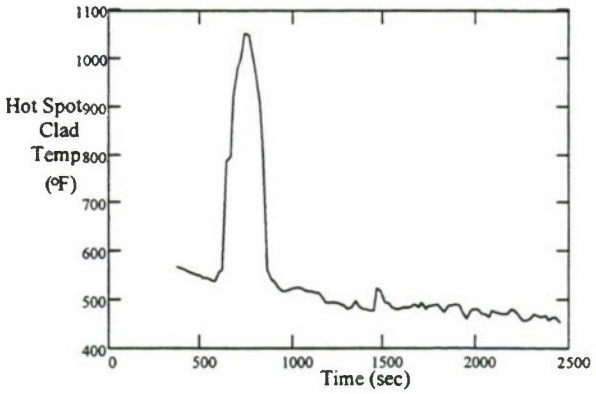


Figure E.4 Clad Temperatures Transient during 3-inch SLOCA Reference Case

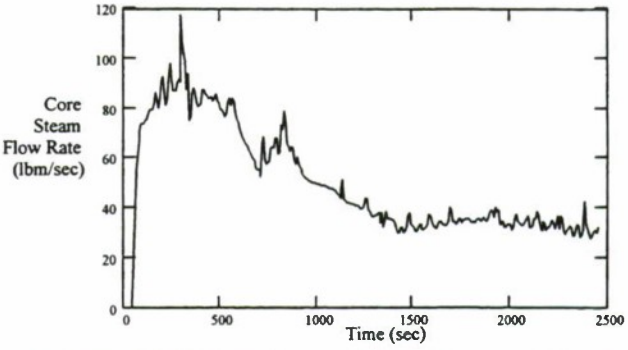


Figure E.5 Core Steam Flow during 3-inch SLOCA Reference Case

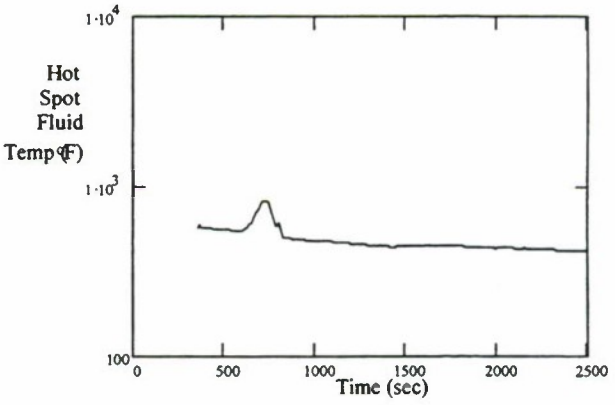


Figure E.6 Hot Spot Fluid Temperature during 3-inch SLOCA Reference Case

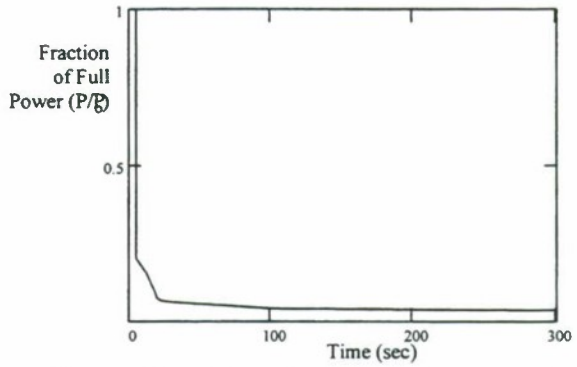


Figure E.7 Core Power during 3-inch SLOCA Reference Case

The maximum hot spot clad temperature calculated during the transient is 1020 °F including the effects of fuel densification... The peak clad temperature transients are shown in Figure [E.4] for the worst break size, i.e., the break with the highest peak clad temperature. The steam flow rate for the worst break is shown on Figure [E.5]. When the mixture level drops below the top of the core, the steam flow...provides cooling to the upper portion of the core...The hot spot fluid temperature for the worst break is shown in Figure [E.6].

The core power (dimensionless) transient following the accident...is shown in Figure [E.7]. The reactor shutdown time (5.0 sec), is equal to the reactor trip signal time (2.0 sec) plus 3.0 sec for rod insertion. During this rod insertion period, the reactor is conservatively assumed to operate at rated power.

Conclusions

...the high head portion of the Emergency Core Cooling System, together with accumulators, provide sufficient core flooding to keep the calculated peak clad temperatures below required limits of 10 CFR 50.46 [2200 °F]. Hence, adequate protection is afforded by the Emergency Core Cooling System in the event of a small break loss-of-coolant accident.

Following the TMI accident, [the vendor] performed generic studies of small break loss-of-coolant accidents. Results of these studies indicated that peak clad temperatures greater than 2200 °F may occur if the reactor coolant pumps are tripped after a significant loss of reactor coolant inventory. To prevent such a loss, the operators are instructed to trip the pumps early in the accident.

Break sizes of 2 and 4 inches were also analyzed. The depressurization transients for all three cases are shown together in Figure E.8. In all three cases, after the pressurizer empties, the pressure falls to RCS saturation pressure, about 1200 psia. As the RCS cools down, pressure again begins to fall,

faster, as expected, for larger LOCA sizes. For the 2- inch LOCA, the core is never uncovered. For the 4- inch LOCA, the core uncovers and peak clad temperature reaches 871 °F, but the effect is not as severe as for the 3-inch LOCA, where the peak clad temperature reached 1020 °F.

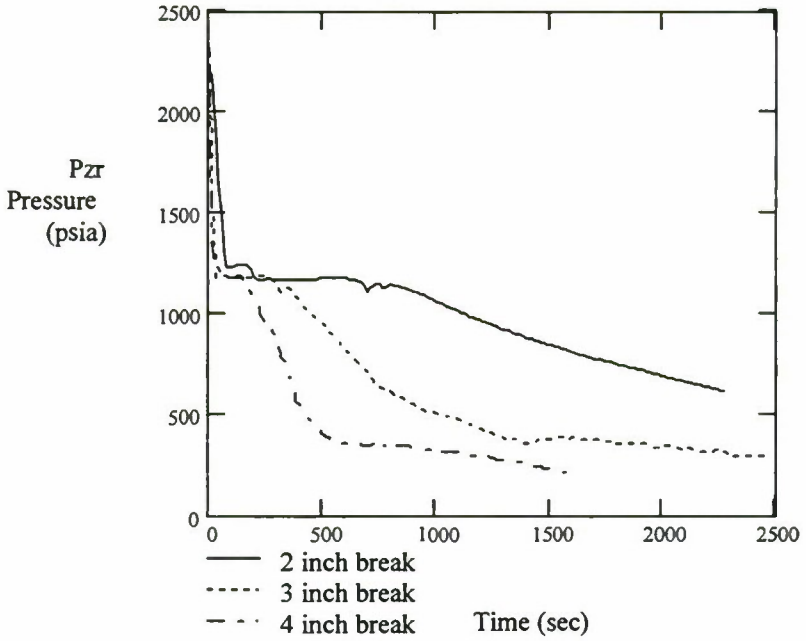


Figure E.8 Comparison of Depressurization Transients for Three SBLOCA Sizes

The key parameters observable to the operators are sketched in Figure E.9. This composite trajectory of the parameters over time constitutes a signature or pattern for the SLOCA, confirmed in reading the FSAR and training materials, and, in the simulator, where the design-basis accident (DBA) SLOCA is standard fare.

The reference scenario ends when the core is reflooded, immediate danger to the core is over, and plant parameters have stabilized, i.e., at about 40 minutes. Long-term stability is assumed as are the operator actions necessary to insure that stability.

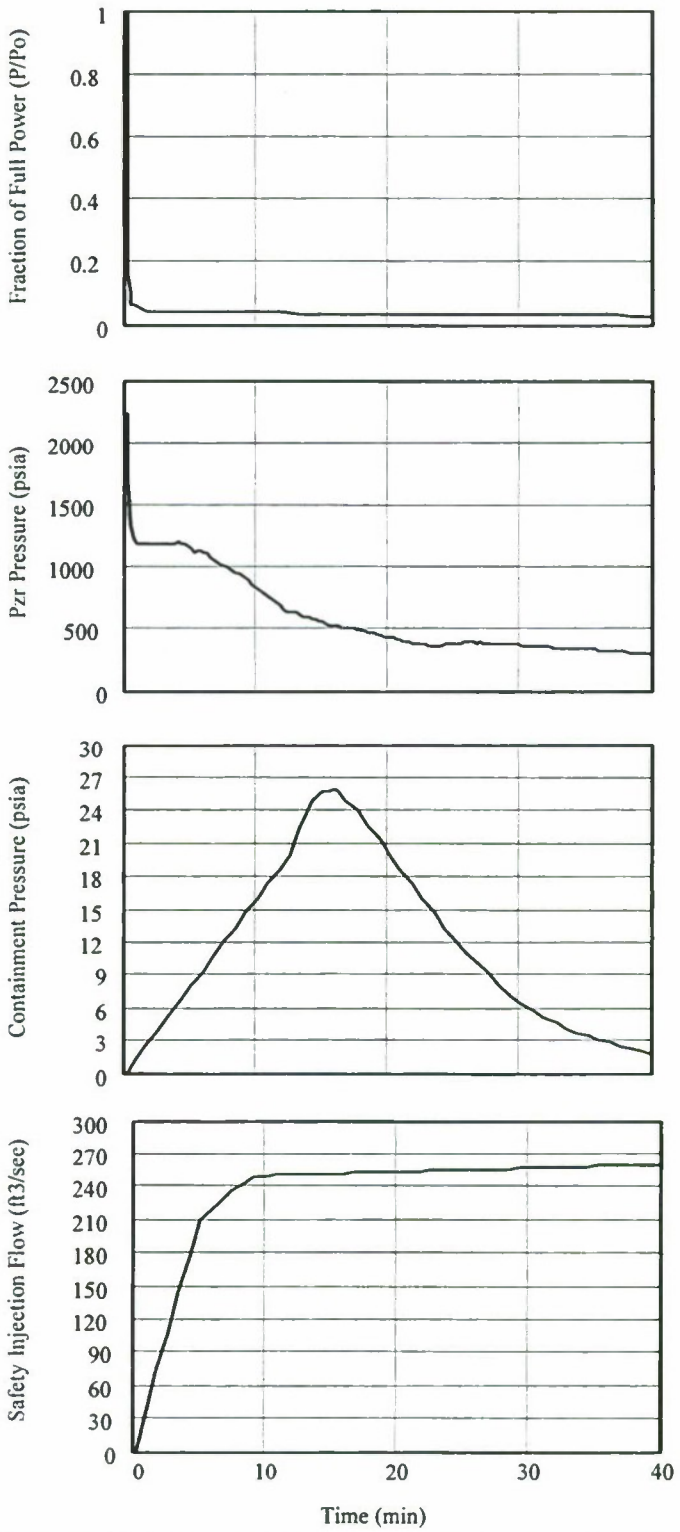


Figure E.9 Observable Parameters during SLOCA Reference Case

E.3.2 Description of the Base Case SLOCA Scenario

The base case scenario is equivalent to the reference scenario for the SLOCA over the first 40 minutes for several reasons:

- Conservatisms in the FSAR analysis of the SLOCA have only minor impact on the sequence of events and parameter changes that occur.

- The view of SLOCA held by operators is guided by their training, which includes the DBA SLOCA

  - operators undergo simulator training on the DBA SLOCA routinely, and
  - essentially all operators would define an SLOCA in terms similar to the reference case, i.e., the COM matches the reference case.

The base case scenario, however, extends well beyond the reference scenario in time. The parameters in Figures E.1 through E.8 had already stabilized. From this point on, power would continue its gradual decline, core pressure should begin to rise as the pressurizer begins to refill, ECCS flow remains about constant until pressure rises, manual switchover to recirculation cooling or RHR will be required, and peak and average clad temperature continue to decrease with falling RCS temperature.

Key points in the base case scenario not present in the reference scenario are

- Operators isolate the accumulators after switchover.[4]

- Operators align for long-term cooling, either placing the RHR system in operation or performing the switchover to recirculation cooling after the refueling water storage tank (RWST) level reaches 37% (to ensure sufficient emergency sump level to supply the RHR pump suction) and must complete the switchover before the pumps lose suction from the RWST (to prevent air binding, pump damage, and starving the core).

E.4 Step 4: Define HFEs and/or Unsafe Actions

The SLOCA event tree from the plant individual plant examination (IPE) is shown in Figure E.10. As shown in the figure, modeled systemic response to the SLOCA includes:

[4]This step is generally omitted from PRAs; thermal-hydraulic analyses in support of PRA indicate that nitrogen injection into the loops is not likely to significantly interfere with core heat removal.

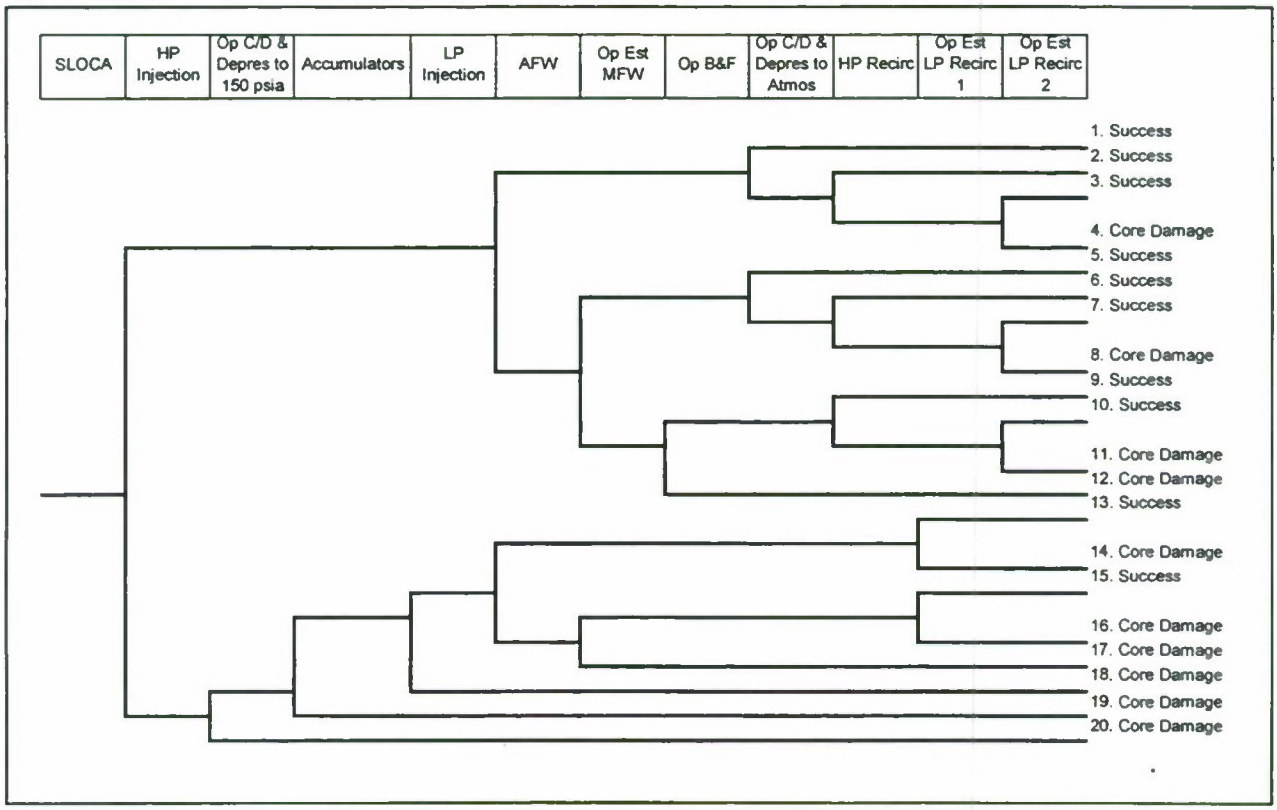


Figure E.10 Small LOCA PRA Event Tree

- high pressure injection (HPI, 1 of 2 pumps to 1 of 2 cold legs required)
- if HPI fails, operators must depressurize the RCS within 30 minutes to permit accumulator and RHR pump injection
- injection of the accumulator water (1 of 1 on the intact loop required)
- low pressure safety injection (LPI, 1 of 2 RHR pumps to the reactor vessel)
- auxiliary feedwater (AFW, 1 of 3 pumps to 1 of 2 SG)
- main feedwater (MFW), operators must align and restart (1of 2 pumps to 1 of 2 SG)
- operator establish bleed and feed (B&F) cooling within 30 minutes (open 1 of 2 pressurizer power operated relief valves (PORVs) and verify 1 of 2 SI pumps to 1 of 2 RCS cold legs)
- operator cooldown and depressurize to atomospheric pressure to minimize LOCA flow
- HP recirculation cooling (1 of 2 SI/RHR trains required)

- low pressure recirculation cooling 1 (LPR1, 1 of 2 RHR trains required); includes a required operator action to align LPR

- LPR2 is same as LPR1, except operators must depressurize via 1 steam generator (SG)

- each sequence ends in success or core damage.

Because the base case SLOCA lies just above the boundary between the small and medium LOCAs of the PRA, we examine the difference between the PRA's small and medium LOCA event trees and success criteria. First, the medium LOCA requires automatic HPI, where auto or manual is acceptable for the small LOCA. Second, if HPI fails, the medium LOCA tree requires starting operator controlled cooldown and depressurization to allow LPI in 15 minutes as opposed to 30 minutes in the small LOCA case. The last difference is that the medium LOCA case requires feedwater, only if depressurization to permit LPI is required. Similarly, B&F cooling is not required for the medium LOCA.

Finally, it should be noted that the rapid depressurization options, while potential last ditch efforts, are reached procedurally only through the critical safety function status tree for core cooling and function restoration guideline FR-C.1. This is a one-shot procedure for recovery in extremis. Likewise the MFW/condensate options are reached only through the critical safety function status tree for heat sink and FR-H.1. Thus these special actions are not reached in stepwise fashion through the procedures. If HPI fails, the EOPs instruct the operator simply to verify operation and start the pumps if they are not already running. No other recovery is directed until core exit thermocouples exceed 1200°F. This operational process is not clear from the event trees.

The ATHEANA process next asks that the systemic event tree of the plant PRA be reconstituted as a functional event tree and that other systems and human actions that can provide the same function be identified. For the SLOCA, this transformation is fairly complex because many system components and operator actions can supply each needed function as shown in Figure E.11. The functions are identified as follows:

- ***Early Makeup*** can be provided by HPI or by depressurizing—either dropping the leak rate to a point where charging pump output can match it or low enough to permit accumulator discharge followed by LPI. For pressurizer PORV LOCAs, operators can eliminate the need for makeup by closing the PORV block valves.

- ***Early Cooling*** can be provided by steaming the SGs using AFW or, if that fails, by following FR-H.1 to feed SGs with MFW, condensate, or even service water and, if all feedwater fails,

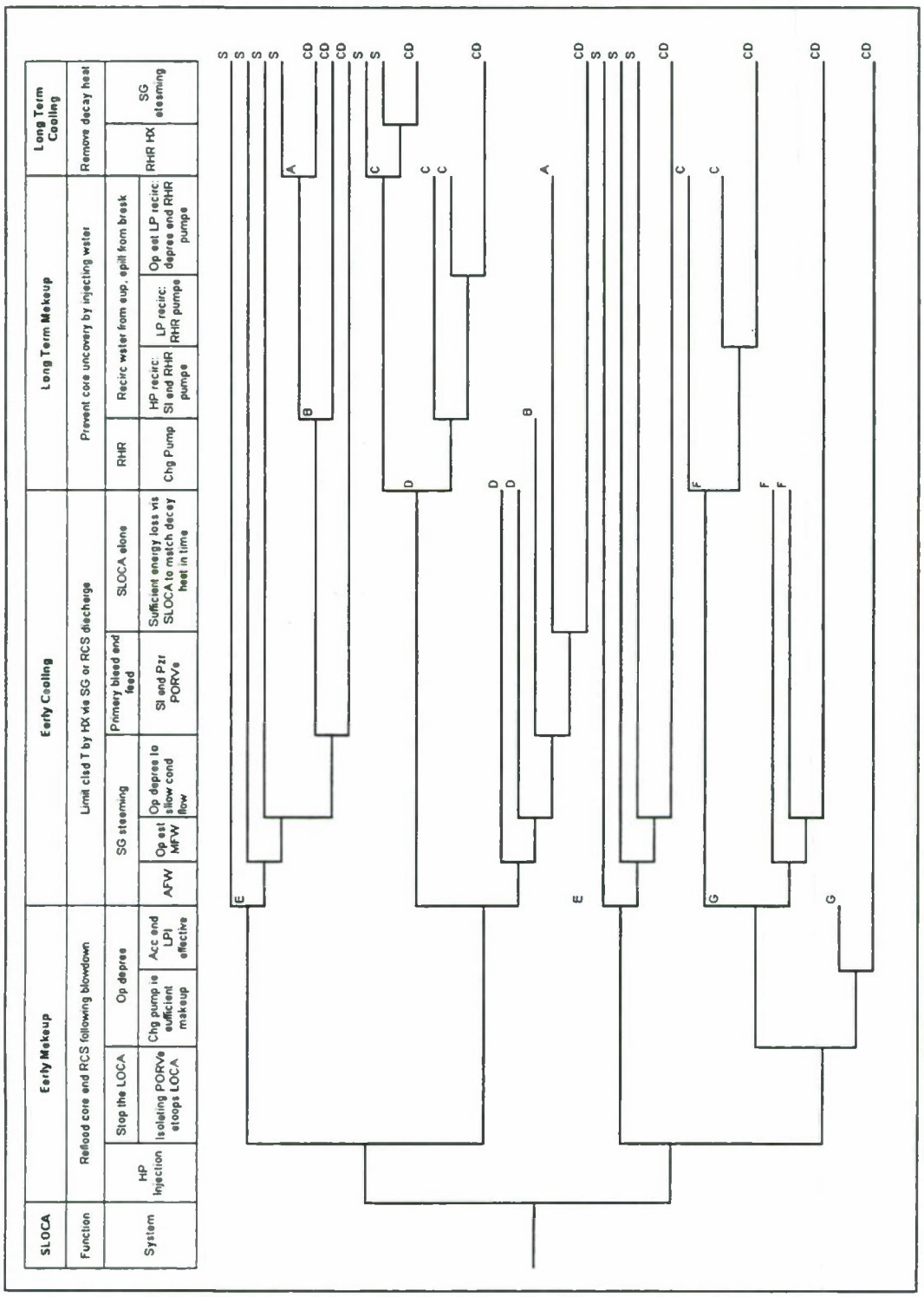


Figure E.11 Small LOCA Functional Event Tree

by aligning B&F cooling. Should B&F fail as well, it is still possible, for particular LOCAs (particular sizes and locations) and specific power time histories, that decay heat may drop to match LOCA blowdown heat removal before temperatures rise high enough to cause significant damage.

- ***Long Term Makeup*** can be provided by charging pumps if the RHR system is in service. If containment sump recirculation cooling is in operation, long-term makeup can be provided by HPR or LPR. If the plant had previously been depressurized, LPR can be placed in service directly. Otherwise, operators must depressurize the plant using an SG, before aligning LPR. Sump recirculation cooling must be initiated at an RWST level of 37% and the lineup must be completed before the RWST runs dry and the pumps are damaged.

- ***Long Term Cooling*** is generally expected to be provided by aligning component cooling water to the RHR heat exchanger for RHR or sump recirculation cooling modes. If that is not available, long-term cooling can be provided by steaming the steam generators, using hoggers, if necessary, to reach desired temperatures.

Application of the HFE identification Tables 9.6 and 9.7 of the main report would lead to a very large number of potential HFEs–several for every system level functional success criterion. Thus we need to establish priorities among all those possibilities. We first set a high priority on those issues that can lead to significant deviations in the physics of the initiating event or ensuing scenario and on those that can quickly lead to core damage. The issue of physics deviation requires a structured review that we will reserve until Step 6. However, we note at this time that failing to isolate an SLOCA associated with the pressurizer PORV can lead to conditions where steam pressures elsewhere in the RCS can be higher than in the pressurizer, which can cause the level to rise while voids are growing in the RCS. So we place a high priority on isolating the PORV. As for rapid onset of core damage, this is most likely to occur if operators interfere with HP injection or fail to align RHR or recirculation cooling before damage to the RHR pumps occurs.

Several cases appear low in priority, low enough to be screened from the analysis at this time. Later efforts in the search (i.e., identifying context that would elevate our concern) may re-introduce these issues. The first category would include errors of commission in disabling equipment that is unlikely to be needed: main feedwater, condensate, service water backup to AFW, and long-term SG cooling.

While most systems not likely to be needed can be dropped for now, until context is identified that can increase the likelihood that they will be called upon, a few will be included because their success has been important in existing PRA/HRAs. Early makeup actions to depressurize the RCS rapidly will be needed only if HP injection fails and the LOCA cannot be isolated. If the operators secure HP injection it will be because they do not believe it is needed (so they will not seek an alternative) or because they fear damage to the pumps or other equipment (in which case, they should already be planning for alternatives). The current structure of the procedures reaches this point only after the core exit temperature is very high, indicating that damage is imminent. Likewise, while it is unlikely that B&F cooling will be required, the frequency of its need has been found to be high

enough to affect risk. Therefore, failing to initiate B&F cooling is included. Note that interrupting B&F is not considered at this time, because its start requires conscious human action and we believe reversing that action will require some specific context. If a relevant context evolves out of the searches in Step 6, we can return to this issue.

The specific HFEs selected at this time include

- Operator improperly removes early makeup from armed/standby status (i.e., improper manual valve lineup blocks accumulator or RHR injection paths, control circuits blocked, or RHR pumps not in AUTO).
- Operator interrupts early makeup (i.e., operator inappropriately terminates RHR pumps).
- Operator fails to close or isolate pressurizer PORVs.
- Operator fails to depressurize RCS, when required.
- Operator fails to properly align RHR or containment sump recirculation cooling.
- Operator prematurely secures long-term makeup or cooling (RHR pumps or component cooling (CC) to the RHR heat exchangers).
- Operator inappropriately diverts resources (sump water).

All of these HFEs are within the scope of the issue defined in Step 1, if the reason for their occurrence can be attributed to a context in which the operators have difficulty applying the EOPs effectively.

E.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

To this point, the development and description of the base case SLOCA have been based on thermal-hydraulic calculations for similar events and highlights of the most salient operator actions that are required for successful response to the scenario. A more complete operational view of the SLOCA can be obtained by examining characteristics of the scenario including information on similarities to training and experience, event timing, identification of operator tendencies, tracking of the EOPs against the scenario, and identification of informal rules that may affect operator thinking. During this process, we develop information that is helpful in identifying potential vulnerabilities that may make the HFEs more likely than they are under nominal conditions. We post this information on our blackboard for ready access during the search for deviations in Step 6.

