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).
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

v  NUREG-1624, Rev. 1
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>BEHAVIORAL SCIENCE PERSPECTIVE</td>
<td>4-1</td>
</tr>
<tr>
<td>4.1</td>
<td>Analysis of Operator Cognitive Performance</td>
<td>4-1</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Situation Assessment</td>
<td>4-1</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Monitoring and Detection</td>
<td>4-4</td>
</tr>
<tr>
<td>4.1.3</td>
<td>Response Planning</td>
<td>4-5</td>
</tr>
<tr>
<td>4.1.4</td>
<td>Response Implementation</td>
<td>4-6</td>
</tr>
<tr>
<td>4.2</td>
<td>Cognitive Factors Affecting Operator Performance</td>
<td>4-6</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Knowledge Factors</td>
<td>4-7</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Processing Resource Factors</td>
<td>4-7</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Strategic Factors</td>
<td>4-9</td>
</tr>
<tr>
<td>4.3</td>
<td>Failures in Operator Cognitive Activity</td>
<td>4-10</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Failures in Monitoring or Detection</td>
<td>4-10</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Failures in Situation Assessment</td>
<td>4-11</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Failures in Response Planning</td>
<td>4-14</td>
</tr>
<tr>
<td>4.3.4</td>
<td>Failures in Response Implementation</td>
<td>4-17</td>
</tr>
<tr>
<td>4.4</td>
<td>Contributing Elements of Error-Forcing Contexts in Power-Plant Operations</td>
<td>4-17</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Characteristics of Parameters and Scenarios</td>
<td>4-18</td>
</tr>
<tr>
<td>4.4.1.1</td>
<td>Parametric Influences</td>
<td>4-19</td>
</tr>
<tr>
<td>4.4.1.2</td>
<td>Scenario Influences</td>
<td>4-20</td>
</tr>
<tr>
<td>4.5</td>
<td>Conclusions</td>
<td>4-20</td>
</tr>
<tr>
<td>4.6</td>
<td>References</td>
<td>4-21</td>
</tr>
<tr>
<td>4.7</td>
<td>Bibliography of Cognitive Psychology Literature Relevant to ATHEANA</td>
<td>4-22</td>
</tr>
<tr>
<td>5</td>
<td>OPERATIONAL EXPERIENCE ILLUSTRATING ATHEANA PRINCIPLES</td>
<td>5-1</td>
</tr>
<tr>
<td>5.1</td>
<td>Contributions of Humans and Error-Forcing Contexts in Past Operational Experience</td>
<td>5-2</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Plant Conditions and PSFs</td>
<td>5-2</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Failures in Information Processing Stages</td>
<td>5-3</td>
</tr>
<tr>
<td>5.2</td>
<td>Analysis of Error-Forcing Context</td>
<td>5-4</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Error-Forcing Context and Unsafe Actions</td>
<td>5-5</td>
</tr>
<tr>
<td>5.2.1.1</td>
<td>Error-Forcing Context in Detection</td>
<td>5-5</td>
</tr>
<tr>
<td>5.2.1.2</td>
<td>Error-Forcing Context in Situation Assessment</td>
<td>5-6</td>
</tr>
<tr>
<td>5.2.1.3</td>
<td>Error-Forcing Context in Response Planning</td>
<td>5-10</td>
</tr>
<tr>
<td>5.2.1.4</td>
<td>Error-Forcing Context in Response Implementation</td>
<td>5-12</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Performance-Shaping Factors</td>
<td>5-12</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Important Lessons from Analyses of Events</td>
<td>5-14</td>
</tr>
<tr>
<td>5.3</td>
<td>An Operational Event Example Illustrating Dependency Effects</td>
<td>5-21</td>
</tr>
<tr>
<td>5.4</td>
<td>Summary</td>
<td>5-27</td>
</tr>
<tr>
<td>5.5</td>
<td>References</td>
<td>5-27</td>
</tr>
</tbody>
</table>
# 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