E.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

All PRW operators receive regular training on the DBA SLOCA of the base case scenario. Therefore their expectations are very strongly aligned with the base case. Many of these simulator drills begin with a small leak that progresses to the 3-inch SLOCA. Small leaks within the capability of the charging pumps are commonplace in drill scenarios. Actual SLOCAs have occurred often enough that they are within all operators' expectations. Several of those caused operational difficulties, but it is generally believed, by operators at our plant, that only the Three Mile Island-2 (TMI-2) accident got out of hand and the causes of that event have been fixed by the current EOPs, the addition of subcooling and reactor vessel level instrumentation system (RVLIS) instruments, and changes in the training program.

On the other hand, few operators receive training on SLOCAs smaller than 3 inches (but large enough to be beyond the capability of the charging pumps) or larger than 3 inches (those greater than 2 inches are called "intermediate LOCAs" in the PRA), so deviations of this sort will be outside of their training and experience. Rules (formal and informal) may not conform with scenarios that deviate from the base case. The timing of such scenarios will be unfamiliar.

In addition, there is a strong bias that the conservatism in the DBA means that real events will be less challenging than the training scenarios. There is, it would seem, a belief that operationally challenging scenarios will align with those thermal-hydraulically challenging scenarios of the safety analysis. This belief leads to a sense that drills involving more safety system failures than in the analysis are somehow "unfair" ("You can't take away more than one SI pump!"), as if nature must play by the single failure rules of our analyses.

While there is familiarity with the base case SLOCA scenario, that familiarity breeds vulnerability to scenarios that are similar but different in timing, impact on instrumentation, and kinds and numbers of failures, and can even contribute to disbelief if scenarios involve multiple failures.

E.5.2 Time Frames for the SLOCA

From the FSAR analysis in Step 3 and the discussion of the base case scenario, five distinct time periods can be identified. These are listed in Table E.3, along with a note of the potential for operator influence.

Table E.3 Time Frames for the Base Case SLOCA

Time Frame	Occurrences	Influences on/by Operators
Initial Conditions	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention.
Initiator/Simultaneous Events	Reactor power prompt drop Pressure drops below SI initiation point	These events are over before the operator even recognizes what is happening.
Early equipment initiation and operator response: 0-20 Seconds	Pressure drops to about 1200 psia and subcooling is lost Reactor and turbine trips ECCS flow begins MFW isolates and AFW starts Steam dump responds to turbine trip	During this time frame, the operator is checking parameters and ensuring appropriate standby equipment has started. Some early decisions in the EOPs may have occurred.
Stabilization phase 1-25 Minutes	Core reflood begins at about 10 minutes and has reached stable conditions by about 25 minutes Fuel temperatures have peaked and have fallen to match bulk RCS temperature Accumulators dump at around 10-12 minutes Pressurizer pressure has stabilized by 25 minutes and the SI pumps are delivering maximum flow Soon, as the pressurizer refills, pressure will begin to rise, SI pump flow will decrease, and subcooling will be restored	During this time, the operators have moved into the LOCA EOP and have passed a number of decision points.
Long term equipment and operator response	Isolation of the accumulators Shift to RHR or cold leg recirculation cooling Repair and recovery	Until alignment of RHR or switchover to cold leg recirculation cooling, the operators are occupied with confirmatory steps in the EOPs, depressurization, and cooldown. Any complications beyond the base case scenarios can impact their performance. This longer time frame extends to days and months. There are no critical operations concerned with the base case scenario, other than the decision to use RHR or recirculation cooling. Problems during this phase would be the concern of a low power and shutdown PRA.

By the end of the first 25 minutes, the potential for immediate damage is over; i.e., the LOCA and its direct consequences are finished, without damage to the core. All that remains is the long-term control of stable conditions. Note, however, that the operators have a number of important activities remaining, especially switchover to RHR or recirculation cooling.

E.5.3 Operator Tendencies and Informal Rules

Of the operator tendencies presented in Table 9.12a of the ATHEANA process, most factors in the SLOCA base case scenario induce appropriate tendencies to control the scenario. For example, low pressurizer level and pressure induce the appropriate tendency to increase injection. They also point toward isolating LOCA paths, decreasing letdown, and turning on pressurizer heaters.

However, after the initial blowdown, if the SLOCA is in the pressurizer, level can begin to rise, as pressurizer pressure is vented and voids form elsewhere in the RCS, possibly threatening the core. The tendency for increasing pressurizer level is to reduce injection and increase letdown–exactly the wrong response. Also later in the accident, high core heat removal (here due to the LOCA blowdown) would, in itself, encourage undesirable tendencies to decrease injection. It would also create a tendency to decrease RCS forced flow.

High containment pressure and temperature would encourage containment isolation, cooling, and spray, all useful tendencies.

A number of informal rules and practices that operators in this plant tend to observe could impact the base case SLOCA and deviations from it. A generic list of informal rules was provided in Table 9.13 of the process and, using the table to guide our thinking, we have evaluated them on a plant-specific basis. We have also evaluated plant-specific practices. The results follow:

- Protect Equipment. A recent history of running two balance of plant pumps to destruction through cavitation and overheating has made operators acutely aware of the hazards to pumps of operating with insufficient net position suction head (NPSH) and dead headed. Vibration noise is one of the factors they are most sensitive to.

- Recent History of Performance. A series of recent problems with the Channel A pressurizer pressure instrument has made operators suspicious of its performance. They tend to follow Channel B, rather than auctioneered pressure.

- Crew Characterization. Formal communications, strong shift supervisors (lower watch standers seldom question supervisor's judgments), low tolerance for perceived gaps in knowledge.

- Lack of Deep Technical Knowledge. Few shift operators have deep understanding of instrument sensor design and the algorithms used in the I&C circuits. Instrument technicians are available during day shift and can be contacted/recalled on back shifts.

Step 6 will investigate potentially negative impacts of these tendencies and informal rules in the face of deviations from the base case or other complicating factors.

E.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

Perhaps the best operational view of the scenario can be developed by tracking those elements of the EOPs that are processed in the SLOCA. A "map" of these procedures is provided in Figure E.12 (provided at the end of this chapter because of its large size). The expected procedural pathway for the base case SLOCA is shown by solid arrows. The procedure map tracks all key decision points in the EOPs: (a) branch points to other procedures, (b) internal steps that disable plant functions (i.e., stopping particular plant components that can supply sometimes needed functions), and (c) steps that call out a major reconfiguration of equipment. Figure E.12 combines all procedures carried out during the base case SLOCA scenario. At each decision point (e.g., E-1, Step 2 in Figure E.12), a table in the figure provides the following information:

- Actions to be taken
- The potential for ambiguity in the decision criteria in the base case
- A judgment on the significance of taking the wrong branch or inappropriate action.

All steps that disable plant functions are indicated by hexagonal boxes (e.g., E-0, Step 20 in Figure E.12). This information is expanded to support the deviation analysis search process by indicating deviation classes under which ambiguity is increased and changes in the significance of taking wrong branches due to effects of possible deviations. For cases in which the significance could be high, the box is **bold** and the key aspects of the significance are shown in ***bold italics***. For those cases, relevant potential ambiguity is also shown in ***bold italics***. The examples cited above show these characteristics. This information will be used later in Step 6, in combination with information concerning informal rules and operator tendencies, to help insure that the consideration of deviations includes identifiable "bad actors."

The path through the procedures for the base case SLOCA is very clear and unambiguous, with the possible exception of the approach to and the decision about selecting RHR cooling or sump recirculation cooling in ES-1.2, Step 24. At this point in the accident, operators are cycling through Steps 3 to 26 of ES-1.2 Post LOCA Cooldown and Depressurization as they depressurize, cooldown, refill the pressurizer, and begin to restrict SI. There are several delicate steps in this process and one that is fairly complicated. They depressurize to allow the pressurizer to refill; depressurizing too quickly will allow voids to occur in the RCS, with resulting rapid increase in pressurizer level. Average RCS temperature (which identifies P_{sat}) must be played against pressurizer pressure to ensure subcooling to avoid erroneous level indication and passing water through the PORVs. Subcooling and pressurizer level requirements change as they proceed through these steps. Step 11, where SI pumps are stopped, has multiple requirements that depend on several plant parameters and warns that time must be allowed for pressures to stabilize after pump stops to avoid incorrect action.

If the operators are able to stabilize plant conditions including subcooling, pressurizer level, pressure <425 psig, and temperature <400°F, it is possible to place the RHR system in operation, but this

decision must be made in consultation with the Emergency Director. A lengthy discussion with plant operators and trainers indicates that this is not such an easy decision. For LOCAs near the DBA SLOCA, we are just at the point where the leak is large enough that repressurization and control are difficult and cooling is still a worry (a little larger and the heat removal through the break causes cooldown on its own). In addition, there are concerns about the viability of RHR, with regard to location of the break. If the break were in the wrong spot, aligning RHR could bypass the core. Then rising core exit thermocouples would be the only indication of the problem. The trainers, who work the technical support center during real emergencies, expressed the view that most operators would lean toward recirculation cooling because that is where the main expectations through training lie, but acknowledge that in all SLOCAs that have occurred (except the TMI-2 accident), RHR has been used. The trainers felt it would be a good exercise. Our view is that the decision point could be a source of delay and distraction, depending on the particular SLOCA.

Taking wrong branches that preclude being alert for early switchover to recirculation cooling (i.e., any path off the SLOCA path) could have serious consequences, because the time available for switchover is short and failure will lead directly to core damage.

In addition to the Figure E.12 information, the EOPs provide for continuous monitoring of "critical safety functions." CSF F-0.6 Inventory is the earliest indicator of problems and requires monitoring of the following:

- Pressurizer level (>19%)
- RVLIS (void fraction % stable or decreasing or RCP A&B OFF ≥100%).

Depending on the outcomes of these decisions, other function recovery procedures may need to be entered if additional complications occur during the scenario. These procedures ensure that operators are reminded that injection is required if pressurizer level is low. If the level is high, steps are recommended to compress voids. In particular, for SLOCA, we already noted that CSFs F-0.2 Core Cooling and F-0.3 Heat Sink are particularly important when failures of HP injection or AFW occur.

E.5.5 Summary of Potential Vulnerabilities

At the close of Step 5, we have posted on our blackboard the information collected on training and experience, time frames, operator tendencies and informal rules, and the EOP map and are ready to begin the systematic search for deviations from the base case scenario in Step 6. Before moving ahead with the search, it will be helpful to summarize the most interesting potential vulnerabilities uncovered during Step 5. That summary is presented in Table E.4.

Table E.4 Summary of Potential Vulnerabilities for SLOCA

Consideration	Observation	Vulnerability/implication
Training and experience	Annual DBA training	Expectations aligned with base case; similarity bias
	No training on SLOCAs greater than the base case	Unfamiliar, therefore weak knowledge; must adapt DBA
	Little or no training or experience on SLOCAs less than the base case, but greater than charging pump capacity	Unfamiliar, therefore weak knowledge; must adapt DBA
	Bias that DBA SLOCA is most severe and conservative case	Multiple equipment failures or ambiguities in procedures not seen in base case may strain credulity and lead to unexpected operator response
Time frames	SLOCA stabilized by 25 minutes	Intervention during this time period, while unlikely, could be serious.
	Approach to long term cooling depends on exact SLOCA; choice of RHR/recirculation may not be clear	Short time available to effect alignment/switchover.
Operator tendencies	Tendencies: most are appropriate and helpful. However, the tendency for high core heat removal and the tendency for rising pressurizer level is to decrease injection	Taken alone, overcooling or rising level implies reduced injection flow
Informal rules	Pumps will be damaged by low NPSH and deadheading	Strong tendency to stop pumps with suspected vibration noise
	History of channel A pressurizer pressure problems	Believe channel B
	Crew follows formal communications practice, with very strong shift supervisors	Low tolerance of knowledge gaps Lower level watch standers are hesitant to question shift supervisors
	Lack of deep technical knowledge of I&C, especially instrument and sensor design, and physics algorithms. No technicians on back shifts.	Operator confusion is likely if deviations from base case operations requires detailed knowledge of I&C systems

Table E.4 Summary of Potential Vulnerabilities for SLOCA (Cont.)

Consideration	Observation	Vulnerability/implication
Formal rules/EOPs	No significant ambiguities identified for the base case, except for ES-1.2, Step 24, which requires that Emergency Director decide if RHR should be placed in service. No criteria are given in the procedure for this decision. A number of steps with high potential significance were identified, which could become ambiguous depending on the deviation from the base case.	See Figure E.12 for details. Potentially significant consequences can be found at: E-0, Steps 3, 4, 6, 11, and 18-20 E-1, Steps 1, 2, 6, 12, 14, 16, and 18 ES-1.2, Steps 3, 9, 11, and 14

E.6 Step 6: Search for Deviations from the Base Case Scenario

This search is structured to identify key elements of plant conditions and some aspects of performance shaping factors that can be primary elements of EFC context for scenarios that deviate from the base case SLOCA. The resultant EFC elements will be refined in later steps of the process. Up to this point in the analysis, the process has been straightforward, proceeding in a well-defined, step-to-step progression. However, the searches described in Step 6 of Section 9, while structured, involve substantial iteration, free-wheeling exploration, and intuitive integration.

Caveat: The analyst new to ATHEANA must resist being fooled by the stepwise presentation of the search in the following paragraphs. What you are about to read is the result of many trials, dead ends, and misdirections. As described in Section 7 of the report, the ATHEANA analysis requires a broad range of multidiscliplinary knowledge: behavioral and cognitive science, the plant-specific design and PRA, understanding of plant behavior (including thermal-hydraulic performance), understanding of the plant's operational practices (including procedures, training, and administrative practices), and generic and plant-specific operating history (including incident history, backlog of corrective maintenance work orders, and current workarounds). The analysts bring this catalog of knowledge to bear, along with the blackboard full of information collected in Step 5, to find the "most significant" deviation cases. The mental process that allows this integration is complex, not well understood, and not well suited to a step-by-step description, just as the view of a chess game by an expert is more complex and effective than a brute-force look-ahead computer program. The process requires a strong facilitator/integrator, who has broad general knowledge of all the disciplines and can challenge any other experts involved in the process. Finally, even if a single analyst can bring all the requisite knowledge to the table, it is essential that others be involved to challenge assumptions, short cuts, and possibly overly narrow analysis.

E.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

This search proceeds in the manner of a hazard and operability analysis (HAZOP), by applying the series of *guide words* introduced in the process description to the base case SLOCA scenario. For

each guide word, we seek physical changes associated with the initiating event that could enable the guide word. [Scenarios can also deviate from the base case because indicators (instruments) follow the guide word, while the scenario is otherwise undisturbed, until the control systems or operators intercede, because of the deviation in instrument response. Such situations are reserved for Step 7, where other complicating factors are considered.]

Using Section 9.6.3 of the process description, the first guide word we apply is "No or Not." The idea is that the guide words trigger the imagination of the analyst to identify potentially significant scenarios. There is no concern that the guide words be independent and there should be no wasted effort worrying if a particular deviation case should be categorized under one guide word or another. The guide words are not tools for categorization, but stimulants to the imagination.

What does it mean for there to be "no" SLOCA? It could mean that the plant says it has a LOCA, when there really isn't one. In thinking this way, the plant says it has a LOCA by initiating SI (spuriously or in response to a low pressure signal) or by exhibiting low pressurizer pressure or level.

"No" SLOCA could also mean that the loss of coolant itself is less than that assumed in the DBA of the base case or that some physical parameters of the plant behave as if the SLOCA were smaller. Note that, if the SLOCA is small enough, it ceases to be an SLOCA initiator and is simply a leak, within the capabilities of the charging pumps.

"No" SLOCA Deviation Case (Spurious SI). A number of plants were plagued with spurious SIs early in their lifetimes, due to instrument problems. In plants with high head centrifugal charging pumps that start on SI, pressures can go well above normal (about 2600 psig), so overpressure and sticking open of pressurizer PORVs and safety valves would be a concern. In our plant, where normal operating pressure is well above the shutoff head of the SI pumps, the only thing that happens is that the SI and RHR pumps operate against their shutoff heads; i.e., they will soon overheat, if not turned off, and be damaged, making them unavailable if needed later. Because of plant concern for pump safety, this could become important, if combined with substantial additional challenging context.

Probably the most significant danger in the spurious SI was that operators would begin to expect it, quickly stopping SI pumps, even if they should not. The current EOPs were developed to avoid such responses, requiring that a suite of conditions be met before terminating SI. The EOPs track quite nicely for this event. Eliminating the source of the mental bias, the spurious SIs themselves, is, nonetheless, a significant measure, because strong mental bias can override procedures and training when the context becomes challenging and often when we least expect it. Given that our plant has no history of spurious SIs and that this event will not cause a pressure excursion, this event appears to have little chance to become significant and will be put aside for now.

An unnecessary SI can occur if pressure is low, but inventory has not been lost. Such events have occurred elsewhere because of stuck open pressurizer spray valves and overcooling events. The latter also lowers pressurizer level. While such events can cause confusion, they are outside the

scope of the issue defined in Step 1. They could add challenging context to reactor/turbine trip or loss of feedwater scenarios.

The spurious SI can be human induced by the actions of an instrument technician. However, we can envision no downstream dependencies associated with that activity.

"No" SLOCA Deviation Case (< 3 inches). The SLOCA can be smaller than the base case if the break size in the RCS is less than the 3-inch break assumed in the FSAR. For a 2-inch break, the depressurization transient was shown in Figure E.8. As break size decreases, the time to reach saturation at about 1200 psia is longer and the time at 1200 psia is extended. Likewise, the time until switchover to RHR or recirculation cooling is extended. The EOPs track this event quite well.

The only problems we envision for these smaller SLOCAs are that (1) focus on RHR cooling may divert attention from the RWST level (thus the low level alarm on the RWST becomes more important as a reminder that time is running out to align long-term cooling) and, conversely, (2) if expectations are strongly aligned with the base case SLOCA, there may be a failure to consider RHR cooling for long-term cooling. In the former case, failure of that alarm could jeopardize successful switchover. The latter case is not particularly significant from a safety standpoint, unless significant additional context combines with this circumstance to create delays or hesitancy, because high pressure recirculation cooling will provide long-term stability.

"No" SLOCA Deviation Case (Physical parameter behavior). The other class of "No" SLOCA scenarios that deviate from the base case SLOCA involve physical parameters of the plant behaving as if the SLOCA were smaller. Parameters identified in the reference case included

- Power. It could fail to drop on SLOCA if the core were over-moderated because of a fuel load error or a violation of control rod program management. This is certainly outside the range of training and operator mental models and could result from human unsafe acts. For now we assume that the probability of such events is low compared to other possible contributors, but it might be worth pursuing at a later date.

- Pressure. Only one phenomenological reason for delayed pressure drop has been identified. One channel of pressurizer pressure displays a processed signal, whose algorithm involves current sensed pressure, the time history of pressure for approximately the past 10 minutes, and the rate of change of pressure. Few operators are aware of this. If the SLOCA is small enough and if that channel of pressure indication is selected, then indicated pressure could lag actual pressure, giving a indication that the SLOCA is smaller than it actually is. We believe that this is such a minor and transient effect that there is no way that it will adversely affect human performance for the base case SLOCA. It is not included in summary discussion of the deviation analysis.

- Pressurizer level. As mentioned earlier, pressurizer steam space SLOCAs can behave quite differently than RCS SLOCAs, affecting level. This case is discussed in more detail below.

- Break flow. No phenomenological reason other than an actual smaller SLOCA for lower break flow has been identified and that case was discussed earlier.

- Containment pressure. The impact of passive heat sinks in the containment could significantly delay pressure rise and peak values. No important impact on operator performance has been postulated.

- ECCS flow. ECCS flow can be blocked because of pump or valve failure and these cases are modeled in the PRA. Such failures could be due to a previous HFE in which the operator improperly removed the equipment from the armed/standby status. Given the plant surveillance process, such a situation is very unlikely (although it happened at TMI).

  "Less" ECCS flow can occur, because of obstructions or impaired pump performance, or because a smaller SLOCA has occurred and pressure remains too high for full SI pump flow. The smaller (< DBA) SLOCA scenario was analyzed earlier. The actual impaired flow scenario falls naturally into two cases: those in which flow is reduced below that required to survive the initiator (this case is modeled in the PRA systems analysis) and those where it is sufficient for long-term success, but decidedly less than expected and, perhaps, less than needed to meet design criteria early on. Such cases again break into two. The first group can be immediately satisfied by depressurizing and allowing full flow by low pressures sources. Although this appears straightforward, especially in the SLOCA PRA event tree, it was pointed out in Step 4 that the procedural link to this action comes only through the critical safety function status tree for core cooling, when core exit thermocouples read greater than 1200°F. Additional context that interferes with that procedural jump would be important. In the second, flow is initially inadequate (from degraded low pressure sources or the charging pumps with decreased loss rate due to depressurization), which would delay core reflood (not observable to the operator), possible fuel damage resulting in high fission products in the RCS, and, possibly, delayed switchover to long-term cooling. Of these, the only one that is likely to be observed and of concern to the operator would be the high fission product concentration in the coolant. It is difficult to see how this would cause significant problems to the operator other than minor confusion and concern, unless this extra burden intensified the pressure due to other outside EFCs.

- Accumulator dump. Improper nitrogen pressure on the accumulators would delay or speed up their discharge, with little anticipated impact on the accident progression or, therefore, on operator response. From thermal-hydraulic analyses of LOCAs with and without accumulator discharge, impact of such problems on operator performance seems unlikely.

- Core reflood rate and timing. No phenomenological reason for delayed reflood has been identified, other than reduced ECCS flow or void formation due to a pressurizer steam space SLOCA, both described above.

- Clad temperature. No phenomenological reason for decreased clad temperature has been identified.

When we applied the other negative guide words ("Less," "Late/Never," "Too slow," "Too long," and "Part of"), we found that all lead the analysis to the same result. In this example, "No" is a surrogate for all these other words.

"No" SLOCA Deviation Case (Pressurizer steam space SLOCA). When the SLOCA occurs in the pressurizer steam space,[5] several unique processes occur. At first, the break involves only pressurizer steam or water. When pressure falls to RCS saturation pressure, the RCS fluid flows toward the pressurizer and out the break. As far as our consideration of effects on the operators is concerned, there are two primary observable manifestations of the steam space SLOCA:

- If the pressurizer vents its steam to containment more quickly than its volume is replenished by the SI system, pressurizer pressure drops below that of the saturated RCS and voids form at hot spots around the system (most likely in the core; also in the SGs, if they are not steaming). With higher pressure in the RCS, the expanding voids force water into the pressurizer and level rises quickly, even as mass is lost from the RCS.

- If the SLOCA is via the PORVs or safety valves, initial flow is into the pressurizer relief tank; i.e., the containment sees no humidity, radiation, or increasing pressure. RT pressure rises.

Figure E.13 sketches the kinds of change in parameter trajectories associated with this deviation. After initially falling, pressurizer level begins to rise, as voids form in the RCS. Pressurizer pressure will indicate slightly less than for a similar size RCS rupture (perhaps overemphasized in the sketch), because of venting in the pressurizer. If the SLOCA is via a PORV or safety valve (SV), containment pressure would be delayed until the pressurized relief tank (PRT) rupture disk (or the SV downstream rupture disk) ruptures and, if RCS pressure falls below the shutoff head of the RHR pumps, SI flow would increase dramatically.

Although operators have been sensitized to this case by the TMI-2 accident and new procedures and instruments were developed to protect against it, the scenario still offers challenges. To better understand this deviation case, we play the scenario against the EOPs, as represented in Figure E.12. We first observe that the procedures work, but we should look more closely at several steps where challenges could occur. With no additional equipment failures, the operators proceed to Step 19.a, where they check whether the pressurizer PORVs are closed; close them, if open; or isolate them by closing the block valves, if the PORVs cannot be closed. This step will end the SLOCA, if it is via a PORV, if the valve position indicators are indicating properly, and if the valves respond to closing signals. If the valves cannot be closed, the EOPs branch to E-1, Loss of Reactor or Secondary Coolant. So at this point one of five things happens:

[5] Pressurizer water space SLOCAs are included, because they will quickly become steam space SLOCAs as the blowdown progresses. SLOCAs via a PORV, a relief valve, or a break anywhere along the surge line, in the pressurizer, or in its taps will behave as a pressurizer steam space SLOCA.

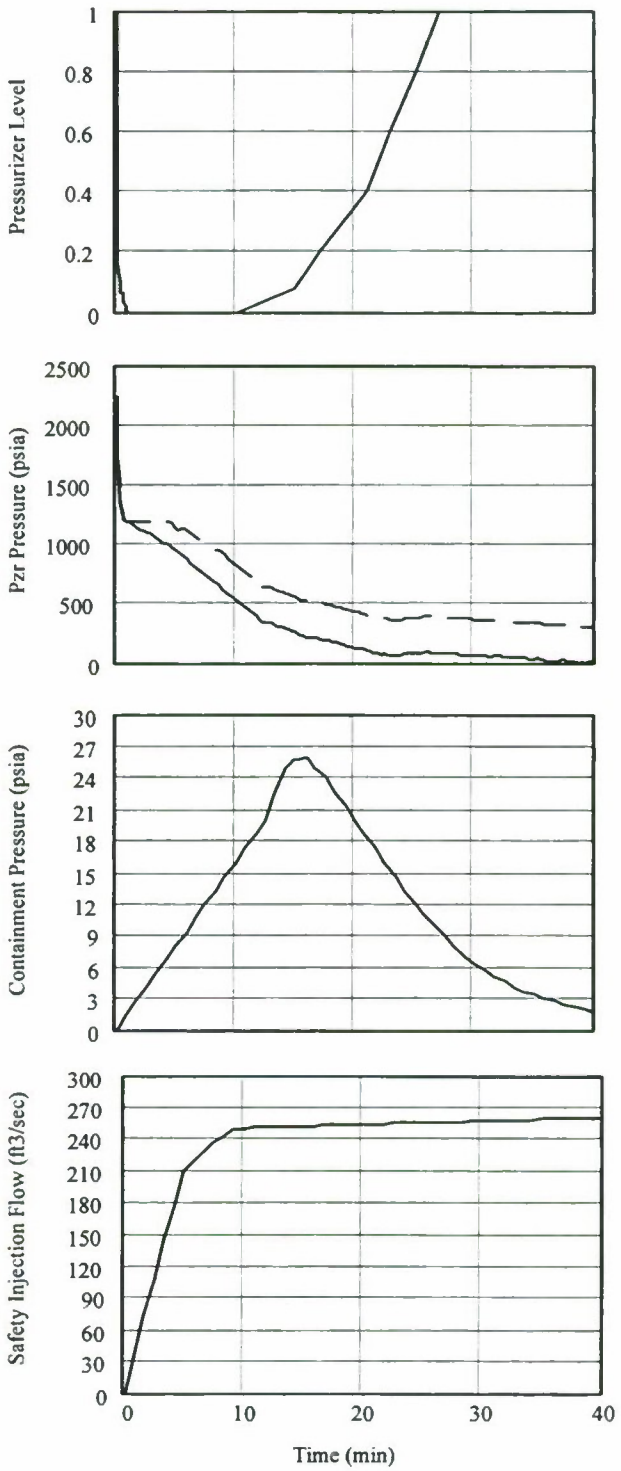


Figure E.13 Observable Parameters during Pressurizer Steam Space SLOCA Deviation Case

(1) The SLOCA is stopped. HP SI continues until the pressurizer refills and the SI pumps reach their shutoff head or until they are stopped by procedure or for some other reason.