NUREG-1624, Rev. 1  v
viii
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
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Multidisciplinary HRA Framework</td>
<td>2-2</td>
</tr>
<tr>
<td>4.1</td>
<td>Major Cognitive Activities Underlying NPP Operator Performance</td>
<td>4-2</td>
</tr>
<tr>
<td>5.1</td>
<td>Oconee 3 Loss of Cooling</td>
<td>5-23</td>
</tr>
<tr>
<td>5.2a</td>
<td>Event Information</td>
<td>5-24</td>
</tr>
<tr>
<td>5.2b</td>
<td>Summary of Human Actions</td>
<td>5-25</td>
</tr>
<tr>
<td>5.2c</td>
<td>Event Dependencies</td>
<td>5-26</td>
</tr>
<tr>
<td>6.1</td>
<td>ATHEANA Prospective Search Process</td>
<td>6-4</td>
</tr>
<tr>
<td>8.1</td>
<td>TMI-2 Represented in ATHEANA Framework</td>
<td>8-2</td>
</tr>
<tr>
<td>8.2</td>
<td>Crystal River Unit 1 Represented in ATHEANA Framework</td>
<td>8-6</td>
</tr>
<tr>
<td>9.1a</td>
<td>Key for the Meaning of the Box Shapes in Figures 9.1 - 9.6</td>
<td>9-3</td>
</tr>
<tr>
<td>9.2</td>
<td>Step 2 - Describe the Scope of the Analysis</td>
<td>9-6</td>
</tr>
<tr>
<td>9.3</td>
<td>Step 3 - Describe Base Case Scenario</td>
<td>9-15</td>
</tr>
<tr>
<td>9.4</td>
<td>Step 5 - Identify Potential Vulnerabilities</td>
<td>9-35</td>
</tr>
<tr>
<td>9.5</td>
<td>Step 6 - Search for Deviations from Base Case Scenario</td>
<td>9-48</td>
</tr>
<tr>
<td>9.6</td>
<td>Step 7 - Evaluate Complicating Factors</td>
<td>9-60</td>
</tr>
<tr>
<td>10.1</td>
<td>Representation of Estimation of UA Probability</td>
<td>10-10</td>
</tr>
<tr>
<td>10.2</td>
<td>Overview of PRA Modeling</td>
<td>10-20</td>
</tr>
<tr>
<td>10.3</td>
<td>Overview of PRA Modeling with HFE Interfaces Shown</td>
<td>10-20</td>
</tr>
<tr>
<td>10.4</td>
<td>Illustration of HFEs in Event Trees</td>
<td>10-21</td>
</tr>
<tr>
<td>10.5</td>
<td>Illustration of HFEs in Fault Trees</td>
<td>10-21</td>
</tr>
<tr>
<td>10.6</td>
<td>Illustration of Failure-to-Recover Events in Cut Sets</td>
<td>10-23</td>
</tr>
<tr>
<td>10.7</td>
<td>Illustration of Incorporating an ATHEANA HFE in an Event Tree</td>
<td>10-25</td>
</tr>
<tr>
<td>B.1</td>
<td>Large LOCA Event Tree</td>
<td>B-3</td>
</tr>
<tr>
<td>B.2</td>
<td>Loss of Main Feedwater Event Tree</td>
<td>B-3</td>
</tr>
<tr>
<td>B.3</td>
<td>$T_{avg}$ During Loss of Main Feed</td>
<td>B-7</td>
</tr>
<tr>
<td>B.4</td>
<td>Pressurizer Volume During Loss of Main Feed</td>
<td>B-7</td>
</tr>
<tr>
<td>B.5</td>
<td>Steam Generator Water Level During Loss of Main Feed</td>
<td>B-7</td>
</tr>
<tr>
<td>B.6</td>
<td>Power Level vs. Time</td>
<td>B-9</td>
</tr>
<tr>
<td>B.7</td>
<td>Turbine Pressure vs. Time</td>
<td>B-9</td>
</tr>
<tr>
<td>B.8</td>
<td>Instrument Air Pressure vs. Time</td>
<td>B-9</td>
</tr>
<tr>
<td>B.9</td>
<td>Service Water Pressure vs. Time</td>
<td>B-9</td>
</tr>
<tr>
<td>B.10</td>
<td>RCS Conditions vs. Time</td>
<td>B-10</td>
</tr>
<tr>
<td>B.11</td>
<td>Steam Generator Status vs. Time</td>
<td>B-10</td>
</tr>
<tr>
<td>B.12</td>
<td>Containment Conditions vs. Time</td>
<td>B-10</td>
</tr>
<tr>
<td>B.13</td>
<td>EOP Highlights Related to Loss of Main Feed Scenario</td>
<td>B-17</td>
</tr>
<tr>
<td>B.14a</td>
<td>RCS Response vs. Time</td>
<td>B-34</td>
</tr>
<tr>
<td>B.14b</td>
<td>SG Response vs. Time</td>
<td>B-34</td>
</tr>
<tr>
<td>B-15</td>
<td>Plant Status After HFE Occurs</td>
<td>B-41</td>
</tr>
<tr>
<td>C.1</td>
<td>Core Power during LLOCA Reference Case</td>
<td>C-4</td>
</tr>
<tr>
<td>C.2</td>
<td>Break Flow Rate during LLOCA Reference Case</td>
<td>C-4</td>
</tr>
</tbody>
</table>
## List of Figures (Cont.)

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

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Examples of Detection Failures</td>
</tr>
<tr>
<td>5.2</td>
<td>Examples of Situation Assessment Failures</td>
</tr>
<tr>
<td>5.3</td>
<td>Examples of Response Planning Failures</td>
</tr>
<tr>
<td>5.4</td>
<td>Examples of Response Implementation Failures</td>
</tr>
<tr>
<td>5.5</td>
<td>Examples of PSFs on Cognitive and Physical Abilities</td>
</tr>
<tr>
<td>5.6</td>
<td>Characteristics of Serious Accidents and Event Precursors</td>
</tr>
<tr>
<td>5.7</td>
<td>Factors Not Normally Considered in PRAs</td>
</tr>
<tr>
<td>9.1</td>
<td>Generic List of Initiating Event Classes and Associated Initiators</td>
</tr>
<tr>
<td>9.2</td>
<td>ATHEANA-Suggested Characteristics of High-Priority Initiators or Accident Sequences</td>
</tr>
<tr>
<td>9.3</td>
<td>ATHEANA-Suggested Characteristics of High-Priority Systems and Functions</td>
</tr>
<tr>
<td>9.4</td>
<td>Development of the Base Case Scenario</td>
</tr>
<tr>
<td>9.5</td>
<td>Examples of Base Case Scenario Development</td>
</tr>
<tr>
<td>9.6</td>
<td>Functional Failure Modes Based upon PRA Requirements</td>
</tr>
<tr>
<td>9.7</td>
<td>Examples of Likely Human Failures and Human Failure Modes by PRA Functional Failure Mode</td>
</tr>
<tr>
<td>9.8</td>
<td>Example Unsafe Actions for Generalized Equipment Functional Failure Modes</td>
</tr>
<tr>
<td>9.9a</td>
<td>Possible EOCs for Systems or Equipment that Automatically Start or Stop</td>
</tr>
<tr>
<td>9.9b</td>
<td>Possible EOCs for Continuation of Operation or No Operation of Systems and Equipment</td>
</tr>
<tr>
<td>9.9c</td>
<td>Possible EOCs or EOOs for Manual Actuation and Control of Systems and Equipment</td>
</tr>
<tr>
<td>9.9d</td>
<td>Possible EOOs for Backup (i.e., Recovery) of Failed Systems and Equipment</td>
</tr>
<tr>
<td>9.9e</td>
<td>Possible EOCs or EOOs for Failures of Passive Systems and Components</td>
</tr>
<tr>
<td>9.10</td>
<td>Event Characteristics and Potential Vulnerabilities</td>
</tr>
<tr>
<td>9.11</td>
<td>Relevant Time Frames for the Examples of Appendices B and C</td>
</tr>
<tr>
<td>9.12a</td>
<td>Summary of Operator Action Tendencies (PWRs)</td>
</tr>
<tr>
<td>9.12b</td>
<td>Summary of Operator Action Tendencies (BWRs)</td>
</tr>
<tr>
<td>9.13</td>
<td>Examples of Informal “Rules” Used by Operators</td>
</tr>
<tr>
<td>9.14</td>
<td>Failures in Response Implementation</td>
</tr>
<tr>
<td>9.15a</td>
<td>Scenario Characteristics and Description</td>
</tr>
<tr>
<td>9.15b</td>
<td>Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors</td>
</tr>
<tr>
<td>9.16a</td>
<td>Questions to Identify Scenario Relevant Parameter Characteristics (Table to be used with Table 9.16b)</td>
</tr>
<tr>
<td>9.16b</td>
<td>Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Table to be used following Table 9.16a)</td>
</tr>
<tr>
<td>9.17</td>
<td>Examples of Hardware Failures, Configuration Problems, or Unavailabilities</td>
</tr>
<tr>
<td>9.18</td>
<td>Examples of Information (i.e., Transmit) Problems</td>
</tr>
<tr>
<td>9.19</td>
<td>Physics Algorithms in Instruments that Can Confuse Operators</td>
</tr>
</tbody>
</table>
List of Tables (Cont.)