(2) The valve position indication fails, with a PORV stuck open. This condition requires a valve failure and, perhaps, an instrumentation failure. (It may be possible for the valve to fail in a way that causes an erroneous indication.)

(3) The PORV is stuck open and the block valve fails to close. This requires two valve failures.

(4) The operators fail to properly carry out Step 19.a, continuing in the procedure with a PORV stuck open.

(5) The SLOCA is via a stuck open SV or a pipe/vessel rupture.

In the *first* case, the event is essentially over. The operators should proceed into E-1, where, at Step 12, they should transfer to ES-1.1, SI Termination. In the *second*, the operators continue believing that the PORV is shut when it is really open; i.e., they are set up for an incorrect situation assessment. In the *third* case, they know that a path from the pressurizer is open. Even though the probability of two valves failing might not be as low as one would expect,[6] this case is not particularly challenging, because the source of the SLOCA is known. Operators would branch to E-1 and later to ES-1.2, Post LOCA Cooldown and Depressurization, where SI would be reduced, the RCS depressurized, and one RCP started, which would mix any steam pockets with liquid reactor coolant, restoring pressure control to the pressurizer. At Step 24 the operators, in consultation with the Emergency Director, will decide if they should place the plant on RHR closed loop cooling, a step that can involve a difficult decision. The *fourth* case involves a lapse on the part of the operators, missing a step in the procedure and missing the open valve indication. Additional strong context would be required for this to become a significant problem. The *fifth* case is a LOCA via the SVs or a pipe/vessel break. Operationally, this looks very much like the stuck open PORV with failed position indication of the second case, in that the operators are likely to believe that the LOCA is not in the pressurizer steam space.

In all five cases, the procedures can work. The second and fifth would appear to be the most likely to cause later problems, because the operators will have formed an incorrect situation assessment. We continue this analysis of the EOP under the assumption that the PORV is open but indicating closed. The other cases will be revisited only if an additional challenging context is identified that makes them more significant.

We continue to track the second case (failed indication that PORV is stuck open) through the procedures at E-0, Step 19.b, believing that the PORV is closed. The operators are expected to have no problems due to the deviation in E-0 and should successfully transition to E-1. In E-1, all should

[6]If, by this point in the procedure, voiding in the RCS has already occurred, passing liquid through the PORVs could have further damaged them. Likewise, the block valves are not designed to close against flow, so the continuous passage of water or a steam water mixture could also lead to block valve failure.

go smoothly and at Step 18 RCS pressure will be >150 psig, so the operators should transition to ES-1.2. Because the base case did not make this transition, ES-1.2 is mapped separately in Figure E.12, which is also shown at the end of this appendix.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes could almost double the break size and create confusion. When the SI pumps have run long enough to reestablish subcooling margin, depressurization can begin. This may be a difficult condition to reach, with no RCPs running, if large voids have formed in the RCS.

Next a warning is provided at depressurization Steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing pressurizer (Pzr) level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. Nevertheless, if the context becomes sufficiently challenging, old rules can be enabled, such as the "Don't go solid" informal rule. Note that they have likely had a solid pressurizer for some time which could trigger undesired actions.

Finally, the SI pump stop criteria in Step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading as the result of an incorrect action. Transfer to sump recirculation could be delayed because of belief that transfer to RHR cooling will occur soon. In addition to all this, the goal of ES-1.2 is to place the RCS on long-term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the Emergency Director does not choose to place RHR in service in Step 24.c (e.g., because of concerns about break location) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

One HFE identified in ATHEANA Step 4 has already occurred: Operator fails to close or isolate PORVs. Three additional HFEs could be enabled:

- Operator interrupts early makeup.
- Operator fails to depressurize RCS.
- Operator fails to properly align containment sump recirculation cooling or RHR.

The first and third HFEs are not likely without further and sufficiently challenging context. The second, failing to depressurize, could occur because of difficulties in controlling the depressurization operation, with uncollapsed steam bubbles in the RCS. Returning to the vulnerabilities summarized in Table E.4, we observe that

- The operators' bias is that the base case SLOCA is the most challenging case.

- The history of Channel A Pzr pressure problems would be unimportant without failure or erroneous indication on Channel B.

- The tendency to decrease injection with rising pressurizer level could come into play.

- If the shift supervisor takes wrong action, because of their mistaken situation assessment, the other members of the crew are unlikely to challenge that action.

- Lack of deep technical knowledge of I&C, in particular reactor vessel level indication system (RVLIS), could lead to confusion.

At this point, the possible physical deviation is well defined and has been determined to be important enough to proceed to the next part of the analysis. The results of the application of the guide word "No" to the SLOCA base case are summarized in Table E.5, which is provided at the end of the guide word analysis of this section. What remains is to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

The deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that the "No" SLOCA Deviation (Pressurizer steam space SLOCA) case involves at least five different, potentially troublesome characteristics:

- Large change in parameter; under the deviation scenario, this characteristic can affect situation assessment and response planning. In itself, this factor may have minor impact, for the drop in pressure and the initial drop in pressurizer level. These changes are well within the range observed in training scenarios. However, the large and rapid rise in level a short time later will be troublesome.

- Relative rate of change in two or more parameters is not what would have been expected; can affect situation assessment.

- Changes in two or more parameters in a short time; can affect situation assessment.

- Direction of change in parameters over time is not what would be expected; can affect situation assessment. The training our operators receive creates an expectation that steam space SLOCAs occur via the PORV and that valve indicators are accurate.

All these human complications would spell difficulty for the operator and could support the HFEs listed above. Nevertheless, the procedure can guide them through the situation successfully, if the context does not lead them to take the associated unsafe actions. For the case examined, a PORV must stick open and its position indicator must erroneously indicate closed. Additional factors, such as those identified as causing increased ambiguity in the EOP discussion above, would make the unsafe acts more likely.

"More" SLOCA Deviation Case. The next guide word to consider is "More." (The related words "Early," "Too quick," and "Too short" do not appear to be useful distinctions when applied to SLOCA.) This requires a break size greater than the 3-inch DBA SLOCA. Consider three cases:

(1) A LOCA somewhat bigger than the DBA SLOCA, but far from the DBA LLOCA
(2) An SLOCA that grows into a near-DBA LLOCA, and
(3) A very large LOCA, beyond the capability of the ECCS.

The *first* case is identical to the "No" LLOCA Deviation (<DBA) case of Appendix C (see Figure C.14). Please refer to that description of the deviation case, where the analysis argues that significant additional EFC is required to seriously challenge the operators. This case was dismissed in Appendix C, because it fell beyond the issue of physical deviations for the LLOCA. It will be considered here in our summary tables and further analysis, based on the description in Appendix C.

The *second* case is very similar to the LLOCA "Switching" Deviation case of Appendix C. The primary difference is that the physics of the situation are more likely in a normal plant, i.e., one that does not contain a flaw making temporary plugging of a LLOCA feasible. It is discussed in detail below as the "Growing" SLOCA Deviation case.

The *third* case was discussed as a deviation on the LLOCA, which is appropriate as it is even more severe than the DBA LLOCA. As described there, some of the scenarios in this group could be survived, if more than the minimum ECCS works, and that is the most likely case. These would not be generally more challenging than the base case LLOCA, as the operators would not know that the LOCA was larger than the DBA and the actions in the EOP for the DBA are equally appropriate for this case. However, should the LOCA be just beyond the capacity of the ECCS, actions to minimize the extent of core damage and reach long-term stability could be very challenging. This event is beyond the scope of the current issue, as defined for this analysis, and will not be discussed further.

"Growing" SLOCA Deviation Case. Here, as shown in Figure E.14, we begin with an SLOCA that begins to refill the pressurizer at about 20 minutes. Over the next 1.5 hours, the crew continues through E-1 and ES-1.2 to stabilize the plant–restoring subcooling margin, securing RHR pumps and SI pumps, stabilizing pressurizer level, and cooling down (reducing RCS temperature and pressure). They have the SLOCA well in hand after having a busy time of controlling conditions to permit placing RHR in service or switching to HP sump recirculation cooling. As they have depressurized, they needed to watch pressurizer level and subcooling very closely to prevent voiding in the RCS as discussed at Steps 9 and 14 of ES-1.2. Now they have a respite, with a stable plant in a well understood condition. It is at this time that the full LLOCA occurs, possibly catching the operators unawares, with no automatic way to re-establish low pressure injection.

Let us take a closer look by tracking the "Growing" SLOCA scenario through the EOPs. Again we begin with the procedure map of Figure E.12. The early plant response would carry the operators through the initial stages of E-0 with little question. If they notice the increasing pressure and limited injection flow, they might begin to suspect a steam or feed rupture inside containment. In

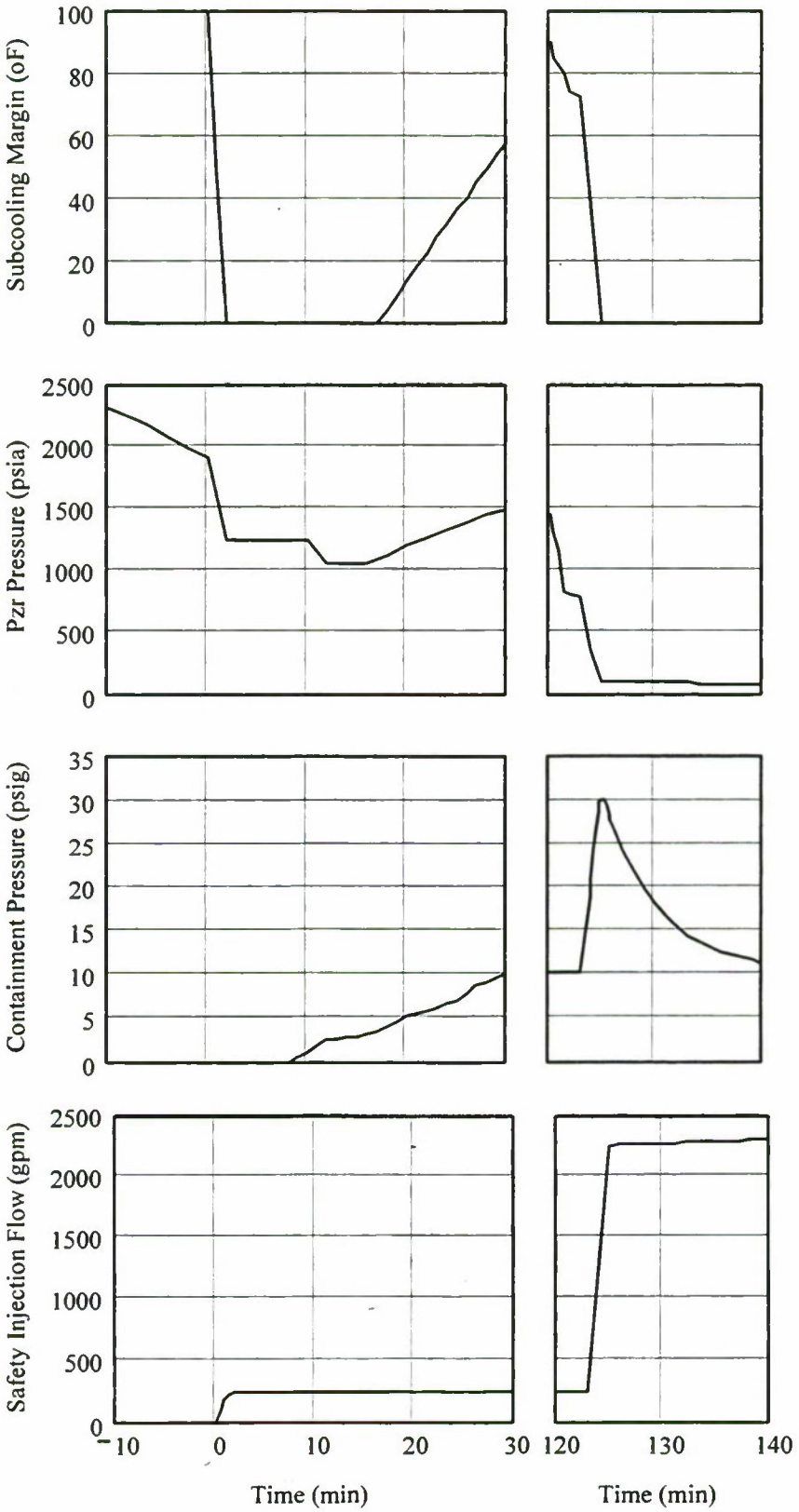


Figure E.14 "Growing" SLOCA Deviation Case

any case, faith in the diagnostic power of E-0 will still be strong. At Step 21, they should find no need to transfer to E-2, the faulted SG isolation procedure, as all SG should look the same. Even if they choose the wrong path due to a strong belief that a steam break must be the problem, E-2 will send them to E-1, loss of reactor or secondary coolant, with only a slight delay, after isolating the SGs. The loss of secondary heat sink could become a problem later, but not at this time.

In E-1, all should go smoothly initially. At Step 14, just before securing the RHR pumps (as in the base case SLOCA), the operators are cautioned that "If RCS pressure decreases in uncontrolled manner below 150 psig, RHR pumps must be manually restarted to makeup the RCS." This is an important warning for the "Growing" SLOCA scenario, but we note that there is no other caution or check for this condition other than the CSF status tree for core cooling, which looks at the core exit thermocouple readings at irregular intervals. The caution is not on the E-1 foldout sheet, which would be available as a ready reminder. When the LOCA grows sometime later, the crew will be involved in wrapping up the stable and supposedly well understood SLOCA. For now, the crew continues with E-1 until Step 18 where, because RCS pressure is above 150 psig, they should transition to procedure ES-1.2, post LOCA cooldown and depressurization. This is the same path followed by the base case SLOCA.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes, while not a major effect, could add to confusion. The next real trap for the "Growing" SLOCA case comes in Step 3.e where, in the first cycle through Steps 3-26, the operators are again asked to stop RHR pumps, which will leave the plant with insufficient injection when the LLOCA begins. Note that this is not an error. If the pumps are not stopped, they will be damaged due to lack of flow. It is, however, an act that leaves the plant vulnerable. Failure to closely monitor pressure, while in a vulnerable state (i.e., until fully depressurized) would be a significant unsafe act.

After Step 6, they may not have recovered subcooling, so the EOP path may move on to Step 7, rather than Step 16, as shown. Next, a warning is provided at depressurization Steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing Pzr level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. (The wiggles in subcooling margin and pressurizer pressure at 120 minutes in Figure E.14 are indicative of cyclic depressurization aimed at preventing voiding.) Nevertheless, if the context becomes sufficiently challenging, old rules can be enabled, such as the "Don't go solid" informal rule. Finally, the SI pump stop criteria in Step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure, and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading due to an incorrect action. Transfer to sump recirculation could be delayed because of belief that transfer to RHR cooling will occur soon. (Furthermore, if the LLOCA occurs during Step 11.d, the careful focus on the step-by-step rules in the EOP, especially as conditions are changing, could involve a type of "tunnel vision," delaying recognition that a LLOCA was in progress.)

The goal of ES-1.2 is to place the RCS on long-term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the Emergency Director does not choose to place RHR in service in Step 24.c (e.g., because of concerns about the unknown rupture point, residual steam in the RCS binding RHR flow, or other conditions) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

Once the LLOCA is established and, if the operators spot it in time to start the RHR pumps and save the core, it is fair to question how they would use the EOPs. They could jump back to E-0 or E-1. The case is formally included in the EOPs as cautions in E-1, Step 14, and ES-1.2, Step 3. Thus the operators could return to one of those points or carry out the action to start the RHR pumps and continue cycling through ES-1.2, Steps 3-26. The first would naturally take them to sump recirculation cooling in Step 19, if they reach that step in time. The second would simply cycle unsuccessfully hoping to refill the Pzr, when this procedure is inappropriate because the >150 psig criterion has not been met. The E-1 foldout, still in effect formally, would transfer to ES-1.3 sump recirculation.

From this discussion, it appears that, while the EOP can work for the "Growing" SLOCA deviation case, there may be some rough spots for the crew. Along the way, several actions listed as HFEs in ATHEANA Step 4 could be enabled by this deviation scenario:

- Operator removes early makeup from armed/standby status. (Note that this action to disable the RHR pumps is required by the EOP to protect the pumps and is not, therefore, an HFE. It does, however, defeat automatic response of the pumps if they are subsequently needed.)

- Operator fails to properly align containment sump recirculation cooling. (This HFE would be enabled simply by the cyclic structure of ES-1.2 and would be reinforced by the "Growing" SLOCA, because of the differences in timing introduced by a LLOCA occurring after the RWST is partially depleted by the preceding SLOCA.)

- Operator fails to manually start RHR pumps, when required. (This is a new HFE, not identified for the base case SLOCA in ATHEANA Step 4, and is introduced due to the "Growing" SLOCA deviation scenario.)

Returning to the vulnerabilities summarized in Table E.4, we observe that

- Training and experience do not directly apply; they apply to either the LLOCA or SLOCA base case, but the "Growing" deviation introduces problems in recognition, timing, and EOP ordering.

- The operator tendency to reduce injection for overcooling is very unlikely to have any impact.

- The history of Channel A Pzr pressure problems would be unimportant without failure or erroneous indication on Channel B.

- The informal rule to protect pumps from damage would reinforce the procedural stopping of RHR pumps and tend to place the focus on protecting the pumps rather than being alert to their future need.

At this point, the possible physical deviation is well defined and appears to be important enough to proceed to the next part of the analysis. It is time to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

The "Growing" SLOCA deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that this case involves at least seven different, potentially troublesome characteristics. This is not surprising; we are involved in a significant deviation from expected plant conditions outside the training and expectations of the crew. This is just the kind of situation implicated in serious accidents in which the operators are "set up" for failure. The identified scenario/parameter characteristics include

- Large (initial) change in parameter; under the deviation scenario, this characteristic can affect situation assessment and response planning. In itself, this factor may have minor impact. The change is well within the range observed in training scenarios.

- Low rate of change in parameter; can affect detection, situation assessment, and response planning.

- Changes in two or more parameters in a short time (following a period of stability); can affect detection and situation assessment.

- Garden path problem; can affect situation assessment.

- Situations that change; can affect situation assessment.

- Multiple lines of reasoning; can affect situation assessment.

These human complications spell difficulty for the operator and support the three HFEs listed above. Although the procedure can guide them through the situation successfully, there are significant factors that can defeat its success.

"More" SLOCA Deviation Case (Physical parameter behavior). The other class of "More"

SLOCA scenarios that deviate from the base case involves physical parameters of the plant that behave as if the LOCA were larger. Applying the guide word "More" to the plant parameters power, pressure, pressurizer level, containment pressure, accumulator dump, core reflood rate and timing, and clad temperature failed to yield meaningful or new scenarios, not uncovered earlier. The results for other parameters are

- Break flow. For certain SLOCA locations (e.g., near the discharge of the RCPs), a higher flow rate for the same size SLOCA could occur. Because operators have no direct indication of break size or location, such differences should have no special impact on operator performance.

- ECCS flow. Break location can impact ECCS pump flow. If the break is such that all or part of the pump flow can bypass the core, flow would be higher. This possibility is built into the success criteria. For other cases, the success criteria may be conservative. It is not observable to the operators and does not directly affect performance.

"Reversed" SLOCA Deviation Case. The next guide word is "Reversed." The notion appears to be meaningless for the SLOCA.

"As Well As" SLOCA Deviation Case. Finally, we consider "As well as," which also includes "Repeated" and "Inadvertent." No new deviation cases were uncovered when we applied these guide words to SLOCA.

Summary of Deviation Cases. Results of the preceding guide word deviation analysis are summarized in Table E.5, where, for each guide word, we summarize the identified possible physical deviations and their significance. We also indicate which of these deviation cases are considered further. The summary analysis is continued in Table E.6, where the scenario/parameter characteristics of the deviation cases from Tables 9.15 and 9.16 are presented. The analysis of these characteristics is extended in the table by identifying the associated error types and error mechanisms from Tables 9.15 and 9.16 that apply to each deviation case.

Consider the "No" SLOCA Deviation Case (Reduced ECCS Flow). If there is a major HP injection flow reduction due to obstructions, degraded pump head, or HPI pump failure, the procedural path to success has a built-in delay that restricts time available for recovery. Nevertheless, it would appear that significant additional EFC is required to delay correct operator response to the point that core damage is likely.

Next consider the "No" SLOCA Deviation Case (Pressurizer Steam Space SLOCA). The EOPs are designed to quickly stop such LOCAs. However, four cases were identified that could prevent isolation of the steam space SLOCA: LOCA not via the PORVs (via SV or pipe/vessel break); PORV stuck open, but indicates closed; PORV stuck open and block valve fails to close; and operator lapse (skip step requiring closure or isolation). The most challenging of these would be cases where the PORV indicates that it is closed, creating the impression that the LOCA is not a

Table E.5 Application of Guide Words to SLOCA Deviation Analysis

Guide Word	Possible Physical Deviation	Significance	Carry Forward? (Explained in Text)
No/Not/ Less/ Late/Never/ Too Slow/Too Long / Part of	Spurious SI	Minor. No history of spurious SI. Shutoff head of SI pumps is less than normal operating pressure, so no pressure excursion.	No
	Break size less than DBA	Unlikely to become challenging, without substantial additional context.	Not evaluated further, at this time
	Power fails to drop (fails to shutdown)	Only possible if pre-existing error violated fuel load/control requirements. Assumed very low probability.	Not evaluated further, at this time
	Reduced ECCS Flow	Reduced flow due to obstruction or impaired pump performance is either too great for success (and is therefore included in ECCS system analysis of the PRA) or impacts timing and RCS radioactivity. The latter does not appear to have significant impact on human performance. Insufficient HP injection requires rapid depressurization, outside the normal flow of the EOPs	Yes, focus on insufficient HP injection
	Pressurizer steam space SLOCA	The LOCA is ended early in E-0, provided it is via the PORV, the valve positioin indication works properly, and the valves respond to closing signals. With failed valve position indication and a stuck open PORV, or if the SLOCA is not via a PORV, incorrect situation assessment is likely.	Yes, but equipment failures required
More/ Early/ Too Quick/ Too Short	Break size greater than SLOCA DBA: Equivalent to "No" LLOCA Deviation (<DBA) Case of Appendix C	Can change timing, no longer have "right" conditions at EOP decision points. If the vulnerabilities identified in the text enable associated error mechanisms, operators could interrupt early makeup or fail to properly align sump recirculation cooling or RHR.	Yes See Appendix C for detailed analysis of this case
	Growing SLOCA: appears to stabilize as an SLOCA, later expands to near DBA LLOCA size: Similar to "Switching" LLOCA of Appendix C	SLOCA leads to disabling LPI and automatic SI actuation, operators fall into a regime where they "know" what is going on. Potentially significant impact on operations.	Yes
Reversed	None	No physical sense other than inadvertent SI, which is another identified initiating event.	No, N/A
As well as/ Repeated/ Inadvertent	No new scenarios identified	N/A	No, N/A

Table E.6 Results of SLOCA Deviation Analysis

Possible Physical Deviation	Characteristics Potentially Affecting Human Response	Potential Error Types and Mechanisms	Further Analysis and Possible Similar Scenarios
"No" SLOCA Deviation Case: Reduced ECCS Flow	Large change in parameter Situations that change (SLOCA becomes SLOCA w/o HPI) Impasse/tradeoff/double bind (cannot get to recovery action, without waiting or prematurely jumping procedures)	A number of error types and mechanisms relevant to one HFE of Step 4 (operator fails to depressurize RCS) and a new HFE (operator fails to provide continued cooling during LPI) are associated with the characteristics Error types include applying a less appropriate procedure step, missing a decision point, and failure to take needed action The underlying error mechanisms include fixation/tunnel vision, satisfying, reluctance, expectation bias, and lack of deep technical knowledge with respect to LPI cooling	Yes; additional context will be needed to have a high chance of an HFE occurring Examine the importance of continued secondary cooling following depressurization. LPI via SLOCA may not carry away sufficient heat to maintain low pressure.
"No" SLOCA Deviation Case: Pressurizer steam space SLOCA	Missing information (break location and void formation) Misleading information Multiple lines of reasoning Double bind Large change in parameter Relative rate of change in two or more parameters is not what would have been expected Higher than expected level	A number of error types and mechanisms relevant to the HFEs (operator interrupts early makeup, operator fails to depressurize RCS, and operator fails to properly align recirculation cooling or RHR) are associated with the characteristics Error types include taking inappropriate action and competing responses The underlying error mechanisms include displayed parameter matches incorrect mental template, expectation bias (primacy), over-eagerness, anxiety and tunnel vision	Yes
"More" SLOCA Deviation Case: Break size greater than SLOCA DBA [Note: the detailed writeup on this case is in Appendix C, where it was labeled "No" LLOCA Deviation Case (< DBA)]	Large change in parameter Low rate of change in parameter Relative rate of change in two or more parameters is not what would have been expected Changes in two or more parameters in a short time Direction of change in parameters over time is not what would be expected	A number of error types and mechanisms relevant to the HFEs (interrupt early makeup and fail to align recirc) are associated with the characteristics Error types include lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to taking inappropriate action, taking correct action too soon, and failure to take needed action The underlying error mechanisms include over-eagerness, simplifying, preoccupation, tunnel vision, and fixation	Yes, but it almost surely requires additional context (e.g., instrumentation problems or significant extraneous demands on attention) to become significant.

Table E.6 Results of SLOCA Deviation Analysis (Cont.)

Possible Physical Deviation	Characteristics Potentially Affecting Human Response	Potential Error Types and Mechanisms	Further Analysis and Possible Similar Scenarios
"More" SLOCA Deviation Case: "Growing" SLOCA: Starts as an SLOCA, later transitions to LLOCA	Large change in parameter Low rate of change in parameter, early on Changes in two or more parameters in a short time (following a period of stability) Garden path problem Situations that change Multiple lines of reasoning	A very large number of error types and mechanisms relevant to one HFE of Step 4 (fail to align recirc) and a new HFE (fail to manually initiate LPI) are associated with the characteristics Error types include lack of awareness of change, generation of false theories to explain seeming anomalies, delay in response while searching for an explanation, lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to missing a decision point, taking inappropriate action, and failure to take needed action The underlying error mechanisms include incredulity, over-eagerness, simplifying, preoccupation, tunnel vision, fixation, lack of deep technical knowledge, and multiple lines of reasoning are creating conflicting choices	Yes, continue. Similar scenario: LLOCA "Switching" Deviation case of Appendix C

steam space SLOCA. Despite the strong significance of this physical deviation, emphasis on meeting SI termination criteria is also strong. Some additional context is necessary for a substantial chance of the relevant HFEs.

Also consider the "More" SLOCA deviation case (> DBA). Despite the large number of error types and error mechanisms that could enable the two HFEs,

- Operator interrupts early makeup
- Operator fails to properly align containment sump recirculation cooling or RHR,

there is substantial time for the operators to respond to the many directions in the EOPs that would restore the scenario to a success path. It appears that the "No" SLOCA deviation case (> DBA) surely requires additional EFC beyond the physical deviations (e.g., instrumentation problems, hardware failures, or significant extraneous demands on attention) to become significant. Informal rules described in the text would then become important and could lead to either HFE.