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

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 (AEOE) 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.

NUREG-1624, Rev. 1 xvi
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...
Executive Summary

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.
Executive Summary

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
Executive Summary

- 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.
Executive Summary

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.
Executive Summary

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

¹This 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
1. Introduction

- 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.
1. Introduction

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.
1. Introduction

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
1. Introduction

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
1. Introduction

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.
1. Introduction

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.
1. Introduction

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
1. Introduction

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.
1. Introduction

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, accessibility).

- **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. Introduction

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
1. Introduction

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. Introduction


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)
2. General Description of ATHEANA

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.

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...
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.
2. General Description of ATHEANA

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. General Description of ATHEANA

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
2. General Description of ATHEANA

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.
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
2. General Description of ATHEANA

- 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


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. The Importance of Plant Conditions & Context

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
The importance of plant conditions & context

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.
3. The Importance of Plant Conditions & Context

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
3. The Importance of Plant Conditions & Context

(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
The Importance of Plant Conditions & Context

rods to increase power. They expected that increasing RCS temperature would create an
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. The Importance of Plant Conditions & Context

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. The Importance of Plant Conditions & Context


3. The Importance of Plant Conditions & Context


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.
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
4. Behavioral Science Perspective

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.
4. Behavioral Science Perspective

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. Behavioral Science Perspective

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...
4. Behavioral Science Perspective

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. Behavioral Science Perspective

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
4. Behavioral Science Perspective

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)
4. Behavioral Science Perspective

- 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"
4. Behavioral Science Perspective

(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
4. Behavioral Science Perspective

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
4. Behavioral Science Perspective

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
4. Behavioral Science Perspective

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. Behavioral Science Perspective

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,
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. Behavioral Science Perspective

4.4.1.2 Scenario Influences

Woods, Roth, Mumaw, and their colleagues (Ref. 4.3, 4.4, 4.8, 4.9)\textsuperscript{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).

\textsuperscript{2}See Footnote 1, page 4-18.
4. Behavioral Science Perspective

4.6 References


4. Behavioral Science Perspective

4.7 Bibliography of Cognitive Psychology Literature Relevant to ATHEANA

General Treatment of the Cognitive Basis for Human Error


Related Works on the Concepts Discussed in this Section


4. Behavioral Science Perspective


4. Behavioral Science Perspective


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
5. Operational Experience Illustrating ATHEANA Principles

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
5. Operational Experience Illustrating ATHEANA Principles

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. Operational Experience Illustrating ATHEANA Principles

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.
5. Operational Experience Illustrating ATHEANA Principles

Table 5.1 Examples of Detection Failures

<table>
<thead>
<tr>
<th>Detection failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators unaware of actual plant state, its severity, and continued degradation in conditions.</td>
<td>(1) Reactor vessel (RV) level instrumentation failed high off-scale as a result of unusual plant conditions (i.e., high N₂ overpressure).</td>
<td>Prairie Island 2 (2/20/92), loss of reactor coolant system (RCS) inventory and shut-down cooling during shutdown.</td>
</tr>
<tr>
<td></td>
<td>(2) Redundant RV level instrumentation readings required correction through hand calculations (and were performed incorrectly).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3) Procedures did not specifically address the high N₂ 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 N₂ overpressure or what the overpressure should be at various points during the draindown (some decreasing trend in overpressure was implied).</td>
<td></td>
</tr>
</tbody>
</table>