Finally consider the "Growing" SLOCA deviation case. This scenario has many nearly overwhelming error mechanisms at work. On top of that, although one can track a success path through the EOPs, there are many opportunities missing and, at least for a short time, necessary pieces of information. All this is combined with unfavorable timing (very short time frame for restarting RHR pumps; a distorted picture of the time until switchover to recirculation, and, possibly, for switchover due to the long time under SLOCA conditions). In addition, there is the belief that the DBA SLOCA is the most severe SLOCA case and the disbelief that a LLOCA can actually occur. All together, this is a very strong EFC for the HFEs under consideration.

E.6.2 Search of Relevant Rules

The EOPs applying to the base case SLOCA were examined in Section 5 and yielded no strong context that would be expected to lead to error without further EFC. Four potentially challenging deviation scenarios, developed from applying the guide words to the base case SLOCA, led to a thorough review of the EOPs applied to these scenarios, under the search of Section E.6.1. In two of those cases, it was clear that additional elements of error-forcing context could change relatively benign scenarios into much more serious situations. That is the purpose of this and the following two searches is to identify additional factors that could make these scenarios more difficult for operators.

We have already walked through the EOP map of Figure E.12, identifying possible ambiguities and significance, in Steps 5 and 6.1. At this point, we can summarize those findings, in light of the identified HFEs. Generally,

- ECCS equipment is to be maintained in an armed/standby status.

- Early makeup, HPI for SLOCAs, is to be maintained until the SI termination criteria are met, at which point SI is stepped back in stages to ensure that the criteria continue to be met.

- PORVs are to be closed or isolated if an SI has occurred.
- RCS is to be depressurized if HH injection fails.
- Long-term makeup and cooling are to be maintained.

In specific cases, these functions can be terminated or unintentionally defeated:

- If indicated RWST level is less than 37%, the operators are to transfer to containment sump recirculation; doing this when actual level is higher (i.e., when level in the sump is low) could lead to vortexing and air binding the RHR system, blocking flow to the reactor.
- If pressurizer PORVs are faulty, operators are to close the block valves.
- If the SI termination criteria (subcooling >30°F and RCS pressure >2100 psig and pressurizer level >5% and secondary cooling) are met, operators are to trip SI pumps and RHR pumps.
- If RCS pressure is not falling and RHR pumps have no flow, operators are to stop RHR pumps.
- If there is no indication of high radiation in auxiliary building, the operators are not directed to search for a LOCA outside containment.
- If complex criteria are met, including pressurizer level and specific subcooling criteria depending on the number of charging pumps and RCPs running, stop SI pump(s).

Besides the above "formal" rules the informal rule/plant practice vulnerabilities identified on our Step 5 blackboard include

- Protect equipment. Operators are acutely sensitive to looking for signs of equipment degradation and rapidly shutting down affected equipment. Apparent equipment problems could lead operators to shut down needed equipment.
- Operators tend to discount Channel A pressure instruments because of the history of Channel A pressurizer pressure problems. This becomes important, in case of failure or erroneous indication on Channel B. Note that the lack of deep technical knowledge of I&C plays a role in how such a history of problems is interpreted and applied.
- The tendency to decrease injection with rising pressurizer level could come into play.

Based on the above summary, in order for any of the HFEs of concern to occur when following the formal or informal rules, one or a combination of the following must occur:

- RWST level is indicating less than 37% when really higher or the operators perceive it so
- Pressurizer PORVs indicating or appearing open, when really closed
- SI termination criteria appear to be met, when really not
- RHR pumps appear to be required (pressure appears to be falling or RHR pumps appear to be providing flow), when really not
- No observed high radiation in auxiliary building, with LOCA outside containment
- Erroneous or misinterpreted subcooling, when actually low
- Equipment trouble, real or perceived.

Each of these conditions is examined in Table E.7 against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science.

Based on the scenario analysis above and information in the tables, we find that the operators could be set up to carry out several of the HFEs: interrupt early makeup, fail to depressurize, fail to properly align recirculation cooling, and prematurely secure long-term makeup/cooling. Thus several of the examined contextual elements may be significant in the final scenario development. Note too that some of them require additional hardware failures and PSFs.

E.6.3 Search for Support System Dependencies

There are no valves that interface with the RCS that can be physically opened under normal RCS pressure and operating conditions, other than PORVs and safety valves (discussed elsewhere), letdown, and small sample valves. RCP seals can fail due to loss of both seal injection and component cooling. Seal LOCAs from all sources (except widespread failure of component cooling) are included in the SLOCA frequency. Widespread loss of component cooling has many significant ramifications for equipment and operators. However, it is considered as a separate initiator and is not included in the analysis of SLOCA events. It is identified here and could be the subject of a similar investigation. Likewise, loss of electric power would be considered separately.

One particular support system dependency that could be significant for our examination is that one instrument ac power bus can fail both the RWST low level alarm (not widely known among operators) and Channel B wide range pressurizer level. While the narrow range Channel A pressure instrument is the one with a history of recent problems, it is not always easy for operators to recall that the wide range pressure instrument is a separate instrument, down to the sensors. So failure or maintenance on this instrument ac bus sets up the operators on a number of counts: Channel B

Table E.7 Results of the EOP/Informal Rule Deviation Analysis

Condition	Example Causes of the Condltion	Characteristlcs Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
RWST level is indicating less than 37% when really higher or thc opcrators perccive them so	Multiple level indicators in error	Missing/misleading information	Taking correct action too soon could air bind the system	Consider in final deviation scenario description (E.6.5).
	Operators mis-read indicators or anticipate lcvels before they are reached, especially if distracted	Attentional load/workload dividing crew attention, in light of expectation bias	Taking correct action too soon could air bind the systcm	No. Coordinated action by multiple crew members.
Pressurizer PORVs faulty or appear so, whcn really closed	Multiple PORV position indicators fail or one fails and opposite block valve fails closed.	Misleading information Attentional load/workload dividing crew attention	None immcdiately, but later, if operator conducting depressurization does not know PORVs blocked, there could be significant delay in depressurization Take inappropriate (incompletc) action	Consider in final deviation scenario description (E.6.5), but only if common cause failure could disable both PORV indicator and block valve or indicator.
	Previous lift of PORVs heats tailpipe or raises pressure in PRT	Misleading information causing operator to believe that PORV is open	None immediately, but later, if opcrator conducting depressurization does not know PORVs blocked, there could be significant delay in depressurization Take inappropriate (incomplete) action	Consider in final dcviation scenario description (E.6.5).
Sl tcrmination criteria appear to be met, when not really met	Erroneous wide range pressure (reading high) would indicate high pressure, high subcooling, and erroneous RVLIS	Misleading information Garden path scenario	Take inappropriate action, i.e., operators would secure all HH injection	Considcr in final deviation scenario dcscription (E.6.5)..
RHR pumps appear to be required, when really not	Erroneous wide range pressure (rcading high)	Missing/misleading information	Fail to take a needed action, i.e., operators do not stop RHR pumps, leading to overheating, failure, and unavailability, if required later	Considcr in final deviation scenario description (E.6.5).

Table E.7 Results of the EOP/Informal Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
	Erroneous RHR pump flow or pump current indication	Attentional load/workload dividing crew attention, in light of expectation bias	Fail to take a needed action, i.e., operators do not stop RHR pumps, leading to overheating, failure, and unavailability, if required later	Consider in final deviation scenario description (E.6.5).
	Operator misreads or misinterprets RHR pump flow or pump current indication	Attentional load/workload dividing crew attention, in light of expectation bias	Fail to take a needed action, i.e., operators do not stop RHR pumps, leading to overheating, failure, and unavailability, if required later	Consider in final deviation scenario description (E.6.5).
No observed high radiation in auxiliary building; LOCA outside containment	Failed radiation monitors	Missing information	Fail to take required action; failure to detect LOCA outside containment leads to running out of water	No. Too many redundant radiation monitors and confirmatory information (sump level), with no wide-spread common cause identified.
	Operator fails to notice alarming radiation monitors in aux bldg, with all other information	Attentional load/workload dividing crew attention, in light of expectation bias	Fail to take required action; failure to detect LOCA outside containment leads to running out of water	No. Specific requirement in EOP to check rad monitors, redundant and diverse checks. Outside scope of issue.
Erroneous or misinterpreted subcooling (similar to SI termination requirement above)	Erroneous wide range pressure (reading high) would indicate high pressure, high subcooling, and erroneous RVLIS	Misleading information Garden path scenario	Take inappropriate action, i.e., operators would secure all HH injection	Consider in final deviation scenario description (E.6.5).
	Erroneous subcooling indication	Misleading information Garden path scenario	Take inappropriate action, i.e., operators would secure HH injection pumps	Consider in final deviation scenario description (E.6.5).

Table E.7 Results of the EOP/Informal Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
	Rapid progression through EOP ES-1.2, Step 11, not waiting for stabilization	Situations that change, tunnel vision Missing information, over-eagerness	Take inappropriate action, i.e., operators would secure all HH injection pumps	Consider in final deviation scenario description (E.6.5).
Equipment trouble induces shutdown by operator	Actual impending failure or damage	Must deal with situation that changes	Possible double bind between maintaining cooling and shutting down equipment	Consider in final deviation scenario description (E.6.5).
	Erroneous indication or misperception	Misleading information Over-eagerness, anxiety	Possible double bind between maintaining cooling and shutting down equipment	Consider in final deviation scenario description (E.6.5).

pressure is out of service, after the SLOCA drops pressure below the normal range; operators only have Channel A, which they do not trust; and they will receive no alarm on low RWST level, which is the normal cue to switch to recirculation cooling.

A related issue is dependency among operator actions. It is possible that, if operators identify the need for restarting RHR pumps in time, there could be some dependency between that action and the eventual action to switchover to recirculation cooling. One was identified in the discussion of the "Growing" SLOCA scenario in Section E.6.1. Depending on which procedural anchor the operators use to start the RHR pumps, they can restart E-0, jump to E-1 Step 14, jump to ES-1.2 Step 3, or simply start the pumps and continue their cycle through ES-1.2. The likelihood of being ready for recirculation, when needed, may depend on this decision.

The results of this search are summarized in Table E.8.

E.6.4 Search for Operator Tendencies and Error Types

This search could develop other potentially significant EFCs that could become contributors to core damage frequency. However, it will not be performed, because this search is a "catch-all" for deviation characteristics that might have been missed in the earlier searches, as indicated in the process description of Section 9.6.6. It is similar to the open-ended search of earlier versions of ATHEANA, albeit a more structured approach. If significant EFC/UA combinations have been identified by the earlier searches, they are more likely to be important, because they focus on elements known to be represented in serious accidents.

E.6.5 Develop Descriptions of Deviation Scenarios

Of the four deviation scenarios selected for further analysis in Table E.6, all either had sufficiently strong context that no further complicating factors were felt necessary or those complicating factors were identified in the searches of Sections E.6.2 and E.6.3:

- "No" SLOCA Deviation Case: Reduced ECCS flow requires the failure of HH injection and problems in depressurization.

- "No" SLOCA Deviation Case: Pressurizer steam space SLOCA is complete as described and has not been extended by searches in E.6.2, E.6.3, or E.6.5, because the context was deemed strong enough without further requirements that diminish the frequency of the event. Likewise, while additional complicating factors would make the context even more cognitively demanding, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be added at this time.

- "More" SLOCA Deviation Case: Break size greater than DBA SLOCA requires instrument problems to obscure the failure to reach SI termination criteria.

Table E.8 Results of System Dependency Deviation Analysis

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
AC instrument bus failed or out of service causing RWST low level alarm and Ch B wide range pressure to be inoperable	Hardware failure and subsequent repair activity	Garden path problem, simplifying, familiarity from drills, tunnel vision Masking, general pattern seems normal enough that operators do not detect or understand important changes (or lack of change) in some parameters Misleading information	Take inappropriate action, i.e., operators would secure HH injection pumps	Consider in final deviation scenario description (E.6.5).

"More" SLOCA Deviation Case: "Growing" SLOCA is complete and has not been extended by searches in E.6.2, E.6.3, or E.6.5, because the context was deemed strong enough without further requirements that diminish the frequency of the event. Likewise, while additional complicating factors would make the context even more cognitively demanding, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be added at this time.

It is appropriate, at this point, to summarize the key elements of these scenarios to identify those vulnerabilities, error types, and potential error mechanisms that we believe are most significant, and identify the associated PSFs. This information is presented in Table E.9.

E.7 Step 7: Identify and Evaluate Complicating Factors and Links to PSFs.

This step is addressed in Section E.6.5 above.

E.8 Step 8: Evaluate the Potential for Recovery

Recovery scenarios are different for each deviation case.

- "No" SLOCA Deviation Case: Reduced ECCS flow requires the failure of HH injection and problems in depressurization. In keeping with the issue for this analysis, we ignore the possibility that the operators anticipate high core exit temperatures and jump to function restoration guideline FR-C.1 before directed by the EOPs. Because the operators are instructed not to attempt depressurization until core exit temperatures are very high (1200°F), which should not occur until the core is substantially uncovered, there is little time for recovery if depressurization is delayed. Therefore, recovery is not considered for this case.

- "No" SLOCA Deviation Case: Pressurizer steam space SLOCA. There are few cues other than those monitored in the CSF status trees (i.e., no alarms or set points for equipment actuation). Therefore, when the CSF status trees call for action, there will be little time available and, given the entire context up to this point, the operators will face a serious dilemma; they will have all the previous indications that they are on the right track. The main hope for recovery in this case is that the technical support center engineers, in reviewing the time history of the event, will realize that steam voiding in the RCS is quite likely and direct that operators restore HH injection and proceed with depressurization and cooldown.

- "More" SLOCA Deviation Case: Break size greater than DBA SLOCA. Even if operators eventually stop HP injection, by this time the RCS has cooled significantly and would take substantial time to heat up, steam off, and begin to cause significant core damage. In addition, the technical support center would be reviewing the accident and could bring dispassionate judgment to bear on the problem. It is very unlikely that they too would not

Table E.9 Deviation Scenarios

Overall Plant Condition (Scenario)	Key Information Related to HFEs, Error Types, and Error Mechanisms	Most Relevant PSFs
"No" SLOCA Deviation Case: Reduced ECCS Flow High pressure injection fails due to pump failure. Eventually, when core exit thermocouples reach 1200F, CSF status tree sends operators to function restoration guideline that directs depressurization and LP injection	HFE of interest (fail to depressurize RCS, when required) Hardware failures: HH injection pumps Late changes in the plan–anxiety, stress, delays Despite EOPs leading to attempted depressurization coming after core is starved and has high temperature, there should be sufficient time, unless activity in delayed due to other factors Additional hardware failures. PORV and block valve position indication failed or combinations of PORV/indicator failure with failed closed block valves.	Procedure. Main EOP (E-0) not built for response to equipment failures beyond design basis, core is in extremis before alternatives to HPI are attempted Procedure/policy/practice. Inadequate crew communications allow other members of team to be unaware of action to isolate PORVs
"No" SLOCA Deviation Case: Pressurizer steam space SLOCA LOCA is via PORV with failed position indicator or via SV or pipe/vessel rupture, masking usual indication of steam space LOCA	HFEs of interest (interrupt early makeup), (fail to depressurize RCS), and (failure to properly align recirculation or RHR) Displayed parameter matches incorrect mental template [likewise, does not match incomplete mental template for steam space (PORV) SLOCA] Expectation bias Over-eagerness and tunnel vision Relative rate of change Double bind. Maintain injection and maintain pressurizer level Other distractions (likely that some additional instruments/equipment is failed)	Training/practice. Trained to believe instruments Training/practice. Belief that TMI accident is "fixed" (steam space LOCA will be via PORV and indicator cannot fail as at TMI) Training. Lack of training for off-expected accident conditions

Table E.9 Deviation Scenarios (Cont.)

Overall Plant Condition (Scenario)	Key Information Related to HFEs, Error Types, and Error Mechanisms	Most Relevant PSFs
"More" SLOCA Deviation Case: Break size greater than SLOCA DBA The SLOCA is larger, with commensurate higher blowdown flow than the 3 inch DBA SLOCA. Differences in timing can lead to unfamiliar accident progression. A failed instrument ac bus causes RWST low level alarm and Ch B wide range pressure to be inoperable	Two HFEs of interest (interrupt early makeup) and (fail to properly align recirc) The event itself does not follow the standard DBA SLOCA event of training drills As accident progresses Channel A pressure instrument hangs at some pressure, about 600 psig also causing subcooling to indicate high and RVLIS to read high The operators observe indications that would imply SI termination criteria are about to be met; while there are inconsistences (hanging pressure, hanging subcooling), these occur early on and may not be noticed, but EOPs have not yet focused attention on them. Other inconsistencies occur later; e.g., lack of pressure transient as RCPs are started. Over-eagerness, simplifying, and preoccupation allow operators to miss anomalies or fail to respond to a serious situation in time	Training/practice. Lack of training or practice for off-normal, unexpected accident conditions and problem solving Training/practice. Base case LLOCA and SLOCA used repeatedly in training HMI. Lack of trending displays allows odd parameter tracks to be put aside HMI. Lack of redundance leads to alarm failure
"More" SLOCA Deviation Case: "Growing" SLOCA Event starts as DBA SLOCA. Later, after the operators have stabilized the SLOCA and are preparing for long term cooling, the LOCA expands to near DBA LLOCA conditions.	Two HFEs of interest (fail to align recirc) and (fail to manually initiate LPI) Unexpected initial events can lead to false theories to explain seeming anomalies caused by incredulity; this allows the initial information to create early confusion and to become lost later, when it would be helpful As operators settle into the SLOCA track, they become vulnerable to the garden path problem and are susceptible to tunnel vision and fixation, simplifying the scenario by ignoring the initial LLOCA-like trends When RHR pumps are secured, the procedure warns that manual restart would be required. Nevertheless, experience and training reinforce the garden path scenario As they begin to focus on moving out of SI and into RHR cooling, they can become preoccupied with the details of EOP ES-1.2 and developing an over-eagerness to reach the stable end point All these factors permit a lack of awareness of change and of attention to other parameters Now they are set up for failure to recognize a serious situation in time; i.e., they can miss a key decision point, failing to take needed action, when RCS pressure suddenly falls because of the reinitiated LLOCA Even if they should respond in time, restarting the RHR pumps, multiple lines of reasoning about where to branch in the EOPs creates conflicting choices, delaying their attention from preparing for recirculation cooling, which will be needed very soon	Training/practice. Lack of training or practice for off-normal, unexpected accident conditions and problem solving Training/practice. Base case LLOCA and SLOCA used repeatedly in training Procedures. Insufficient warning to be prepared for rapidly increasing LOCA Lack of trending displays allows odd initial parameter tracks to be put aside

focus on inconsistent pressure and subcooling traces. Thus recovery for this case seems almost guaranteed, albeit after some very serious events have transpired. No formal recovery analysis seems to be needed.

- "More" SLOCA Deviation Case: "Growing" SLOCA. Because of the short time available for restarting RHR pump, the short time later when switchover to recirculation must begin, and the short time available to complete the switchover, recovery is not considered separately. Definition of the HFEs will include the idea that failure means failure to accomplish the activity within the time before unrecoverable damage occurs.

E.9 Step 9: Quantification Considerations

The issue to be addressed in this analysis was: Can reasonable variations on the SLOCA scenario be identified, such that progress through the EOPs is significantly more difficult than for the SLOCA of the FSAR safety analysis? This question can generally be answered without formal quantification of the HFEs. However, the idea of "reasonable variations" must include some sense of likelihood and this may require formal quantification, depending on the particular case, as defined in Table E.9, shown earlier.

We consider each of the four deviation cases separately, in the following paragraphs:

- "No" SLOCA Deviation Case: Reduced ECCS flow
- "No" SLOCA Deviation Case: Pressurizer steam space SLOCA
- "More" SLOCA Deviation Case: Break size greater than DBA SLOCA
- "More" SLOCA Deviation Case: "Growing" SLOCA

E.9.1 "No" SLOCA Deviation Case: Reduced ECCS Flow

No quantification will be performed. The scenario is interesting in that the normally modeled response to failure of HH injection is more difficult than usually acknowledged. However, the only combinations of failures that we have postulated to cause delay in depressurization are very low in frequency and not especially likely to cause significant delay. The fact, noted in Step 1, that some instrument/equipment failures that may attract the operators' attention are sure to have happened, does not seem sufficient in itself. There is some time for the operators to deal with those events, before the trigger point for depressurization is reached. Other unconnected failures placing high demands on the operators are unlikely, so the frequency of such scenarios would be rather low.

While this may not be a "reasonable" contributor to core damage, the initial deviation, failure of HH injection, is a reasonable variation in the SLOCA scenario and is modeled in all PRAs. Therefore, it will be addressed in the issue resolution section below.

E.9.2 "No" SLOCA Deviation Case: Pressurizer Steam Space SLOCA

Although this case appears to be a challenging deviation, on its face, because of its similarity to the "fixed" TMI-2 scenario, its "reasonableness" and degree of significance is likely to be questioned. Therefore, a more complete quantification is prudent.

Frequency of Error-Forcing Context. The full deviation case outlined in Table E.9 involves either an SLOCA via a stuck open PORV with failed position indication (indicating closed) or an SLOCA via a stuck open SVs or pressurizer pipe/vessel rupture. From the PRA we estimate the frequencies of these cases as follows:

Freq = F(stuck open PORV and failed VPI) + F (stuck open SV) + F (rupture)

If the PORV disk separates from the stem and lodges where it does not block flow, then the valve will indicate closed but be passing fluid. This was not the failure mode envisioned when the TMI fixes were made. Although the failure mode is much less likely (about $1x10^{-6}$ to $1x10^{-7}$ per year) than a simple stuck open PORV ($1x10^{-3}$ per year), it is more likely than the coincident failure of the PORV and its indication system. The pipe/vessel rupture frequency for the entire RCS is $5x10^{-3}$ per year in the PRA data and if the pressurizer and surge line are one tenth of that, the frequency is $5x10^{-4}$ per year. Finally, the frequency of open safety valve initiators is $5x10^{-3}$ per year, but this is based on minor events of reactor trip associated with an open relief or safety valve (with some limited blowdown and closure before SI). A rough estimate of the chance of an SLOCA may be based on combining this frequency with a generic probability of sticking open an SV of $5x10^{-3}$ per demand or a total frequency of $3x10^{-5}$ per year. So the frequency of the scenario is on the order of $5.3x10^{-4}$ per year.

Probability of Unsafe Acts. We address the probability of the UAs including non-recovery in an integrated one-step process. Thus we evaluate

$P(UA_1)$ = P(operators interrupt early makeup),

$P(UA_2)$ = P(operators fail to depressurize RCS | do interrupt early makeup), and

$P(UA_3)$ = P(they fail to complete the sump recirculation cooling lineup before the RWST runs dry | they do not perform UA_1 or UA_2).

Taking into account the deviation scenario, including the associated EFC documented in Table E.9 and the time available for each action, the analysts have developed a consensus judgment of the likelihood of the crew performing these UAs. Their judgment is based on their experience, their observations of many crews in the plant and in simulators, and their understanding of the context of this event, including the status of procedures and training discussed earlier. Given the difficult context of the scenario, our estimates are

$P(UA_1) =$ 0.10; i.e., perhaps 1 in 10 crews would be set up sufficiently to carry out UA_1.

$P(UA_2) =$ nearly 0; i.e., if they interrupt early makeup, it is because they believe that the core is protected, so there is no need to carry out this act.

$P(UA_3) =$ 0.01; i.e., about 1 crew in 100 would be likely to miss the time window available for transfer to recirculation cooling, given the context.[7]

Our estimate for UA_1 is reasonably consistent with the generic estimates in HEART.

Frequency of the Event Leading to Core Damage. Combining the frequency of the EFC and the probability of the HFEs yields an estimate of core damage frequency of about $5x10^{-5}$ per year for the operators in the control room. When the technical support center team is factored into the analysis, our team believes that there is roughly 1 chance in 100 that they will miss the voiding and allow the operators to continue on their chosen path. Thus we believe that the core damage associated with this scenario is very low, perhaps on the order of $5x10^{-7}$ per year, when the technical support center is included.

E.9.3 "More" SLOCA Deviation Case: Break Size Greater then DBA SLOCA.

In this case, the scenario becomes very difficult, because of the misleading readings and lack of encouragement to question unfamiliar and confusing conditions. We think that this scenario meets the issue on its face and without complete quantification.[8] We note that previous detailed

---

[7]As a sanity check on these estimates, we examine the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10. First we must match our actions and EFC with those in HEART. The following are reasonable matches:

- Stopping the HH injection pumps is, in the words of HEART, a "routine, highly practiced, rapid task involving relatively low levels of skill" (0.007 - 0.045), but EFC is "unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel" (multiplier of up to 17 and we would judge it to be in about the upper third of the range). The associated probability is roughly 11 * 0.02 or 0.22, with uncertainty of 0.08 to no more than 0.5.
- Switchover to recirculation cooling is, in the words of HEART, almost a "complex task requiring a high level of comprehension or skill" (0.12 - 0.28). It is tempered by the fact that they did continue with SI despite the strength of the EFC. The associated probability from HEART is 0.16 and ranges from 0.12 to 0.28. This is substantially higher than our estimate.

[8]The interested reader will find that a very similar scenario was identified through a less direct process, in a trial of an earlier version of ATHEANA (NUREG-1624). That analysis proceeded by identifying potential HFEs; searching procedures and informal rules for rules that would direct the HFE, if used improperly; and then trying to add on plant and human context that would enable the HFE. There was no direct search for deviations or procedure mapping, so success depended on close familiarity with EOPs by operators on the analysis team and a rather free association of principles from behavioral science with plant conditions and the HFE, to complete the context. The scenario of the previous analysis included an initiating event that is nearly identical to the "No" LOCA deviation case; that analysis also identified significant failures in instruments. The conditional probability of the HFE and failure to recover was quite high (0.8 and 0.1). However, the plant-specific probability of the particular postulated instrument failure was very low, leading to a very small contribution to core damage frequency.

quantification of a similar case found a high probability of committing the UA.

E.9.4 "More" SLOCA Deviation Case: "Growing" SLOCA

Quantification of the "Growing" SLOCA deviation case is appropriate, because the resulting LLOCA is a DBA and may not be expected to present any difficulties. After all, the DBA is shown to avoid undue consequences in the FSAR and the EOPS have been well tested against this event. Quantification will focus first on the probability of the UAs, given the scenario.

Probability of Unsafe Acts. We address the probability of the UAs including non-recovery in an integrated one-step process. Thus we evaluate

$P(UA_1)$ = P(operators fail to restart RHR pumps | EFC), and

$P(UA_2)$ = P(they fail to complete the sump recirculation cooling lineup before the RWST runs dry | they restart RHR pumps $\wedge$ EFC).

Taking into account the deviation scenario, including the associated EFC documented in Table E.9 and the short time available for each action, the analysts have developed a consensus judgment of the likelihood of the crew performing these UAs. Their judgment is based on their experience, their observations of many crews in the plant and in simulators, and their understanding of the context of this event, including the status of procedures and training discussed earlier. Given the difficult context of the scenario our estimates are

$P(UA_1)$ = 0.30; i.e., they are only slightly more likely to restart the pumps than not.

$P(UA_2)$ = 0.07; i.e., about 1 in 15 crews would be trapped by the short time, multiple lines of reasoning, and deceptive timing, and fail to shift to recirculation in time.[9]

---

[9]As a sanity check on these estimates, we examine the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10. First we must match our actions and EFC with those in HEART. The following are reasonable matches:

- Restarting the RHR pumps is in the words of HEART, a "routine, highly practiced, rapid task involving relatively low levels of skill," but EFC is "unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel." The associated probability is no more than 17 * 0.02 or 0.34, with uncertainty of 0.12 to no more than 0.77.
- Switchover to recirculation cooling is in the words of HEART, almost a "complex task requiring a high level of comprehension or skill." It is tempered by the fact that they did restart the pumps and hardened by the strength of the EFC. If we assume that the positive impact of having restarted the pumps balances the difficult EFC, the associated probability from HEART is 0.16 and ranges from 0.12 to 0.28.

Our estimate for UA_1 is surprisingly consistent with the generic estimates in HEART. Our estimate for UA_2 is lower than HEART by about a factor of 2; i.e., reasonably close.

Frequency of Error-Forcing Context. To be consistent with the PRA, we note that their estimate of the frequency of LLOCA is $1x10^{-4}$ per year.[10] The frequency of SLOCA is much higher, but we have no good way to move from the SLOCA to the LLOCA. Starting with the LLOCA frequency, we ask, is it reasonable that a LLOCA would begin full bloomed? Or is it more likely that it would begin small, and grow larger after some time at lower blowdown rates? First, we observe that the few ruptures that have occurred in our direct experience began as very small leaks, and later expanded, although never to the size we are discussing. The forces due to vibration, rapidly changing temperature, or other causes seems to lead to progressive failure. We estimate that one in ten LLOCAs could begin quite small (SLOCA size or somewhat larger) and later expand significantly. So the frequency of the "Growing" SLOCA is 1×10^{-5} per year.

Frequency of the Event Leading to Core Damage. Combining the frequency of the EFC and the probability of the HFEs yields an estimate of core damage frequency due to the physical deviation of the "Growing" SLOCA scenario creating an EFC that sets up the operators for failure. To have failure, either the operators fail to restart RHR pumps or they successfully start the pumps and fail to complete the sump recirculation cooling lineup before the RWST runs dry; i.e.,

$$P(UA_1) + \{[1 - P(UA_1)] * P(UA_2)\} = 0.35.$$

Combining the frequency of the EFC with the probability that one of the UAs occurs yields a core damage frequency of 3.5×10^{-6} per year for the "Growing" SLOCA deviation case.

E.10 Issue Resolution

This ATHEANA example analysis was performed to address one specific issue:

> *Can reasonable variations on the SLOCA scenario be identified, such that progress through the EOPs is significantly more difficult than for the SLOCA of the FSAR safety analysis?*

The analysis defined several deviation scenarios in Table E.5 and expanded in Table E.9 that go beyond training and FSAR analysis and could lead to core damage. They all increase the difficulty of progressing through the EOPs compared to the SLOCA of the FSAR. However, they are not equally "reasonable." We consider each of the four deviation cases separately in the following paragraphs.

---

[10]Current thinking is that the frequency of the DBA LLOCA must be much less than estimates used in most PRAs, including ours. Addressing that issue is beyond the scope of the current analysis. We note, however, that a most likely estimate much lower is not inconsistent with a $1x10^{-4}$ per year average frequency, if the average comes from slightly higher than average frequency in very small number of pipes, with significant flaws present due to fabrication, construction, operational, or maintenance-related damage.

E.10.1 "No" SLOCA Deviation Case: Reduced ECCS Flow

The key issue in this case is that an expected response to a scenario modeled in all PRAs is less direct and more time constrained than is generally assumed in the existing analyses. The functional restoration guidelines are in general not as direct as the normal EOPs and are performed under greater time constraints and higher anxiety. Moreover, some of the actions are last ditch efforts; operators get only one chance to do them correctly. This is pointed out in EOP back up documents, but is not always a strong focus. Our sense is that HRA of all functional restoration (FR) procedures might identify cases where a more direct approach to responding to equipment failures would be helpful.

E.10.2 "No" SLOCA Deviation Case: Pressurizer Steam Space SLOCA

The key lesson from this deviation case is that, even when the EOPs "work," there are entry conditions (deviations) that, while related, are different enough to go unrecognized by the operators. Then the high level of training on the more likely, or more expected, scenarios can create a bias against following a helpful EOP, because the common, related conditions are not recognized.

In this particular case, a better understanding of phenomena associated with voiding would be helpful.

E.10.3 "More" SLOCA Deviation Case: Break Size Greater than DBA SLOCA

In this case, the scenario becomes very difficult, because of the misleading readings. From observations of drills on similar scenarios, the scenario difficulties would not be so easily addressed in EOPs as in plant operations practice. An approach that relies on collegial agreement among operators and encouragement to speak one's mind when the situation is not well understood would seem to offer the best hope for unraveling such a convoluted scenario. The EOP is something of a trap until the problems with pressure (somewhat easy to dismiss due to previous problems) and subcooling margin are understood. And they are unlikely to be seen until someone in the control room mentions to their colleagues that there are inconsistencies in the scenario.

We note that plots of trends in parameters could highlight the inconsistences and that the team in the technical support center are likely to do this, even if the control room operators do not. Nevertheless, it is not a convincing solution and it may be limited to specific cases. The collegial approach to operations provides a more robust solution.

E.10.4 "More" SLOCA Deviation Case: "Growing" SLOCA

The remaining case, the "Growing" SLOCA, involves many challenging aspects. The probability of an HFE, given the scenario, is quite high. In a generic sense, the frequency of this initiator is very low. Nevertheless, there are several reasons to consider the case seriously:

- It is more than frequency. In the spirit of medical diagnosis, it is not simply the probability of a possible diagnosis that is of interest. If some very high consequence *treatable* disease has a low probability of being correct, we hope our physician does not dismiss it because of its low probability, but investigates further (more research on the characteristics of the disease, more tests, etc.). We are more willing to play the odds, if the consequences are low. This is not to say that risk is not a suitable criterion for programmatic decision making, but that in diagnostics, it is worthwhile digging deeper and being better prepared for high consequence events.

- The frequency might not be correct. There may be failure modes not yet evidenced that can occur under specific conditions, including aging. Even if generically the chance of the "Growing" SLOCA may be very low, specific plants with specific designs, operating histories, maintenance histories, and vulnerabilities could have a much higher frequency for such events.

- Similar events. As identified in Table E.6, a LLOCA that plugs and later expands could have similar consequences. Other possibilities include a smaller, more likely LLOCA combined with

- One RHR pump out of service and a second that was allowed to run "too long" in the operators' view such that they believe it is damaged.

- Channel B pressure instrument out of service and the operators disbelieve channel A (as in the greater than DBA SLOCA case.

Thus the issue resolution process may demand that the analysis be extended or that, because of the broad range of possibilities, some precautions in training or practice be instituted to ensure, if an unlikely or unforeseen condition arises, the operators are well prepared to deal with it.

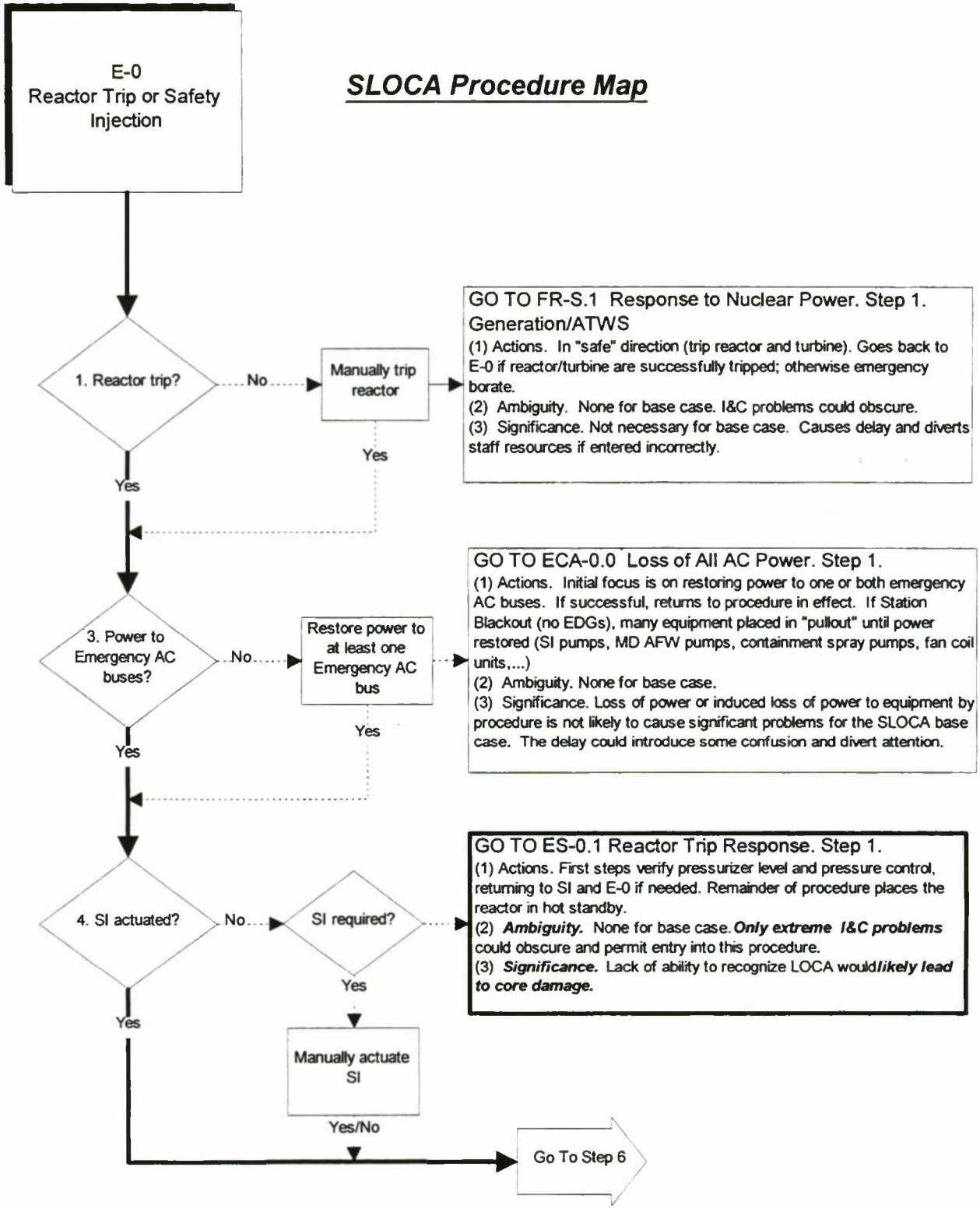


Figure E.12 EOP Map of Base Case SLOCA (Sheet 1)

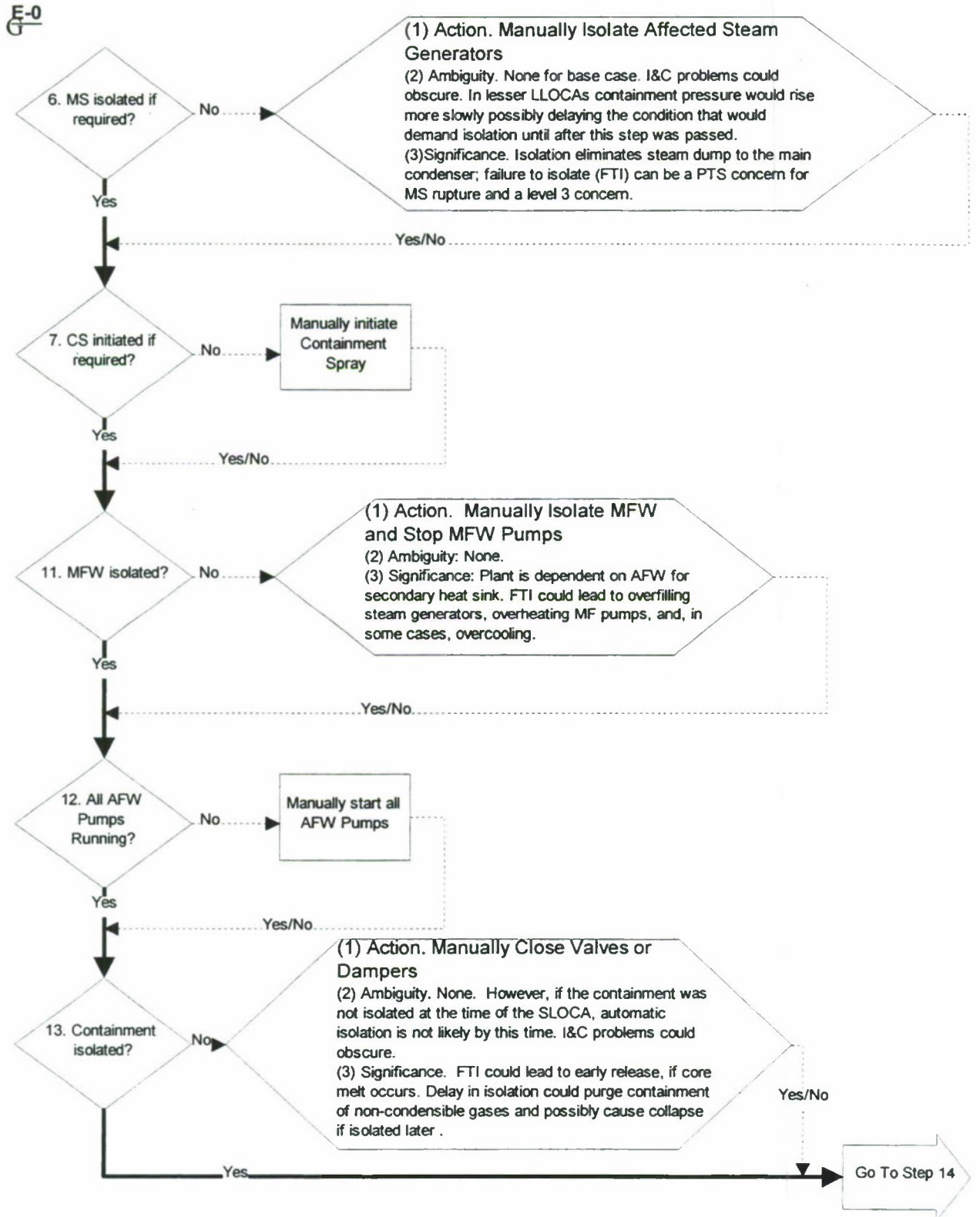


Figure E.12 EOP Map of Base Case SLOCA (Sheet 2)

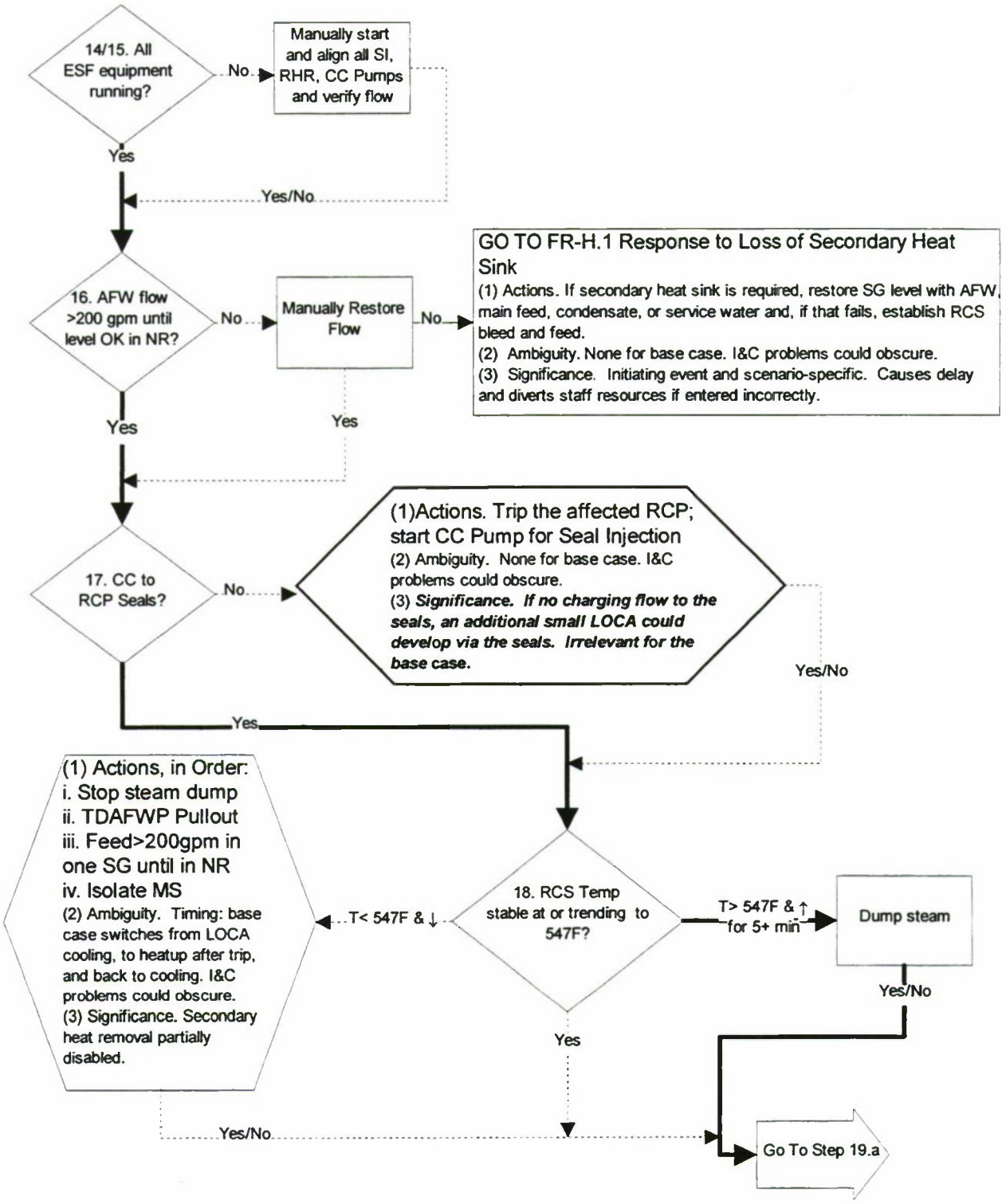


Figure E.12 EOP Map of Base Case SLOCA (Sheet 3)

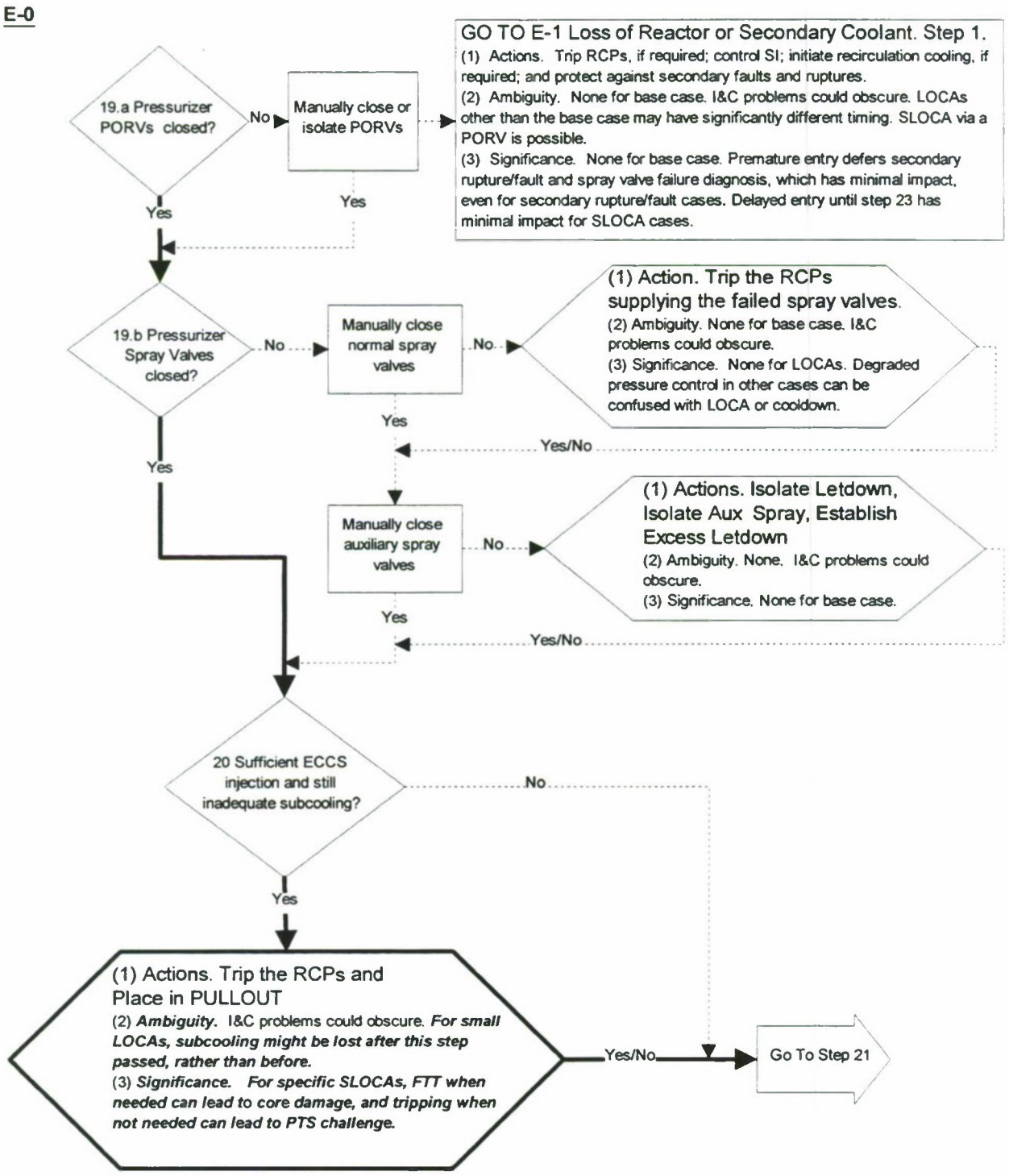


Figure E.12 EOP Map of Base Case SLOCA (Sheet 4)

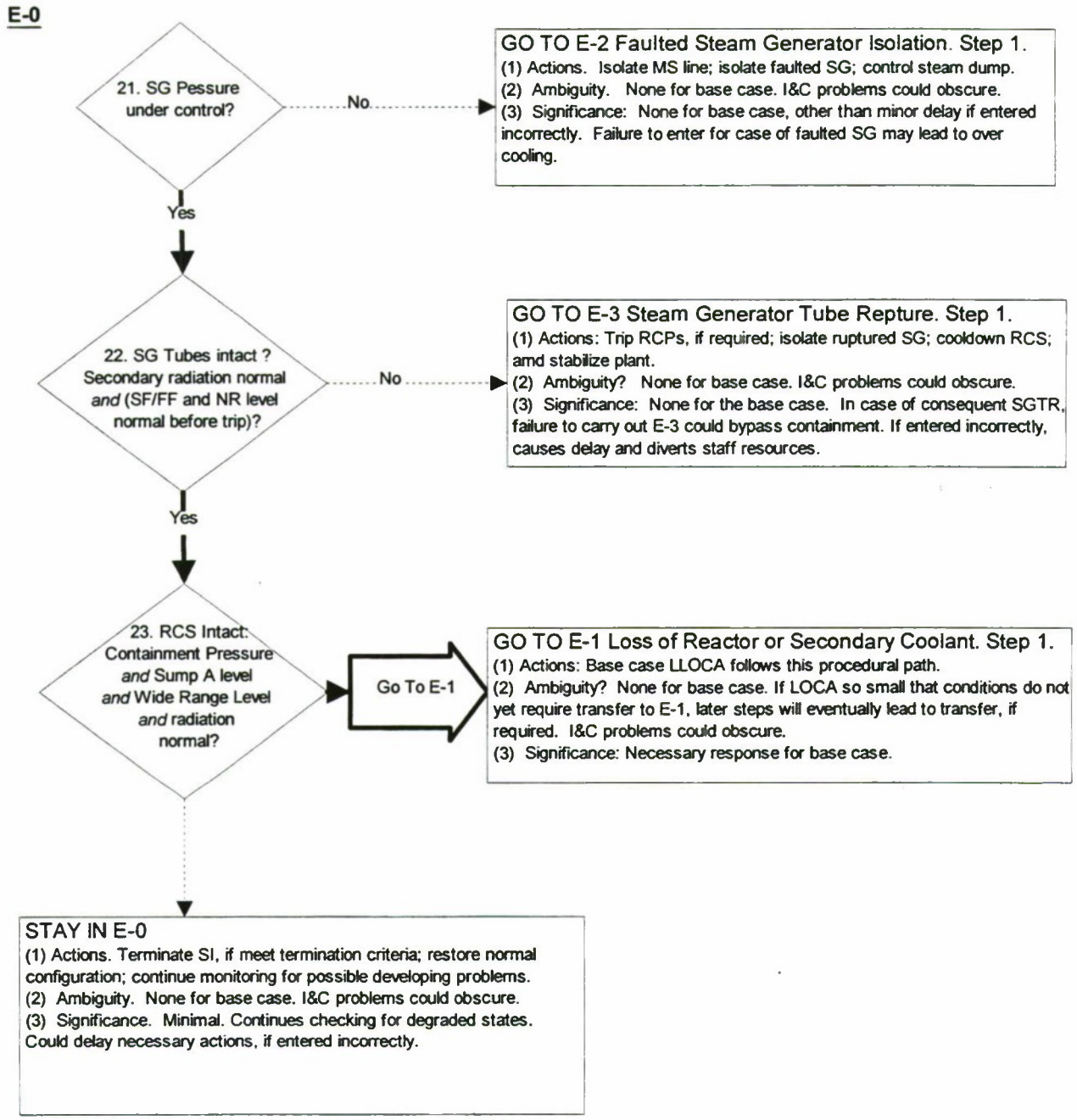


Figure E.12 EOP Map of Base Case SLOCA (Sheet 5)