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 N₂ 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

<table>
<thead>
<tr>
<th>Situation Assessment Failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators develop wrong situation model (or cannot explain) plant state and behavior.</td>
<td>(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.</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(1) Computer displays normally used for containment temperature and RCS subcooling parameters were malfunctioning and operators had difficulty obtaining required information.</td>
<td>Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td>Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown.</td>
</tr>
<tr>
<td>Operators unable to distinguish between results of their own actions and accident progression.</td>
<td>(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).</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
</tbody>
</table>
### 5. Operational Experience Illustrating ATHEANA Principles

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

<table>
<thead>
<tr>
<th>Situation Assessment Failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators unable to distinguish between results of their own actions and accident progression.</td>
<td>(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)</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td>Operators misinterpret information or are misled by wrong information, confirming their wrong situation model.</td>
<td>(1) Erroneous report from technicians that one bank of PRZR heaters are at 0% power.</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
<tr>
<td></td>
<td>(2) Cycling of switch for PRZR spray valve did not terminate the transient (because valve was broken).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(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)</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(1) High-level alarm from reactor building normal sump (interpreted as being the result of washdown operations).</td>
<td>Oconee 3 (3/8/91), loss of RCS and shut-down cooling during shutdown.</td>
</tr>
<tr>
<td>Operators reject evidence that contradicts their wrong situation model.</td>
<td>(1) Strip chart recorders showed PRZR level increasing (which is inconsistent with RCS overcooling and associated inventory shrinkage), but were not monitored.</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
<tr>
<td></td>
<td>(2) Recollection of information passed during shift turnover concerning a problem with PRZR spray valve indication discounted because of unsuccessful valve cycling.</td>
<td></td>
</tr>
<tr>
<td>Operators reject evidence that contradicts their wrong situation model.</td>
<td>(1) Indication of increased SRV tailpipe temperature (310°F). (^b)</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(2) Back panel acoustic monitor showed red open light. (^b)</td>
<td></td>
</tr>
<tr>
<td>Operators reject evidence that contradicts their wrong situation model.</td>
<td>(1) Reactor vessel level reading at 20 inches and decreasing. (Erroneous operation of the RV wide-range level transmitter suspected.)</td>
<td>Oconee 3 (3/8/91), loss of RCS and shut-down cooling during shutdown.</td>
</tr>
<tr>
<td></td>
<td>(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.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(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.)</td>
<td></td>
</tr>
</tbody>
</table>
5. Operational Experience Illustrating ATHEANA Principles

Table 5.2 Examples of Situation Assessment Failures (Cont.)

<table>
<thead>
<tr>
<th>Situation Assessment Failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators reject evidence that contradicts their wrong situation model.</td>
<td>(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.</td>
<td>Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown.</td>
</tr>
</tbody>
</table>

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.

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.

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)
5. Operational Experience Illustrating ATHEANA Principles

- 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 N₂ 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

<table>
<thead>
<tr>
<th>Response Planning Failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators follow prepared plans (e.g., procedures), but these plans direct operators to take actions that are inappropriate for specific situation.</td>
<td>(1) Draindown procedure assumed a lower $N_2$ overpressure; therefore RV level conversion calculations, time for draindown, etc., were different than assumed in procedure.</td>
<td>Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.</td>
</tr>
<tr>
<td>Operators follow prepared plans (e.g., procedures), but these plans are wrong and/or incomplete (resulting in inappropriate actions).</td>
<td>(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.)</td>
<td>Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td>Operators do not explicitly use prepared plans (e.g., procedures) and take actions that are inappropriate.</td>
<td>(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.</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
<tr>
<td>Operators forced into knowledge-based (wrong) actions because prepared plans (e.g., procedures) are incomplete or do not exist.</td>
<td>(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).</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
</tbody>
</table>
5. Operational Experience Illustrating ATHEANA Principles

Table 5.3 Examples of Response Planning Failures (Cont.)