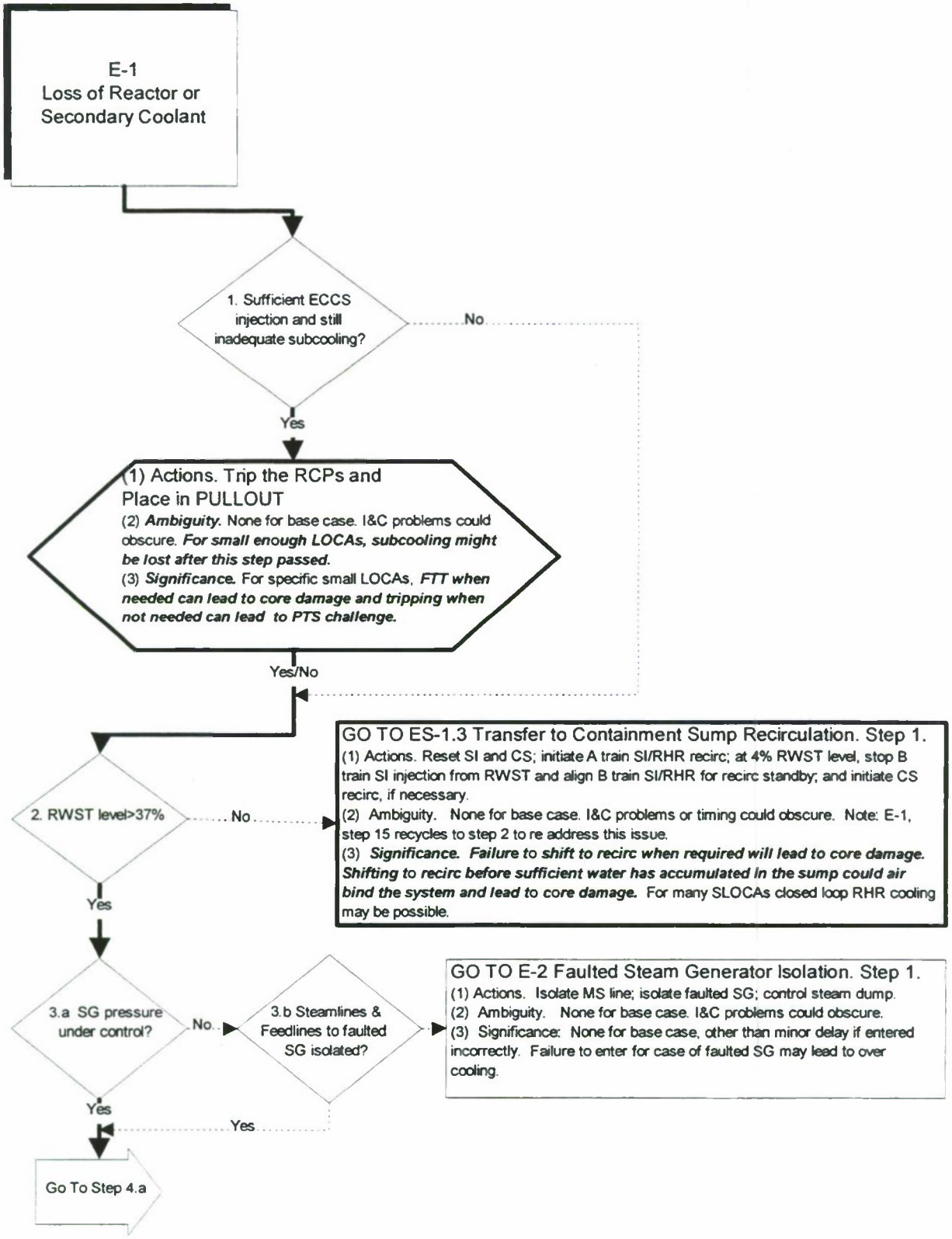


Figure E.12 EOP Map of Base Case SLOCA (Sheet 6)

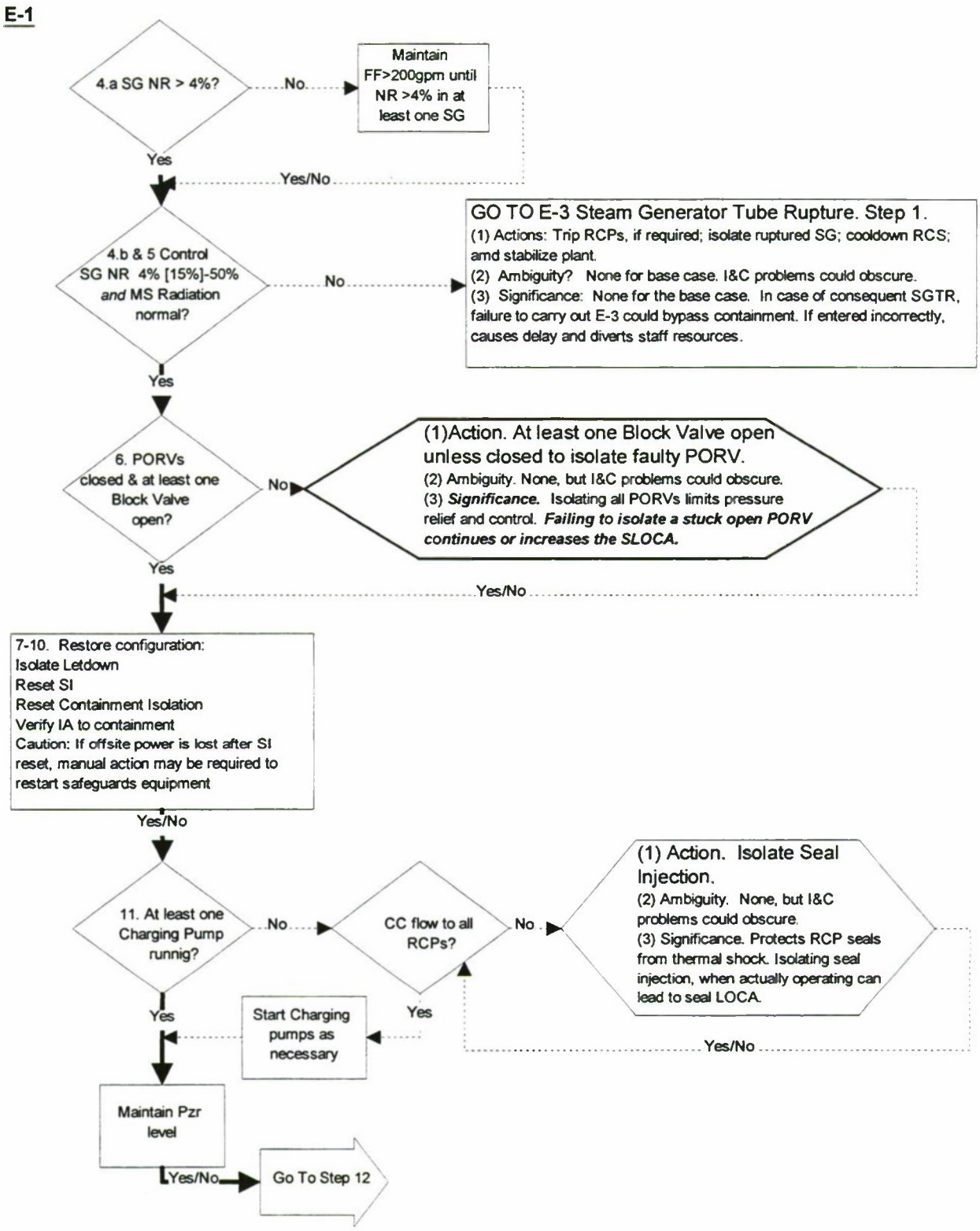


Figure E.12 EOP Map of Base Case SLOCA (Sheet 7)

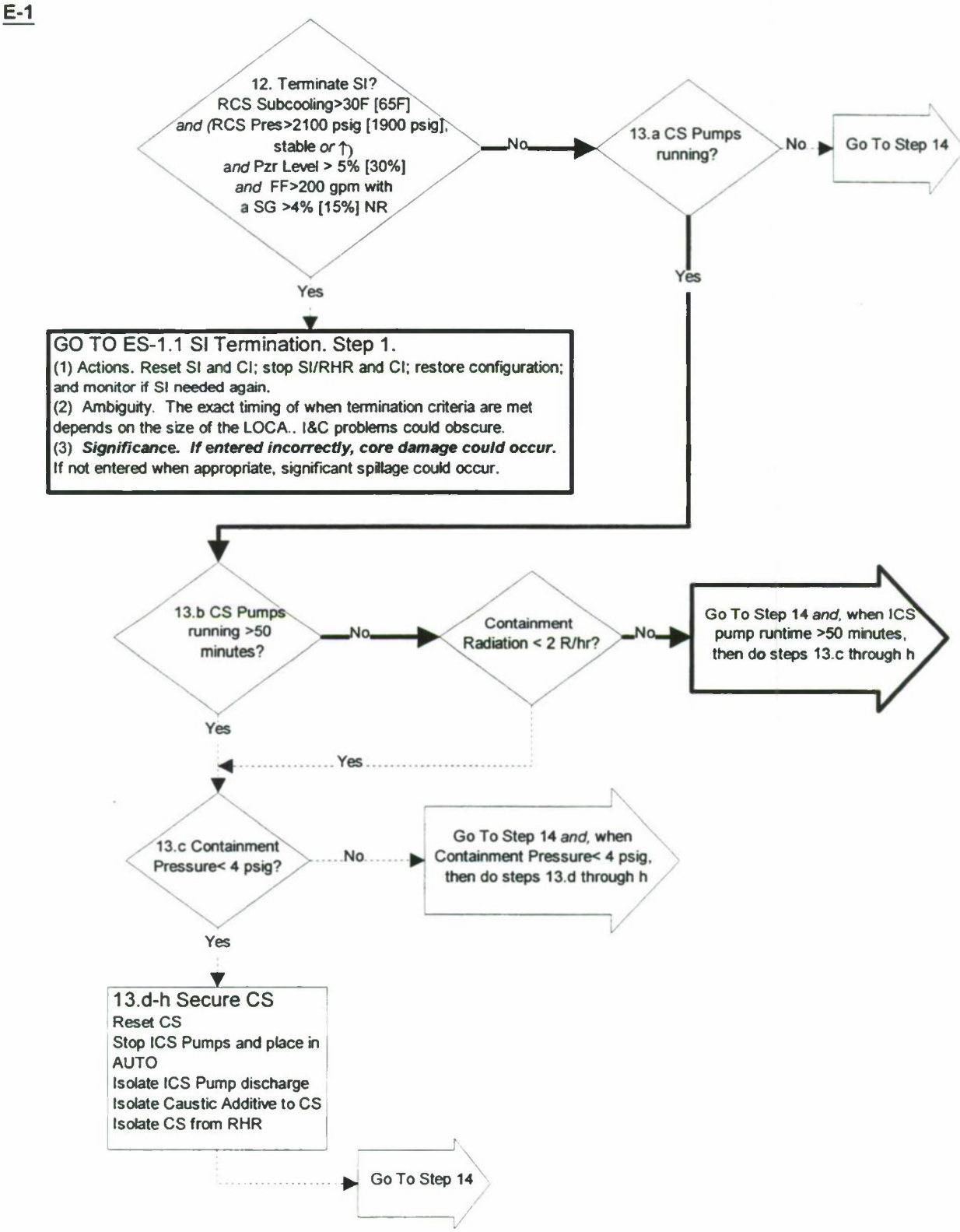


Figure E.12 EOP Map of Base Case SLOCA (Sheet 8)

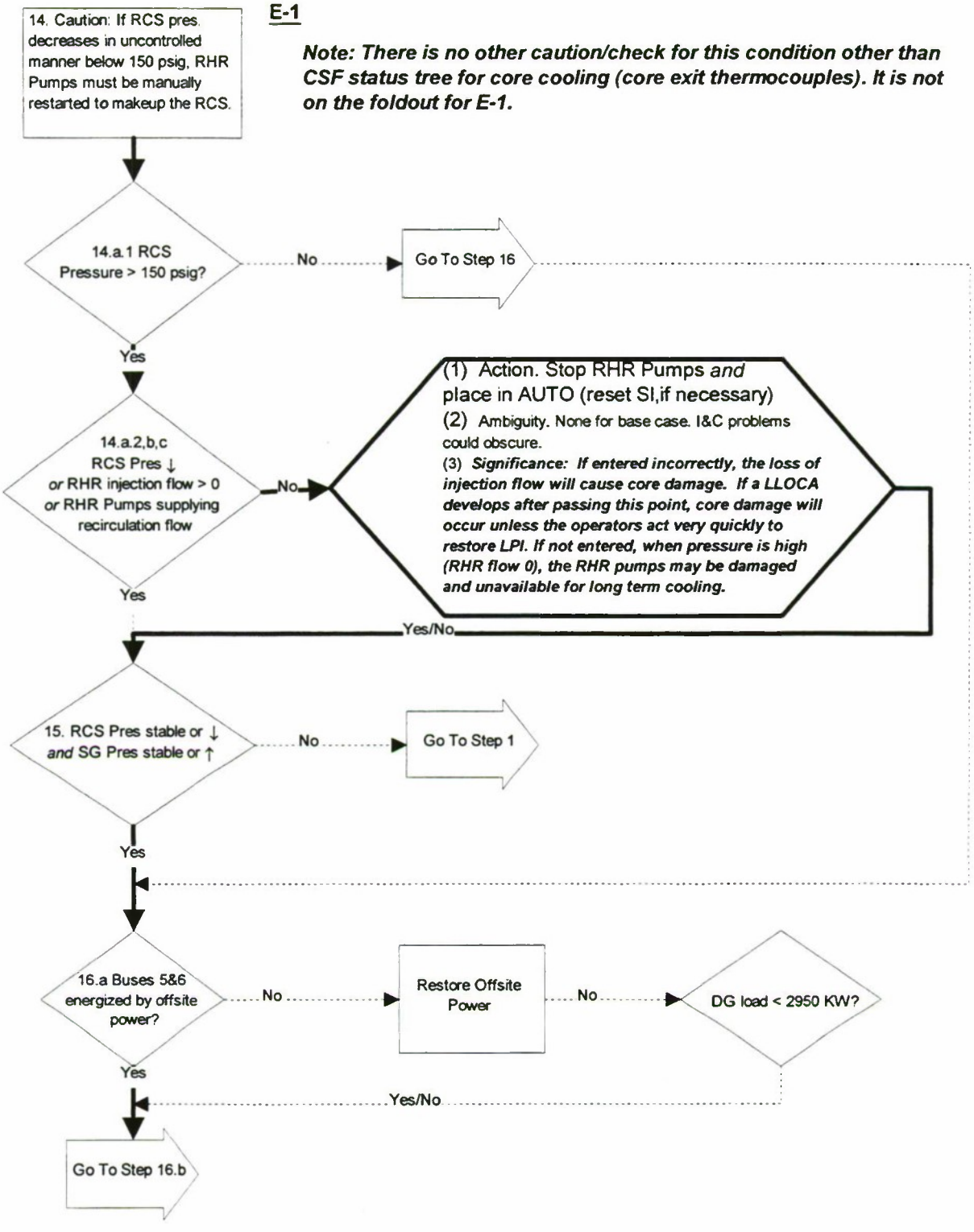


Figure E.12 EOP Map of Base Case SLOCA (Sheet 9)

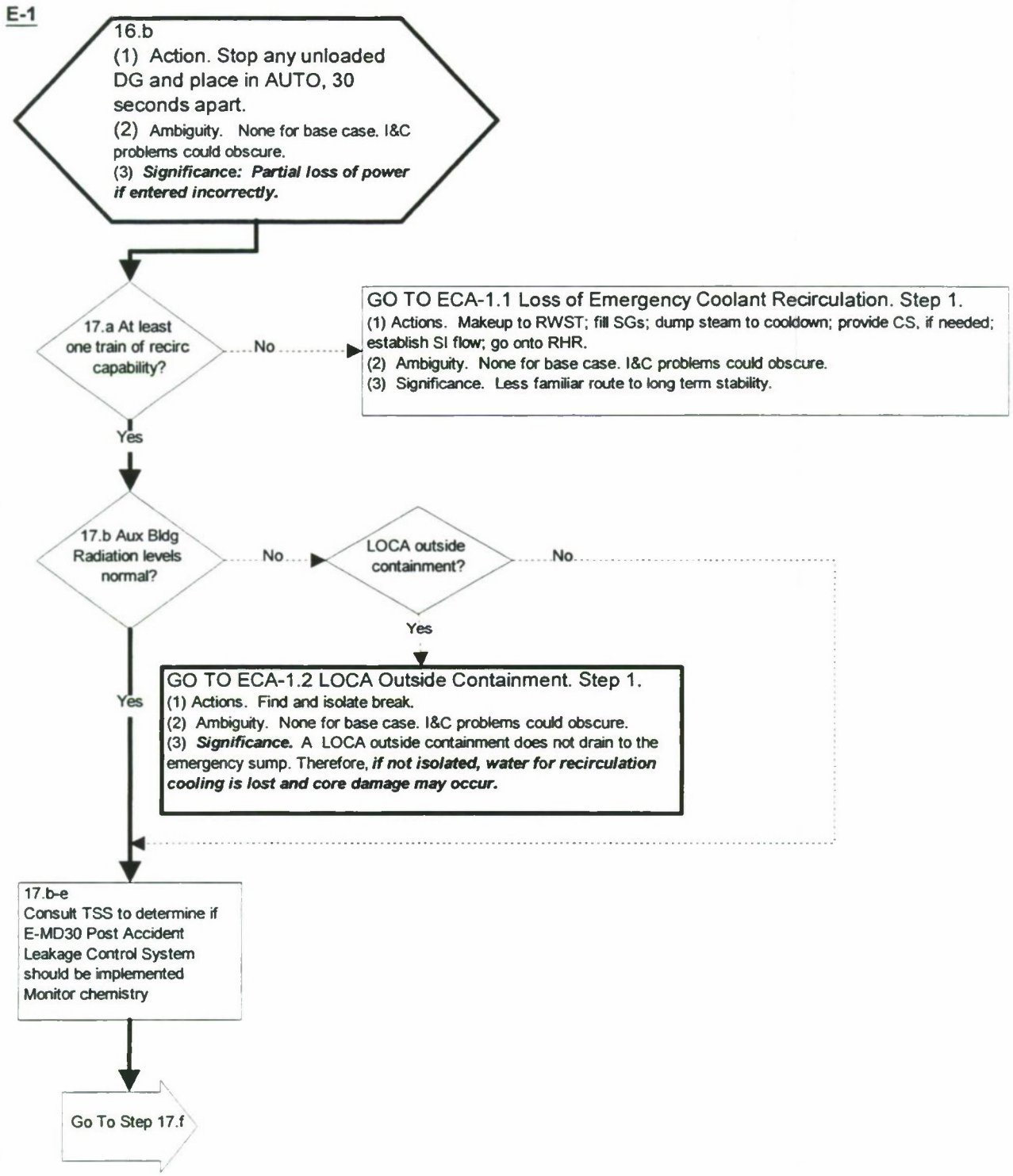


Figure E.12 EOP Map of Base Case SLOCA (Sheet 10)

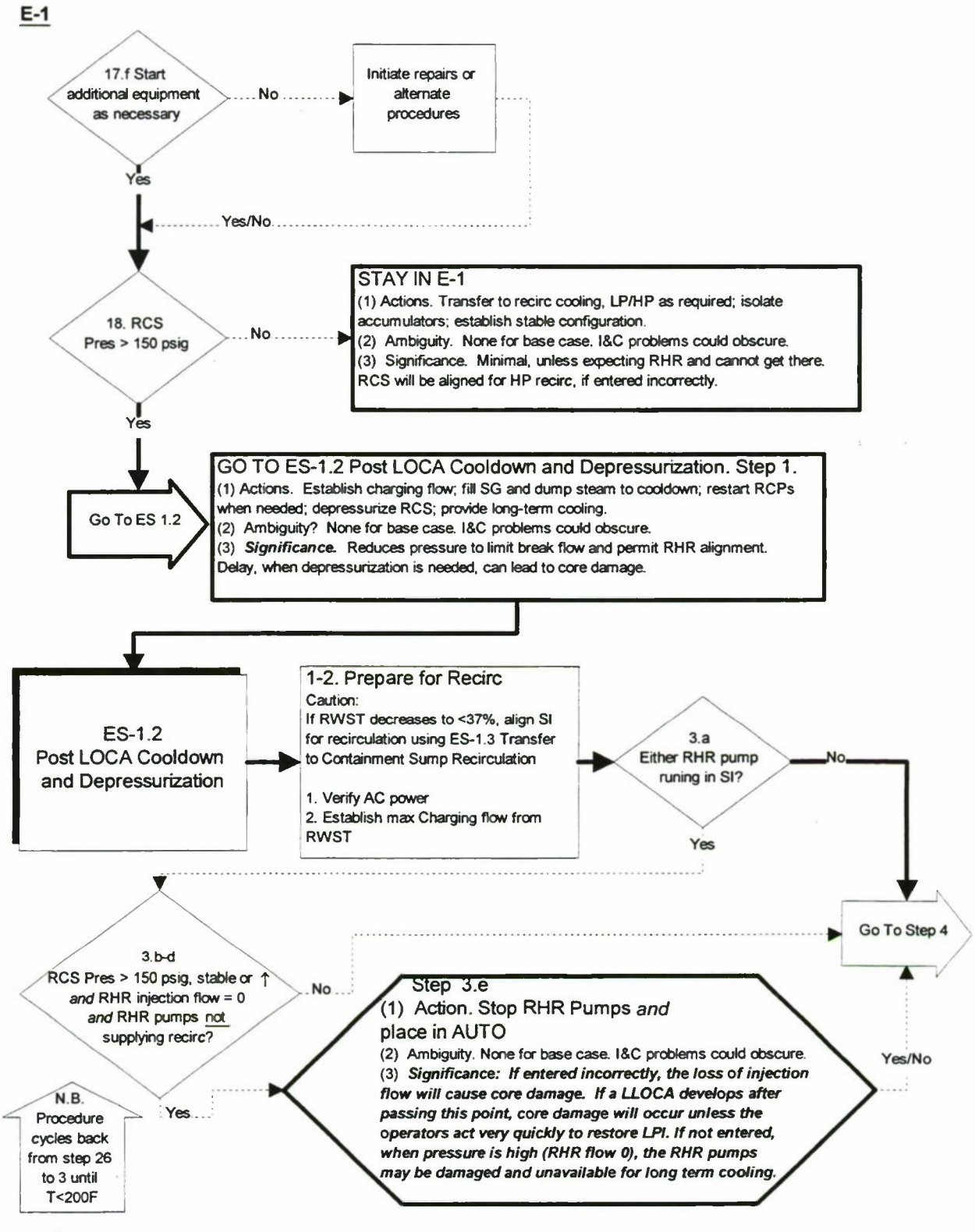


Figure E.12 EOP Map of Base Case SLOCA (Sheet 11)

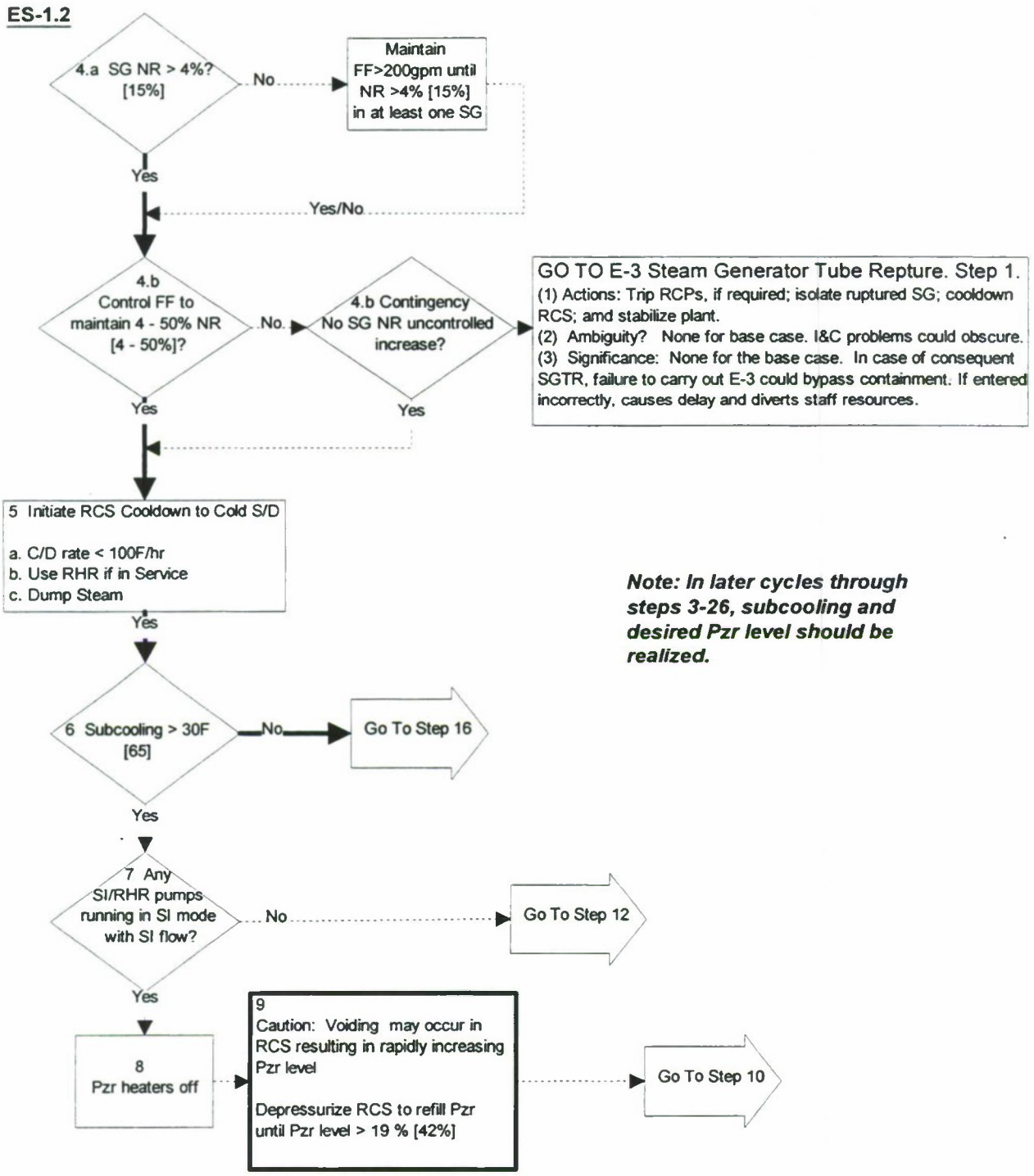


Figure E.12 EOP Map of Base Case SLOCA (Sheet 12)

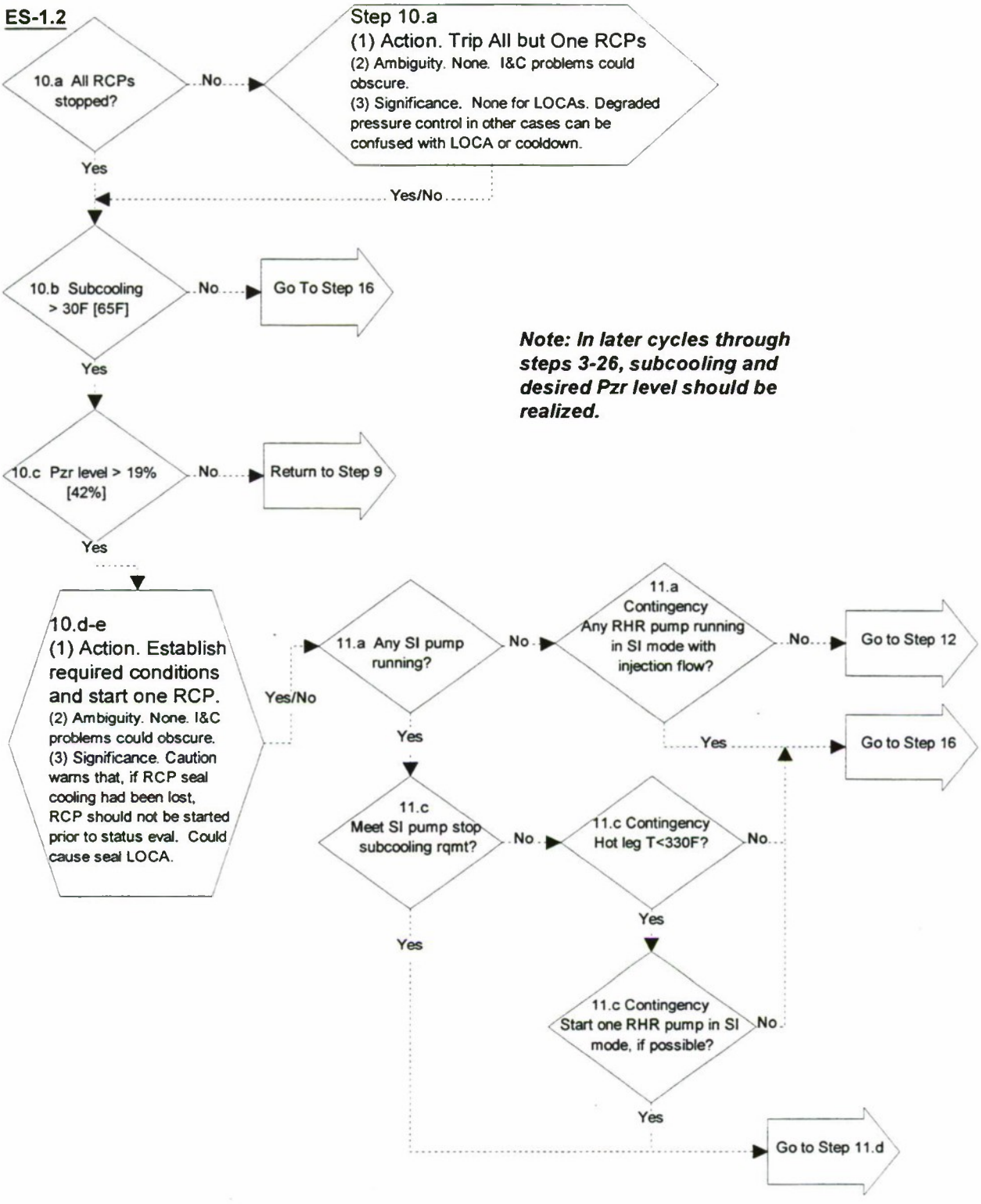


Figure E.12 EOP Map of Base Case SLOCA (Sheet 13)

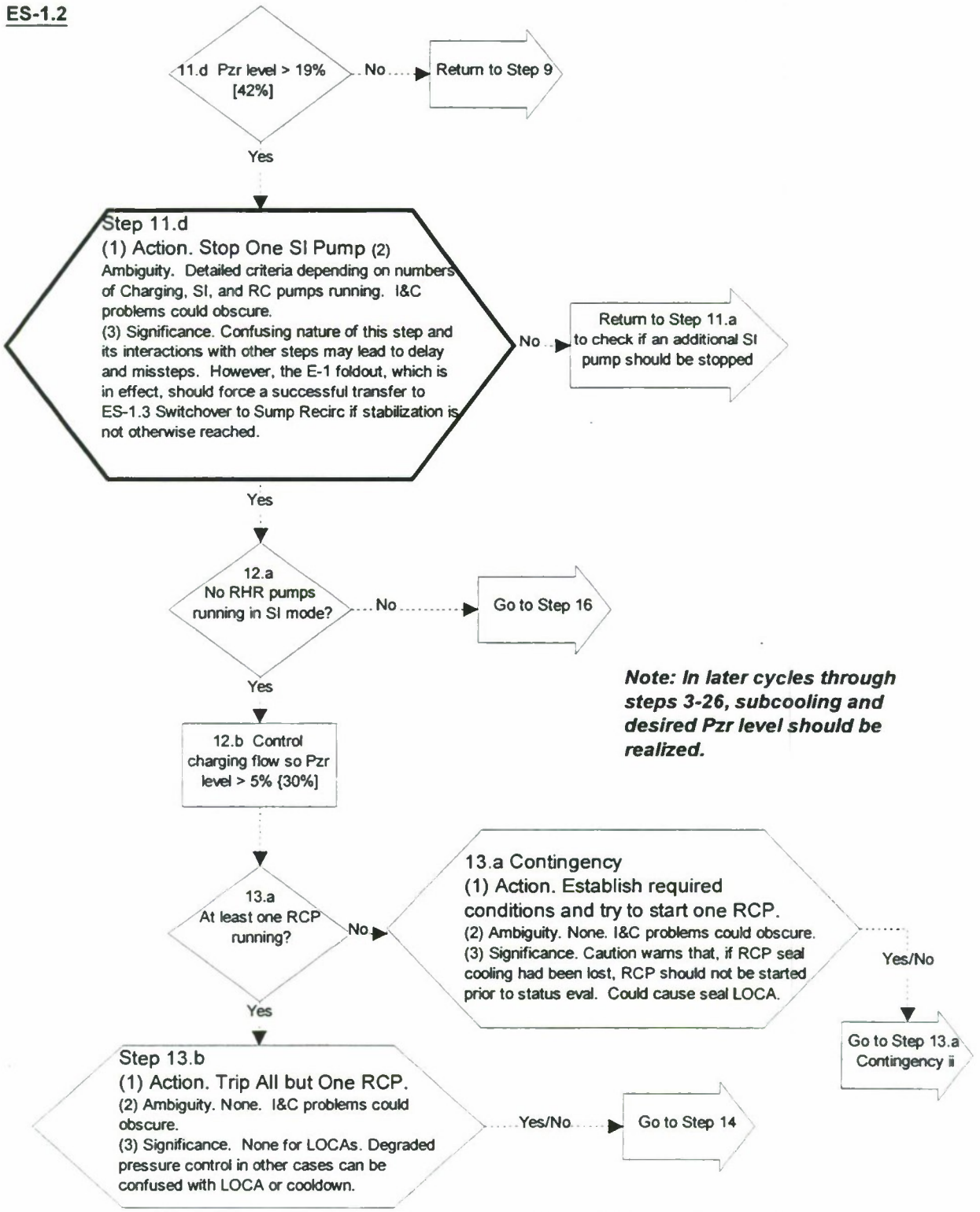


Figure E.12 EOP Map of Base Case SLOCA (Sheet 14)

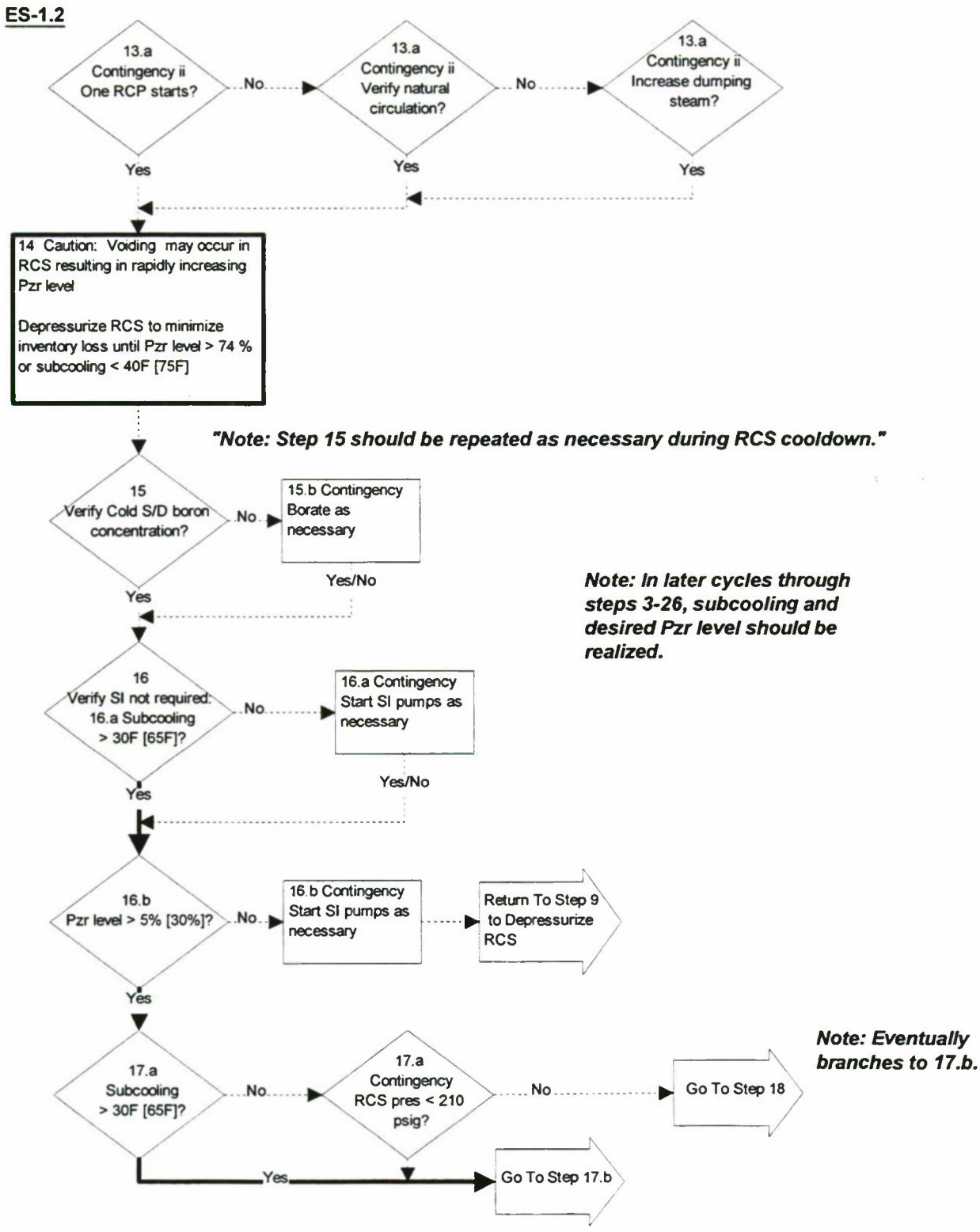


Figure E.12 EOP Map of Base Case SLOCA (Sheet 15)

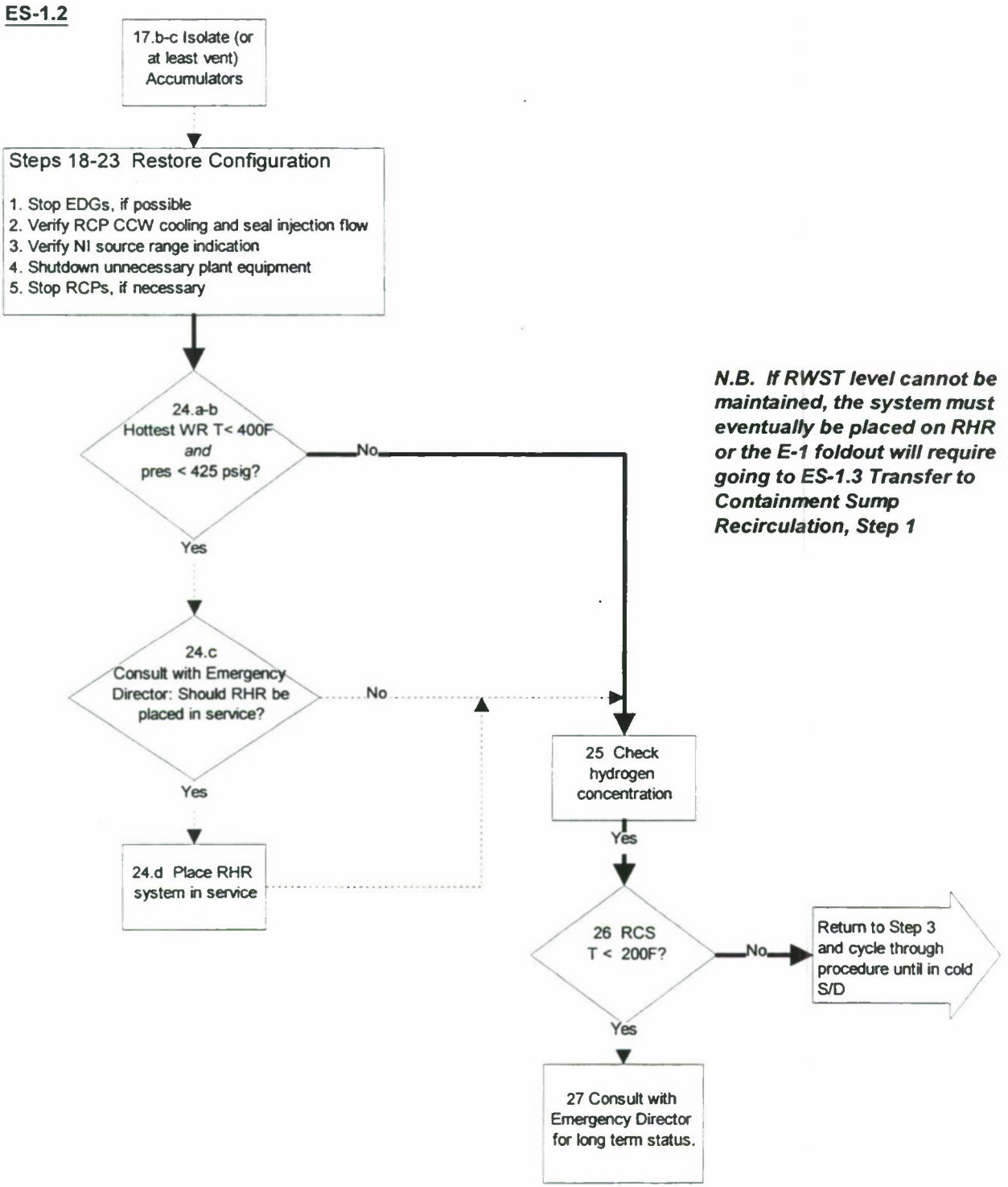


Figure E.12 EOP Map of Base Case SLOCA (Sheet 16)

APPENDIX F
DISCUSSION OF COMMENTS FROM A PEER REVIEW OF A TECHNIQUE FOR HUMAN EVENT ANALYSIS (ATHEANA)

(Paper appears in the *Proceedings of the 26th Water Reactor Safety Information Meeting*, NUREG/CP-0166, U.S. Nuclear Regulatory Commission, Bethesda, MD, 1998.)

Please note that comments described in this appendix were used to guide the revisions to ATHEANA contained in the main body of this report (NUREG-1624, Rev. 1).

Discussion of Comments from a Peer Review of A Technique for Human Event Analysis (ATHEANA)[1]

John A. Forester, Sandia National Laboratories
Ann Ramey-Smith, US Nuclear Regulatory Commission
Dennis C. Bley, Buttonwood Consulting, Inc.
Alan M. Kolaczkowski and Susan E. Cooper, Science Applications International Corp.
John Wreathall, John Wreathall & Co.

Abstract

In May of 1998, a technical basis and implementation guidelines document for A Technique for Human Event Analysis (ATHEANA) was issued as a draft report for public comment (NUREG-1624 [Ref. 1]). In conjunction with the release of draft NUREG-1624, a peer review of the new human reliability analysis (HRA) method, its documentation, and the results of an initial test of the method was held over a two-day period in June 1998 in Seattle, Washington. Four internationally known and respected experts in HRA or probabilistic risk assessment were selected to serve as the peer reviewers. In addition, approximately 20 other individuals with an interest in HRA and ATHEANA also attended the peer and were invited to provide comments. The peer review team was asked to comment on any aspect of the method or the report in which improvements could be made and to discuss its strengths and weaknesses. They were asked to focus on two major aspects: 1) Are the basic premises of ATHEANA on solid ground and is the conceptual basis adequate? 2) Is the ATHEANA implementation process adequate given the description of the intended users in the documentation? The four peer reviewers asked questions and provided oral comments during the peer review meeting and provided written comments approximately two weeks after the completion of the meeting. This paper discusses their major comments.

Introduction

In May 1998, a technical basis and implementation guidelines document for A Technique for Human Event Analysis (ATHEANA) was issued as a draft report for public comment (NUREG-1624

[1]This work was supported by the U.S. Nuclear Regulatory Commission and was performed at Sandia National Laboratories. Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the U.S. Department of Energy under Contract DE-AC04-94AL85000.

[Ref. 1]). In conjunction with the release of draft NUREG-1624, a peer review of the new human reliability analysis (HRA) method, its documentation, and the results of an initial test of the method was held over a two-day period in June 1998 in Seattle, Washington. Four internationally known and respected experts in HRA served as the peer reviewers. A brief description of the reviewers and their credentials follows:

- Dr. Eric Hollnagel - An internationally recognized specialist in the fields of human reliability analysis, cognitive ergonomics, cognitive systems engineering, and the design and evaluation of man-machine systems. Dr. Hollnagel is the author of more than 230 publications, including six books, articles from recognized journals, conference papers, and reports. In January 1998, he published a book entitled *Cognitive Reliability and Error Analysis Method (CREAM)*, which is itself a new HRA method. He is a member of the Swedish Reactor Safety Council and president of the European Association of Cognitive Ergonomics. Since 1995 Dr. Hollnagel has been principal advisor at the Organization for Economic Cooperation and Development (OECD) Halden Reactor Project, and since 1997 adjunct professor of Human-Machine Interaction at Linköping University, Sweden. He has a Ph.D. in cognitive psychology from the University of Aarhus, Denmark.

- Dr. Pietro Carlo Cacciabue - A sector head at the European Commission, Joint Research Centre, Institute for Systems, Informatics, and Safety, in Ispra, Italy. He has published more than 100 papers in professional journals and conferences and is the editor of a number of conference proceedings and books on safety assessment and human factors. Dr. Cacciabue serves as liaison for and holds a number of positions in several international organizations, such as: the International Association for Probabilistic Safety Assessment and Management (director since 1993), consultant for the Direction Générale Aviation Civile, France (since 1994), Institution of Nuclear Engineers, UK, (member since 1984), European Safety Reliability and Data Assoc. (executive committee member 1992-1995), and the European Association of Aviation Psychology (member from 1996 to the present). He has a Ph.D. in nuclear engineering from Politecnico di Milano, Milan, Italy.

- Dr. Oliver Straeter - A researcher for Gesellschaft fur Anlagen und Reaktorsicherheit (GRS) in Germany in the Safety Analysis and Operational Experience Branch. He was a researcher at the RWTH in Aachen and the Ruhruniversität in Bochum and also worked at Siemens Nixdorf AG compiler laboratory in Munich. Dr. Straeter has published several journal articles in the area of human reliability, including a recent article in *Reliability Engineering and System Safety* (Vol 58, 1997), entitled "Human-Centered Modeling in Human Reliability Analysis: Some Trends Based on Case Studies." Dr. Straeter holds a Ph.D. in human engineering psychology from Technical University of Munich.

- Mr. Stuart R. Lewis - A consultant specializing in the application of reliability and quantitative risk analysis methods. Mr. Lewis is the president of Safety and Reliability Optimization Services (SAROS), Inc., Knoxville, TN, which he co-founded in 1984. Examples of current and past relevant work include assisting nuclear licensees in updating and maintaining their

probabilistic safety assessments (PSAs) and updating the HRAs for the PSAs of several licensees. He has also assisted the Oak Ridge National Laboratory by reviewing analyses performed under its Accident Sequence Precursor Program, and is assisting Electricité de France in keeping abreast of technical and regulatory developments concerning severe accidents. He performed the HRA portion of several of the probabilistic risk assessments (PRAs) performed by nuclear power plant licensees for the U.S. Nuclear Regulatory Commission's Individual Plant Examination program. Mr. Lewis holds both B.S. and M.S. degrees in nuclear engineering from Purdue University.

In addition, approximately 20 other individuals with an interest in HRA and ATHEANA also attended the peer review meeting and were invited to provide comments. The peer review team was asked to comment on any aspect of the method or the report in which improvements could be made and to discuss its strengths and weaknesses. They were asked to focus on two major aspects:

(1) The soundness of the philosophy underlying ATHEANA. Are the basic premises on solid ground and is the conceptual basis adequate?

(2) Is the ATHEANA implementation process adequate, given the description of the intended users in the documentation? Assuming the technical basis is adequate, is the guidance for conducting the search and quantification processes and for integrating the results into the PRA adequate, for example, clear, effective, usable?

The four peer reviewers asked questions and commented orally during the peer review meeting. They also provided written comments approximately two weeks after the meeting. All of the reviewers indicated that the ATHEANA method had made significant contributions to the field of PRA/HRA, in particular by addressing the most important open questions and issues in HRA, by attempting to develop an integrated approach and by developing a framework capable of identifying types of unsafe actions that generally have not been considered using existing methods. The reviewers had many (and sometimes similar) concerns about specific aspects of the methodology and made many recommendations on ways to improve and extend the method and to make its application more cost effective and useful to PRA in general.

This paper discusses the major comments received from the peer review team and provides responses (but not necessarily resolutions) to specific criticisms and suggestions for improvements. A list of the general strengths and weaknesses of ATHEANA, as indicated by the reviewers, is provided first. Next, specific comments bearing on major aspects of the method are presented and discussed . Finally, general comments related to improving the efficiency and usefulness of ATHEANA are addressed.

General Strengths and Weaknesses of ATHEANA

The reviewers' general opinion of ATHEANA is that the method represents a significant improvement in HRA methodology; it is a useful and usable method; and it is a "good alternative

to first-generation HRA approaches." However, the method does not yet go far enough and therefore needs to be improved and extended. Several of ATHEANA's strengths, as indicated by the four reviewers, are listed below.

(1) "Until now, in my opinion, there is no other published approach that tries to solve the problem of including EOC [errors of commission] in PSA in such an extensive way. Other methods address only parts of this. Overall, the general approaches and concepts developed in the ATHEANA-method are appropriate to deal with the problem of EOC. I think that the ATHEANA-method as currently documented contains a lot of important aspects for understanding and integrating EOCs into PRA. However, many aspects are only mentioned implicitly. An explicit and concise elaboration is necessary to assure practicability..."

(2) "The real value of ATHEANA seems to be as a systematic way of exploring how action failures can occur. This is something that conventional HRA methods do not do well, if they do it at all, since they tend to focus on producing numbers. Although this use of ATHEANA does not really answer the need for an HRA approach, it might have a value in itself (as the comments from the demonstration participants expressed) and it might conceivably be decoupled from the HRA side. In that case a more streamlined method may be developed, that is less cumbersome to use. The demonstration of ATHEANA very clearly showed how it can be used to develop detailed qualitative insights into conditions that may cause problems, how it may generate a solid basis for redesign of working procedures, training, and interface, and how it may be used as a tool for scenario generation. Each of these are significant achievements in their own right."

(3) "The method described in ATHEANA is certainly well suited for overcoming the difficulties encountered when applying more classical human reliability methods and focuses on the important issues of context and cognition that need to be tackled. Many aspects of the methodology are commendable and give great added value to the whole methodology. In particular, the following features are important:

- the details in describing many processes and steps in the application of the methodology;
- the consideration for the crucial features that affect human cognition and behaviour in managing modern plants, included in concepts like the error-forcing context; and
- the identification of the appropriate retrospective approach for the evaluation of the factors influencing behaviour and basic data for prospectively analysing the likely outcome of erroneous behaviour and probabilities."

(4) "Properly applied, the methods that comprise ATHEANA should be able to yield significantly more insight into the nature of human actions that can contribute to the occurrence of a core-damage accident. These methods clearly provide a framework for

identifying some types of unsafe actions, and especially errors of intention, that would generally not have been considered using current methods. Moreover, they allow for a much more careful definition of the context and causes of these unsafe actions.

Without broader application of the methods, however, it is impossible to draw conclusions regarding the degree to which important actions that are not considered in present PRAs will be identified. It is reasonable to expect that some of the most important potential unsafe actions would be the result of subtle aspects relating to interactions among plant conditions or performance shaping factors that would be very difficult to postulate, even with the proper team makeup and extensive time available for the analysis.

What can be expected is that the methods will provide for the integration of understanding from the diverse team members that will lead to these new insights. This should be a synergistic process, allowing knowledge to be shared and captured in a way that enhances both the completeness and realism of the PRA, and the quality of training and procedures. A significant advantage of the method could be to provide a rationale for the characterization of the human failure events that often eludes us in present PRAs. While present methods may arguably yield reasonable quantitative results, they often fail to provide an understanding of the underlying causes of the human failures that are analyzed. Absent that understanding, it is very difficult to identify measures that can be taken to reduce the risk associated with unsafe actions. Consequently, it is often frustrating to identify a human action as risk-significant, but not to be able to give very satisfactory answers as to why, or what could be done to reduce that significance. With ATHEANA, on the other hand, the analysis of an unsafe action is necessarily truncated if an error forcing context cannot be identified."

The above statements clearly indicate that the ATHEANA method has made significant improvements in HRA methodology and that the method, as documented, is a useful and usable tool. Perhaps not surprisingly, current members of the ATHEANA development team (the authors of this paper) agree generally with the above statements. However, the reviewers were also very clear in indicating that, in their opinion, there are several important general shortcomings of ATHEANA. These are listed below.

(1) "There seems to be an inconsistency in the level of models being used, ranging from EOO-EOC (errors of omission - errors of commission) over the information processing model to the notion of slips and mistakes. It would be interesting to consider how the search process could be strengthened while relaxing the dependence on the model(s)."

(2) "There is no identifiable way of encompassing management and organization [M&O] factors or responding to the challenges of the broader socio-technical or contextual way of thinking (which also is seen by the conceptual problems in taking M&O factors into account in PSA)."

(3) "Insufficient consistency in the terms and concepts used, and significant differences between what is written in NUREG-1624 and what was said at the review."

(4) "The ATHEANA method is very cumbersome and presumably very costly. The guidance is too complex and depends too much on subject matter experts."

(5) "The quantification method is weak, and the quantitative results (of the demonstration) are unsubstantiated. The quantification is excessively dependent on expert judgement, hence possibly has low reliability as a method."

(6) "The qualitative results are good, but these might have been obtained in other ways, perhaps more efficiently. It is also doubtful whether a utility will undertake a significant effort just to get the qualitative results."

(7) "The implementation of the basic approaches is sometimes not elaborated far enough from my perspective. This makes the use of the method in the current status difficult and may cause high variance between different users. I also observed that the document NUREG-1624 and the presentations on the peer-review are sometimes not in accordance to each other. In order to have a usable and profound method, the basics has to be refined and extended."

(8) "Especially, I see the danger that the whole suggested procedure may fail if the role of the cognitive model (i.e. to work out and structure EMs [error mechanisms]) is not elaborated further. The cognitive model has a considerable effect on the consistency between EMs, the compatibility of prospective and retrospective analysis, the link between EFC [error-forcing context], EM and UA [unsafe actions] as well as the quantification procedure."