<table>
<thead>
<tr>
<th>Response Planning Failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators give priority to one accident response goal (or safety function) at the expense of another or disregard the importance of the safety function.</td>
<td>(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).</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
<tr>
<td>(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).</td>
<td></td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td>(2) Operators were generally unconcerned with the RPV cooldown rate because they assumed the technical specification cooldown rate limit would have been exceeded anyway.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
5. Operational Experience Illustrating ATHEANA Principles

Table 5.4 Examples of Response Implementation Failures

<table>
<thead>
<tr>
<th>Response Implementation Failure</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators do not check all applicable sections of procedure before exiting results in omission of important actions.</td>
<td>(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.</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during startup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miscommunication results in inappropriate or less than optimal actions.</td>
<td>(1) Suppression pool cooling was not initially maximized, as required by procedure.</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td></td>
</tr>
<tr>
<td>Equipment problems hinder operators' ability to respond to event.</td>
<td>(1) Failure of the safety valve created LOCA from the PRZR that could not be isolated.</td>
<td>Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td></td>
</tr>
</tbody>
</table>

- 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
5. Operational Experience Illustrating ATHEANA Principles

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

<table>
<thead>
<tr>
<th>PSF*</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human performance capabilities at a low point (environmental conditions).</td>
<td>(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 abilities more than skill- or rule-based activities.)</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during start-up.</td>
</tr>
<tr>
<td></td>
<td>(1) Event occurred at 1:05 a.m.</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(1) Event occurred at 11:35 p.m.</td>
<td>Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(2) Event occurred at the beginning of the shift, when awareness is typically high.</td>
<td>Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.</td>
</tr>
<tr>
<td>Human performance negatively affected by time constraints (stress).</td>
<td>(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.</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during start-up.</td>
</tr>
<tr>
<td>Aspect of the plant or its operation is new and unfamiliar to operators (training).</td>
<td>(1) First time electronic reactor vessel level instrumentation was used- its operation and design are not understood.</td>
<td>Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.</td>
</tr>
<tr>
<td></td>
<td>(2) First time draindown was performed with such a high N₂ overpressure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3) First time draindown was performed without experienced SE to support draindown operators.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(4) Decay heat high (~6 MW) because only 2 days after shutdown.</td>
<td></td>
</tr>
<tr>
<td>Operators inexperienced (training, procedures).</td>
<td>(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).</td>
<td>Crystal River 3 (12/8/91), RCS pressure transient during start-up.</td>
</tr>
<tr>
<td></td>
<td>(1) Operators and assisting system engineer performing draindown were inexperienced.</td>
<td>Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.</td>
</tr>
</tbody>
</table>
### Table 5.5 Examples of PSFs on Cognitive and Physical Abilities (Cont.)

<table>
<thead>
<tr>
<th>PSF</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excessive workload interferes with operators ability to perform (organizational factors).</td>
<td>(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.</td>
<td>Dresden 2 (8/2/90), LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(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.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td>Ft. Calhoun (7/3/92), inverter failure followed by LOCA (stuck-open relief valve).</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
<td>Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown.</td>
</tr>
</tbody>
</table>
### Table 5.5 Examples of PSFs on Cognitive and Physical Abilities (Cont.)

<table>
<thead>
<tr>
<th>PSF</th>
<th>Contextual Influences</th>
<th>Event</th>
</tr>
</thead>
</table>
| 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.
5. Operational Experience Illustrating ATHEANA Principles

Table 5.6 Characteristics of Serious Accidents and Event Precursors

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Extreme and/or unusual conditions</td>
<td>Seasonal grass intrusions in Salem 1 event, earthquakes, unusual plant configurations, high nitrogen pressure during shutdown at Prairie Island 2.</td>
</tr>
<tr>
<td>(2) Preexisting conditions that complicate response, diagnosis, etc.</td>
<td>Failed auxiliary feedwater (AFW) system in TMI-2, instruments miscalibrated, etc.</td>
</tr>
<tr>
<td>(3) Misleading or wrong information</td>
<td>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.</td>
</tr>
<tr>
<td>(4) Information rejected or ignored</td>
<td>Core exit thermocouples in TMI-2, sump level alarms in Oconee 3 shutdown event, multiple evolutions whose effects cannot be separated.</td>
</tr>
<tr>
<td>(5) Multiple hardware failures</td>
<td>Davis Besse loss of feedwater event, TMI-2.</td>
</tr>
<tr>
<td>(6) Transitions in progress</td>
<td>Prairie Island 2 shutdown event—draining down; Crystal River 3—startup.</td>
</tr>
<tr>
<td>(7) Symptoms similar to frequent and/or salient events</td>
<td>Symptoms of going “solid” in TMI-2.</td>
</tr>
</tbody>
</table>
## Table 5.7 Factors Not Normally Considered in PRAs

<table>
<thead>
<tr>
<th>Factors</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Instrumentation fails (or is caused to be failed) and fails in many ways</td>
<td>• indication is high, low, lagging, stuck, or miscalibrated</td>
</tr>
<tr>
<td></td>
<td>• preaccident failures (human and hardware-caused)</td>
</tr>
<tr>
<td></td>
<td>• unavailable because of maintenance, testing, etc.</td>
</tr>
<tr>
<td></td>
<td>• does not exist</td>
</tr>
<tr>
<td>(2) Instrumentation problems that cause operators to not use the instruments</td>
<td>• recent or persistent history of reliability and availability problems</td>
</tr>
<tr>
<td></td>
<td>• inconsistent with other indications and/or initial operator diagnosis of plant status and behavior</td>
</tr>
<tr>
<td></td>
<td>• lack of redundant instrumentation to confirm information</td>
</tr>
<tr>
<td></td>
<td>• not conveniently located</td>
</tr>
<tr>
<td></td>
<td>• redundant, backup indicator that is not typically used</td>
</tr>
<tr>
<td>(3) The instrumentation used by operators is not necessarily all that is available to them or what designers expect them to use.</td>
<td>• 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]</td>
</tr>
<tr>
<td></td>
<td>• 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]</td>
</tr>
<tr>
<td></td>
<td>• indicators used outside their operating ranges (e.g., reactor vessel level indicators during midloop operations at shutdown [Prairie Island 2 (2/20/92)])</td>
</tr>
<tr>
<td>(4) Operators typically will believe valve position indicators in spite of contradictory indications.</td>
<td>• 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)]</td>
</tr>
<tr>
<td></td>
<td>• RCS drain path through an open RHR valve (which was being locally stroke-tested) during shutdown [Oconee 3, (3/8/91)]</td>
</tr>
<tr>
<td>(5) Operators can misunderstand how instrumentation &amp; control (I&amp;C) systems work, resulting in erroneous explanations for their operation and indications.</td>
<td>• misunderstand the location of a sensor or what is sensed (e.g., valve stem position versus controller position)</td>
</tr>
<tr>
<td></td>
<td>• misunderstand how what is sensed is translated into an instrument reading (e.g., RVLJS system, PRZR pressure is not “real,” really an algorithm)</td>
</tr>
</tbody>
</table>
5. Operational Experience Illustrating ATHEANA Principles

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

<table>
<thead>
<tr>
<th>Factors</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>(6) A history of false or spurious or automatic actions will result in</td>
<td>• 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</td>
</tr>
<tr>
<td>operator conditioning to expect these events (especially when reinforced</td>
<td>• spurious main feedwater pump trips in Davis Besse loss of feedwater resulted in MFW being in manual control at the time of reactor trip</td>
</tr>
<tr>
<td>by management directives) thereby overriding the formal diagnosis</td>
<td></td>
</tr>
<tr>
<td>required for a real event.</td>
<td></td>
</tr>
<tr>
<td>(7) One plausible explanation can create a group mindset for an operating</td>
<td>• 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</td>
</tr>
<tr>
<td>crew.</td>
<td></td>
</tr>
<tr>
<td>(8) Operators will persist in the recovery of failed systems.</td>
<td>• the alternatives have negative consequences</td>
</tr>
<tr>
<td></td>
<td>• recovery is imminent (in the operators’ opinion)</td>
</tr>
<tr>
<td></td>
<td>• they were the cause of the system failure (i.e., recoverable failure)</td>
</tr>
<tr>
<td>(9) The recovery of slips may be complicated.</td>
<td>• Encounter unexpected I&amp;C resetting difficulties (problems starting AFW in the Davis-Besse loss of feedwater event)</td>
</tr>
<tr>
<td>(10) Management decisions regarding plant configurations can result in</td>
<td>• scheduling of maintenance and testing activities</td>
</tr>
<tr>
<td>defeated plant defenses and additional burdens on operators.</td>
<td>• on-line corrective maintenance and entering limiting condition for operation (LCO) statements in technical specifications</td>
</tr>
<tr>
<td></td>
<td>• special configurations or exceptions from technical specifications to address persistent hardware problems</td>
</tr>
<tr>
<td>(11) Multitrain (or “all-train”) maintenance has been performed.</td>
<td></td>
</tr>
<tr>
<td>(12) Systems do not always fail at T=0 in accident sequence (i.e.,</td>
<td></td>
</tr>
<tr>
<td>simultaneous with initiating event).</td>
<td></td>
</tr>
<tr>
<td>(13) Systems and components are not truly binary state.</td>
<td>• can experience a range of degraded conditions between optimal performance and catastrophic failure</td>
</tr>
</tbody>
</table>
5. Operational Experience Illustrating ATHEANA Principles