(9) "The methodology clearly presents a dilemma. Its effectiveness results from forming a diverse, experienced project team to perform a comprehensive, broad-ranging analysis. Few organizations, however, appear to be in a position to undertake such an extensive analysis without clearly defined, commensurate benefits. Thus, even if it is an excellent methodology from a technical standpoint, it will not be very valuable if it will not be used."

(10) "The potential wide application and popularity of the method are, however, associated with the *easiness of application* of the method and the *completeness* of the supporting information and data. The first issue (*easiness of application*) is related to the clear differentiation between retrospective and prospective analysis, which contains also the question of applicability of the cognitive model. The method, as presented in the report, generates some confusion, especially for non-specialists in human factors, even though one could argue that the ATHEANA team should contain such expertise. The question of the availability and *completeness* of a reference database and clear tables of parameters and variables sustaining the HRA approach has, in practice, already been almost completely tackled and solved. What remains to be done is simply the clear definition of the connections between such databases

and parameters on the one hand and models, paradigms and structure of ATHEANA on the other."

Although the above set of comments is not necessarily complete in regard to the limitations of ATHEANA as indicated by the peer reviewers, it is thought that the selected set does represent the more important general limitations identified by the reviewers. Some of the above criticisms are responded to directly, but in other cases, some future decisions are required. The criticisms and responses are grouped below according to major aspects of ATHEANA.

The ATHEANA Framework and Underlying Models

Two important aspects of the ATHEANA methodology are (1) the multi-disciplinary HRA framework (see Figure 2.1, NUREG-1624 [Ref. 1]) that describes the interrelationships between human error mechanisms, the plant conditions and performance-shaping factors (PSFs) that set them up, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe, that is, UAs and (2) the human information processing or "cognitive" model (see Figure 4.1, NUREG-1624 [Ref. 1]) that is used to describe the human activities and mechanisms involved in responding to abnormal or emergency conditions and thereby assist analysts in searching for potential unsafe human actions. Several of the criticisms listed above (e.g., 1, 8 and 10) raise concerns about the descriptions and use of the framework and the cognitive model in ATHEANA. Essentially all of the peer review team had questions or concerns about these aspects of ATHEANA.

Regarding the multi-disciplinary HRA framework, several reviewers thought that the definitions and distinctions between the components of the framework and their interrelationships with each other and with the cognitive model were not sufficiently clarified. The reviewers considered this important because they correctly assumed that understanding the framework (and to some extent its relationship with the cognitive model) was important to understanding the ATHEANA methodological approach. One concern was exactly what was meant by "error mechanisms," how they are used in ATHEANA, and whether or not the terminology was appropriate, given the underlying assumptions of ATHEANA, for example, people usually behave rationally and are led to UAs as a function of the circumstances. Another concern was that the distinction between error mechanisms, PSFs and plant conditions was not sharp enough.

Clearly, "crisper" definitions of these terms are needed in the ATHEANA documentation because they are used to guide analysts in their search for UAs and the associated EFCs. One goal of using the construct of error mechanisms is to convey to analysts that there are human information processing activities that may be appropriate in some circumstances, but not in others. Examples of such activities are provided in the ATHEANA documentation and they are elaborated to some degree in the discussion of the cognitive model (Section 4 of NUREG-1624). The main purpose of the discussion in Section 4 is to encourage analysts to think about the potential for human error in a different manner than has been done in other HRA methods and not necessarily to provide a complete and validated set of error mechanisms. It is not obvious that further elaboration of possible error mechanisms will necessarily facilitate the ATHEANA search process or the quantification

process. Nevertheless, the clear use of the construct of "error mechanisms" in the context of ATHEANA will be addressed. To the extent that additional explanation and elaboration of potential error mechanisms will facilitate the search and quantification processes, such work will be performed for later revisions.

Consideration will also be given to a couple of reviewers' suggestion that the term "error mechanism" should be dropped because human information processing is probably not limited only by processing "mechanisms," which implies structures, (e.g., processing is probably also limited by inappropriate processing strategies) and because the behavior that leads to UAs is only an "error" in hindsight. As is assumed by ATHEANA, the information processing performed may have been perfectly appropriate in most situations and is inappropriate only because of special circumstances; it therefore is not an error in the usual sense. Recommendations for a replacement term for the construct included "behavior mechanisms" or simply "cognition."

As noted earlier herein, another concern expressed by the reviewers was with the distinction between plant conditions, PSFs, and error mechanisms. It was argued that it is not always easy to determine whether a particular factor belonged in one category or another (e.g., whether procedures and instrumentation problems should be categorized as plant conditions or PSFs) and that it was necessary for ATHEANA to make the distinctions clear. One reviewer indicated that the PSFs should be standardized and made complete. The current ATHEANA documentation has acknowledged that, in some cases, the distinctions are not always perfectly clear, but the emphasis from the analysis point of view is to ensure that the factors relevant to the EFCs are considered. Although it may be possible for the ATHEANA team to develop a useful underlying model for grouping the relevant factors and this effort may be attempted for revisions to the method, the main consideration in the application of ATHEANA is that as many relevant factors as possible are considered in identifying the EFCs.

Other issues regarding the models used in ATHEANA concerned the use of the EOC-EOO distinction, the slips versus mistakes categorization in the context of the other models used in ATHEANA (e.g., see criticism 1), and the ability of the method to correctly consider crew-related factors when the cognitive model generally applies to information processing by an individual. The latter concern suggests that it might be useful to include a "crew interaction" model that could be integrated with the cognitive model. The team will examine the feasibility and usefulness of such an endeavor.

Regarding the slips versus mistakes categorization, several reviewers argued that this categorization was probably not necessary and at least one argued that it was inappropriate. The use of such terminology, which does presume an underlying model not explicitly adopted by ATHEANA, will be addressed in future revisions.

Finally, several reviewers also suggested that the framework and models used in ATHEANA be compared to other more familiar models from existing methods in order to elucidate the differences between ATHEANA and other HRA approaches. This would certainly be a useful addition to the

ATHEANA report in that it would assist analysts in realizing the advantages to conducting an ATHEANA HRA. Clearly, revision of the ATHEANA documentation should discuss the uses and appropriate application of ATHEANA to various analysis tasks.

The ATHEANA Process

This section addresses a variety of important comments on aspects of the ATHEANA process.

Retrospective Analysis

The use of an ATHEANA-driven retrospective analysis of plant and other operational events was listed as one of the strengths of the ATHEANA process (see strength 3). More than one of the reviewers commented on the positive aspects of the use of retrospective analysis for assisting analysts in evaluating their plant and supporting the proactive HRA. In fact, their main concern was that a formalized, structured procedure, separate from the proactive search process detailed in ATHEANA, was not provided in the existing documentation. They suggested that a separate write-up and flow diagram be developed on how to perform retrospective analysis and on how it interfaces with the proactive analysis. Reviewers concerned with the definitions and relationships/connections between the elements in the framework and cognitive model also felt that clarification of these aspects would also greatly facilitate the retrospective analysis (see criticism 8). They argued for "taxonomies for actions, errors, and PSF" and clear rules for event decomposition in the retrospective analysis. In addition, they also suggested providing improved guidance on how to use the HERA database (Ref. 2) and the retrospectively analyzed events documented in Appendix B of NUREG-1624. [Note that HERA is a database being developed for the USNRC that contains documentation of significant events from nuclear and other industries. The events are represented from the ATHEANA perspective and in ATHEANA terminology.]

The ATHEANA team agrees that additional guidance on how to perform and use retrospective analysis and the HERA database would be useful additions to the ATHEANA documentation. Analysts would be able to learn more directly about the characteristics of ATHEANA and in addition to "self-training" on the ATHEANA "philosophy," framework, and models, they would better understand events that have occurred at their plant and how other events might occur in the future.

Prioritization Process

Several of the criticisms listed above (e.g., 4, 6, and 9) indicate that the demands of applying ATHEANA may be cost and time-prohibitive for many nuclear power plants. One aspect of ATHEANA that was developed in an attempt to allow users to focus their limited resources was a process for prioritizing the more important accident scenarios. While the reviewers generally were supportive of the prioritization process, several suggested that the process be further improved and proceduralized. Specifically, they wanted a "greater consideration of the risk potential of possible human failure events (HFEs)" and (on the basis of information provided at the peer review on the results of the trial application of ATHEANA) an earlier identification and assessment of crew

characteristics and other M&O factors that might make certain types of scenarios more likely to contain risk significant UAs than others.

Once again, the ATHEANA team agrees that improvements in the prioritization process, as suggested by the reviewers, would be useful. A characterization of the way plant crews interact with one another and approach accident scenarios would assist analysts in determining the types of scenarios likely to be problematic (see Appendix A, Section A.7, of NUREG-1624 for details). Explicit incorporation of other M&O factors (which is considered a weakness of ATHEANA; see criticism 2) at the prioritization stage may also be beneficial. It should be noted that there is nothing about ATHEANA that is inherently incompatible with the consideration of M&O factors (contrary to criticism 2). The main problems associated with accounting for M&O factors in ATHEANA are that there are no currently accepted methods for modeling such factors, and the costs associated with the additional analysis may offset the benefits.

In addition to these two items, there were several other comments related to the ATHEANA process that the ATHEANA team, in principle, agree with. They include the following:

- Provide further guidance for the creative thinking/search process to lessen variability and interpretation, including providing guidance on how to "manage" group discussions. Also emphasize the need to document the process "as you go" and more closely link the documentation tables with the relevant sections of the search process.

- Stress more strongly the importance of modeling the support systems, in addition to the main safety systems, in searching for potential HFEs and UAs.

- Discuss to what extent dynamic reliability is or is not part of the process and why.

- Further stress where and how one treats organizational factors, team interactions, recovery, and dependencies

One additional comment on the ATHEANA process warrants a response from the ATHEANA team. It was suggested that there should be an explicit use of formal task analysis in conducting ATHEANA. While it is true that some of the existing HRA methods recommend the use of formal task analysis in order to understand the operators' tasks during accident scenarios, it is not clear that the additional costs associated with formal task analysis would necessarily be useful in applying ATHEANA. In conducting ATHEANA, the HRA team, using appropriate procedures, examines the crew's responsibilities during various accident scenarios and, when possible, conducts simulator exercises. It may be beneficial, however, to emphasize the step of carefully examining procedures relevant to particular accident scenarios early in the process of identifying potential UAs and their EFCs. This step is certainly part of task analysis and should assist analysts in identifying the more critical and likely UAs for further analysis.

The ATHEANA Quantification Process

The reviewers raised several issues associated with quantification. These include the overall ATHEANA approach of identifying and quantifying situations where the likelihood of failure is very high, the methods used to quantify a UA in a particular EFC, and the effect of the various PSFs and plant conditions on the likelihood of failure. Other comments pertained to the need to address recovery actions and dependencies in the quantification process.

A basic premise driving the development of ATHEANA is that the HFEs that have heretofore been most problematic for identifying and assessing their impact on plant risk are those in which a particular context creates a very high likelihood of failure. This premise is in contrast to the premise implicit in most other HRA methods that there is a constant (and usually low) likelihood of human failure for any given accident scenario. (It is true that some HRA methods have moved beyond this simple assumption, but they have not been widely used and have rarely been applied in a systematic way.) Therefore, the search process and the associated quantification process are principally aimed at identifying those conditions in which the UA probability will be much higher than in other non-forcing conditions. However, this fact does not imply that the application of ATHEANA would never identify situations in which the probability of the UA, given the EFC, is significantly less than 1.0. In such situations in which human error probabilities must be estimated, existing applicable HRA methods may be useful for quantifying the error probability, given the defined EFC.

Several reviewers suggested that the methods for estimating the probability of the UA be revised or broadened. We agree that alternative methods can be used. In the trial application, HEART (Ref. 3) was used because it most directly used conditions similar to those identified as EFCs in the scenarios, bearing in mind the data sources used in HEART and the level of description for the conditions under which the data were gathered. It is important to ensure that the method and data used to quantify the likelihood of an unsafe action in a particular EFC will be sensitive to those factors that create the forcing nature of the EFC conditions. An alternative approach that was suggested is to use a subjective-assessment method like SLIM-MAUD (Ref. 4). Such methods could be used in principle. However, the continuing difficulty is one of selecting appropriate anchor points for the assumed probability distribution. This problem has been raised previously in reviews of HRAs that have used methods like SLIM-MAUD in which the analyst provides the range within which a point probability is interpolated.

One reviewer suggested the use of tables for specific PSFs and plant conditions that showed their influence on the likelihood of unsafe actions. Such data could be derived from historical experience in the events reported in the database. However, this approach is at odds with the ATHEANA method, which considers the influence of PSFs and plant conditions to be an integral set of influences on performance, and not separable and discrete influences such as those reported in THERP (Ref. 5). In ATHEANA, the typical issue is "What combination of plant conditions and weaknesses in the displays, procedures, etc., has to occur to mislead operators into believing that action 'x' needs to be taken?" The key is that it is the combination, not each influence separately, that is important.

It is agreed that the analysis of recovery actions is problematic. In applying ATHEANA, the team has considered recovery on a case-by-case basis, looking specifically at ways the scenario may develop, where additional outside staff may become involved, and so on. The approach thus far has not been to treat recovery actions as separate from the initial UAs. Similarly, the method does not include explicit processes to model and quantify dependencies between actions. Clearly, future revisions and applications of ATHEANA must better address the analysis of recovery actions and dependencies.

Improving the Efficiency, Usefulness, and Consistency of ATHEANA

Several of the comments from the reviewers (e.g., criticisms 4, 6, and 7) express concerns about the resources required to apply ATHEANA and whether or not the obtained results will be important enough and complete enough for users to justify the costs. A related concern is whether the method has been specified in enough detail and "elaborated far enough" to allow consistency in the results obtained by different analysts applying the method. Similar concerns regarding resource demands and completeness were raised by the participants of the first demonstration of ATHEANA, which was held in 1997 at a pressurized water reactor nuclear power plant (see Appendix A, Section A.7, of NUREG-1624 for details).

The ATHEANA team acknowledges that a broad and careful application of ATHEANA will require significant resources. Although the search for important HFEs, UAs, and their EFCs will never be trivial, it can be manageable. Thus, steps will be taken to improve its efficiency (some of which are discussed below). Will the resources demanded by the method be worth it? ATHEANA will identify demanding accident scenarios and potential UAs and EFCs that could lead to serious accidents. Whether or not the method will identify numerous events that result in large increases in calculated plant risk metrics remains to be seen. Moreover, given the inadequacies of the HRA methods that were used to conduct the existing nuclear plant PRAs, it is impossible to know exactly what a realistic estimate of the baseline HRA contribution should be. Therefore, it is difficult to predict what kinds of changes in risk metrics to expect. In any case, the benefits of ATHEANA are much broader than those from performing revised PRA calculations alone. The improvements in HRA modeling to better identify operator vulnerabilities in accident scenarios and to better understand what are the contributors to operator performance will certainly be of significant benefit in assessing and managing plant risk. Nevertheless, it must be the case that the method can be applied without an excessive demand on licensee resources.

The peer reviewers and others identified several actions that will increase the effectiveness and efficiency of ATHEANA. These actions include the following:

- developing a computer-based user support system to guide the process and the documentation of the results,

- refining the prioritization process to facilitate identification of the types of scenarios and situations most likely to create problems,

- developing better guidance on when and how to develop and use simulator exercises to learn as much as possible about where and how unsafe actions can occur, and

- producing a "quick reference guide" that would allow analysts to bypass reliance on the NUREG document once they have some experience with the method.

Another issue raised by the peer reviewers concerns consistency in the application of the process and the potential for significant variability in results because of some of the "open-ended" aspects of ATHEANA, (for example, the creative thinking and brainstorming aspects of the process for identifying EFCs and the use of expert judgment in the quantification process). The ATHEANA team agrees that additional guidance is needed to ensure consistency in the results obtained using the method.

Finally, it should noted that reviewers of the method suggested that the documentation provide estimates of the costs and resources required to perform ATHEANA and that criteria should be provided for when ATHEANA should be used. While the former suggestion may be difficult to implement until additional tests of ATHEANA are completed, it is a reasonable suggestion. Providing a listing of criteria for when use of ATHEANA is called for would seem to be straightforward and will be considered for the revision.

Other Useful Suggestions

Several other comments received from the peer review team are worth noting because they are good suggestions that would improve ATHEANA. They include the following:

- ATHEANA should include an overview of PRA for participants without a background in PRA. Any training programs developed for ATHEANA could also provide such an overview, and aspects of PRA could be treated in more detail as the analysis progressed.

- It was recommended that a single "running" example be used while discussing the implementation process.

- It was recommended that additional examples for BWRs should be added. PWRs are overemphasized.

Conclusion

Taken together, the comments from the peer review team indicate that the work performed in the development of ATHEANA has resulted in significant contributions to the field of HRA and that ATHEANA is a viable HRA method. However, the reviewers also indicated that there were important clarifications and improvements that needed to be made to ATHEANA. Clearly, many of the recommendations made by the reviewers would, if implemented, make ATHEANA a better,

more effective, easier to use, and more "encompassing" methodology. However, a number of factors must be considered in determining which of the suggested changes are necessary, which would be useful but are not critical, and which would be useful but are currently impossible. The development of an HRA method such as ATHEANA is certainly limited by the state of current knowledge in a number of domains such as cognitive psychology, crew dynamics, and management and organizational factors. In addition, the unavailability of actual data from crew performance in nuclear power accidents or from other domains that might be generalized to control room performance certainly limits the ability of any HRA method to precisely predict performance. Other factors include the danger of over-complicating the method in attempts to be more precise and complete. It seems to the ATHEANA team that the most important goal is to provide a usable method that is as cost-effective as possible -- one that will allow analysts to identify, understand as much as possible, and quantify as accurately as possible, potential unsafe human actions that could lead to serious accidents in nuclear power plants or other domains. The explicit procedures, information, and guidance provided in ATHEANA certainly provides HRA analysts with a new and explicit set of tools to achieve this goal. To the extent viable changes recommended by the reviewers will further this goal, in particular by making the method more valid and easier to use, attempts will be made to incorporate them into the ATHEANA methodology.

References

1. U.S. Nuclear Regulatory Commission, *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis, Draft Report for Comment* , NUREG-1624, Washington, DC, May 1998.

2. S. E. Cooper, W. J. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report No. L2415/95-1, Brookhaven National Laboratory, Upton, NY, December 1995.

3. J. C. Williams, "A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance," 1988 IEEE Fourth Conference on Human Factors and Power Plants, Monterey, California, IEEE, 1988.

4. D. E. Embrey, et al., "Slim-Maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment," Vols. 1-2, NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, D.C., March 1984

5. Swain, A.D., and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque, NM, August 1983.

APPENDIX G
GLOSSARY OF GENERAL TERMS FOR ATHEANA

GLOSSARY OF GENERAL TERMS FOR ATHEANA

Availability Heuristic : The tendency of individuals to base interpretations or judgements on the ease with which relevant information can be recalled or with which relevant instances or occurrences can be imagined. Availability can be influenced by factors such as the recency and salience of the individual's own experiences.

Circumvention: A deliberate, deviation from rules and practices that has the intention of maintaining safe and/or efficient operations.

Cognitive Activity: Cognitive activity is the thought process associated with the operator's (1) situation assessment, (2) monitoring and detection, (3) response planning, and (4) response implementation.

Cognitive Factors: Cognitive factors affect the quality of output of major cognitive activities and therefore, affect operator performance. Three classes of cognitive factors are knowledge, processing resource, and strategic factors. Errors arise when there is a mismatch between the state of these cognitive factors and the demands imposed by the situation.

Confirmation Bias: The tendency of individuals to seek or interpret indications in ways that confirm expectations. The result can be a failure to appropriately revise opinions or interpretations in light of new, conflicting information.

Error-Forcing Context (EFC): The situation that arises when particular combinations of *performance shaping factors* and *plant conditions* create an environment in which unsafe actions are more likely to occur.

Error of Commission (EOC): A *human failure event* resulting from an overt, unsafe action, that, when taken, leads to a change in plant configuration with the consequence of a degraded plant state. Examples include terminating running safety-injection pumps, closing valves, and blocking automatic initiation signals.

Error of Omission (EOO): A *human failure event* resulting from a failure to take a required action, that leads to an unchanged or inappropriately changed plant configuration with the consequence of a degraded plant state. Examples include failures to initiate standby liquid control system, to start auxiliary feedwater equipment, and to block automatic depressurization system signals.

Error Mechanism (of humans): A psychological mechanism that can cause a particular *unsafe action* and is triggered by particular combinations of *performance-shaping* factors and *plant conditions*. Error mechanisms are often not inherently bad behaviors, but represent mechanisms by which people often efficiently perform skilled work. However, in the wrong context, these mechanisms may lead to inappropriate human actions that have unsafe consequences.

Expectation Bias: The tendency for people to give more significance to information that confirms their beliefs than to information that contradicts their beliefs.

Frequency Bias: Frequently occurring events are often recalled more easily than scarce events. This can lead to a tendency in people to interpret in-coming information about an event in terms of events that occur frequently, rather than infrequently occurring or unlikely events.

Fixation Error: A failure to appropriately revise the assessment of a situation as new evidence is introduced.

Human Error: In the PRA community, the term 'human error' has often been used to refer to human-caused failures of a system or component. However, in the behavioral sciences, the same term is often used to describe the underlying psychological failures that may cause the human action that fails the equipment. Therefore, in ATHEANA, the term 'human error' is only used in a very general way, with the terms *human failure event*, *unsafe action*, and *error mechanism* being used to describe more specific aspects of human errors.

Human Failure Event (HFE): A basic event that is modeled in the logic models of a PRA (event and fault trees), and that represents a failure of a function, system, or component that is the result of one or more *unsafe actions*. A human failure event reflects the PRA systems' modeling perspective.

Information Processing Model: A general description of the range of human cognitive activities required to respond to abnormal or emergency conditions. The model used in ATHEANA considers actions in response to abnormalities as involving four steps (1) monitoring/detection, (2) situation assessment, (3) response planning, and (4) response implementation.

Mental Model: Mental representations that integrate a person's understanding of how systems and plants work. A mental model enables a person to mentally simulate plant and system performance in order to predict or anticipate plant and equipment behavior.

Monitoring/Detection: The activities involved in extracting information from the environment. Monitoring is checking the state of the plant to determine whether the systems are operating correctly. Detection, in this context, refers to the operator becoming aware that an abnormality exists.

Performance Shaping Factors (PSFs): A set of influences on the performance of an operating crew resulting from the human-related characteristics of the plant, the crew, and the individual operators. The characteristics include procedures, training, and human-factors aspects of the displays and control facilities of the plant.

Plant Conditions: The plant state defined by combinations of its physical properties and equipment conditions, including the measurement of parameters.

Polarization of Thinking: The tendency to attribute events to one global cause instead of a combination of causes.

Primacy Bias/Effects: The tendency in people to give more significance to the data they first see (and may draw conclusions from) than to later data. When judgments or decisions are required, initial information is sometimes more easily recalled than later occurring information.

Probabilistic Risk Assessment/Analysis (PRA): PRA of a nuclear power plant is an analytical process that quantifies the potential risk associated with the design, operation, and maintenance of a plant to the health and safety of the public.

PRA Model: The PRA model is a logic model which generally consist of event trees, fault trees and other analytical tools and is constructed to identify the scenarios that lead to unacceptable plant accident conditions, such as core damage. The model is used to estimate the frequencies of the scenarios by converting the logic model into a probability model. To achieve this aim, estimates must be obtained for the probabilities of each event in the model, including HFEs.

Recency Bias/Effects: Events that happened recently are recalled more easily than events that occurred a long time ago. In attempting to understand in-coming information about an event, people tend to interpret the information in terms of events that have happened recently, rather than relevant events that occurred in the more distant past.

Representativeness Heuristic: The tendency to misinterpret an event because it resembles a "classic event" which was important in past experience or training, or because there is a high degree of similarity between the past event and the evidence examined so far.

Response Implementation: Taking the specific control actions required to perform a task, in accordance with *response planning*. Response implementation may involve taking discreet actions (e.g., flipping a switch) or it may involve continuous control activity (e.g., controlling the steam generator level). It may be performed by a single person, or it may require communication and coordination among multiple individuals.

Response Planning: Deciding on a course of action, given a particular *situation model*. In general, response planning involves identifying plant-state goals, generating one or more alternative response plans, evaluating the response plans, and selecting the response plan that best meets the goals identified.

Rules: Rules are the guidance operators follow in carrying out activities in the plant. Rules can be either formal or informal in nature. *Formal rules* are specific written instructions and requirements provided to operators and authorized for use by plant management. *Informal rules* sources include training programs, discussions among operators, experience, and past practices.

Salience Bias: The tendency to give closer attention or to weight more heavily information or indications that are more prominent, (e.g., the most visible, the loudest, or the most "compelling" instrument displays.)

Satisfying: The tendency in people (under some circumstances) to stop looking for a solution when an acceptable, but not necessarily optimal one, is found.

Scenario Definition: PRA *scenario definitions* provide the minimum descriptions of plant state required to develop the PRA model and define appropriate HFEs. Examples of scenario definition elements include the initiating event, operating mode, decay heat level (for shutdown PRAs), and function/system/component status or configuration. The level of detail to which scenarios are defined can vary and include the functional level, system level, and component state level.

Simplifying: People tend to disregard complex aspects of data, e.g., interaction effects, and give more significance to aspects of the data they understand. This is analogous to searching for a lost item under the lamppost because that is where the light is.

Situation Assessment: Situation assessment involves developing and updating a mental representation of the factors known, or thought to be affecting the plant state, at a given point in time. The mental representation resulting from situation assessment is referred to as a situation model.

Situation Model: A mental representation of the current plant condition, and the factors thought to be affecting the plant state resulting from the operators' situation assessment. The situation model is created by an interpretation of operational data in light of the operator's mental model. (An operator's situation model is usually updated constantly as new information is received; failure to update a situation model to incorporate new information is an error mechanism).

Tunnel Vision: The tendency in people to concentrate only on the information that is related to their prevailing hypothesis, neglecting other important information

Unsafe Action (UA): Actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-1624, Rev. 1

2. TITLE AND SUBTITLE

Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)

3. DATE REPORT PUBLISHED

MONTH	YEAR
May	2000

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Division of Risk Analysis & Applications
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Same as above

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

This report introduces a next-generation HRA method called "A Technique for Human Event Analysis," (ATHEANA). ATHEANA was developed to address limitations identified in current HRA approaches by: (1) addressing errors of commission and dependencies; (2) more realistically representing the human-system interactions that have played important roles in accident response; and (3) integrating advances in psychology with engineering, human factors, and PRA disciplines.

This report is the step-by-step guidebook for applying the method. It describes how to:

1. select and organize the ATHEANA team,
2. perform and control the structured search processes for human failure events and unsafe acts, including a discussion of the reasons that such events occur (i.e., the elements of error-forcing context),
3. use the knowledge encoded in the PRA along with the specialized knowledge and experience of the ATHEANA team to focus the searches on those events and reasons that are most likely to affect the risk, and
4. quantify the error-forcing contexts and probability of each unsafe act, given its context.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

probabilistic risk assessment
human reliability analysis
severe accident

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)

unclassified

(This Report)

unclassified

15. NUMBER OF PAGES

16. PRICE