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

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

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
5. Operational Experience Illustrating ATHEANA Principles

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
5. Operational Experience Illustrating ATHEANA Principles

<table>
<thead>
<tr>
<th>Plant Name: Oconee 3</th>
<th>Event Date: 3/8/91</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type: Loss of RCS Inventory</td>
<td>Event Time: 08:48</td>
</tr>
<tr>
<td>Secondary Event: Loss of SDC</td>
<td>Plant Type: PWR/</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Initial Conditions</th>
<th>Accident Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Other Unit Status:</strong></td>
<td><strong>Other Unit Status:</strong></td>
</tr>
<tr>
<td>RCS Conditions:</td>
<td>RCS Conditions:</td>
</tr>
<tr>
<td>Power: Cold S/D</td>
<td>Power: Cold S/D</td>
</tr>
<tr>
<td>Temperature (°F): 94</td>
<td>Temperature (°F): 117</td>
</tr>
<tr>
<td>Pressure: (head off)</td>
<td>Pressure: (head off)</td>
</tr>
<tr>
<td>RV Level: 12 ft. above core (76 in. on wide RV wide-range level transmitter)</td>
<td>RV Level: 4 ft. above core</td>
</tr>
<tr>
<td>Other:</td>
<td>Other:</td>
</tr>
<tr>
<td>* 24th day of refueling outage</td>
<td>* Loss of 9,700 gal. of RCS</td>
</tr>
<tr>
<td>* Refueling complete</td>
<td></td>
</tr>
</tbody>
</table>

**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)

**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

**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

NUREG-1624, Rev. 1 5-24
5. Operational Experience Illustrating ATHEANA Principles

Event Timeline:

- **PRE-ACCIDENT**
  - U1
  - U2
- **INITIATOR**
  - U3
- **POST-ACCIDENT**
  - R1

**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

<table>
<thead>
<tr>
<th>Act No.</th>
<th>Error Effect</th>
<th>Error Mode</th>
<th>Error Type</th>
<th>S/R/K</th>
<th>Location</th>
<th>Personnel Type</th>
<th>Activity</th>
<th>PSFs (+/-)</th>
</tr>
</thead>
</table>
| 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    | 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)

<table>
<thead>
<tr>
<th>Event No.</th>
<th>Effect</th>
<th>S/R/K</th>
<th>Recovery Time</th>
<th>Recovery Location</th>
<th>Personnel Type</th>
<th>PSFs &amp; Defenses (+/-)</th>
</tr>
</thead>
</table>
| 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

5-25 NUREG-1624, Rev. 1
5. Operational Experience Illustrating ATHEANA Principles

**HARDWARE DEPENDENCIES**

**System(s) Involved:**
LPI

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

**Interfacing Systems:**
RCS

**Spatial Dependencies:**

**HUMAN DEPENDENCIES**

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

**ACCIDENT DIAGNOSIS LOG**

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

Figure 5.2c Event Dependencies
5. Operational Experience Illustrating ATHEANA Principles

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. Operational Experience Illustrating ATHEANA Principles