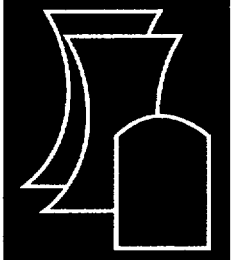
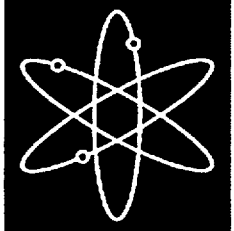
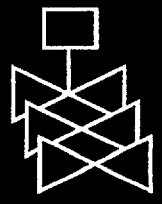






Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)

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

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

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

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

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

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

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

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

Non-NRC Reference Material

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

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

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

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

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

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

NUREG-1624, Rev. 1

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

Manuscript Completed: April 2000
Date Published: May 2000

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

ABSTRACT

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

Table of Contents

Table of Contents (Cont.)

Table of Contents (Cont.)

Table of Contents (Cont.)

Table of Contents (Cont.)

List of Figures

List of Figures (Cont.)

List of Tables

List of Tables (Cont.)

EXECUTIVE SUMMARY

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

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

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

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

ATHEANA: An HRA Method and an Event Analysis Tool

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

More specifically, ATHEANA provides the following:

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

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

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

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

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

Motivation for Developing an Improved Human Reliability Analysis Capability

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

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

Lessons Learned from Serious Accidents

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

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

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

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

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

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

The Significance of Context

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

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

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

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

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

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

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

Integration of Multiple Disciplines in ATHEANA

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

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

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

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

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

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

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

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

Overview of ATHEANA

As noted above, ATHEANA consists of:

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

Both of these processes are briefly described below.

The ATHEANA Retrospective Analysis Process

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

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

The ATHEANA HRA Process

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

The essential elements of the ATHEANA HRA process are:

- integration of the issues of concern into the ATHEANA HRA/PRA perspective
- identification of human failure events and unsafe actions that are relevant to the issue of concern

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

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

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

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

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

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

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

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

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

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

Benefits of Applying ATHEANA

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

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

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

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

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

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

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

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

FOREWORD

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

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

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

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

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

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

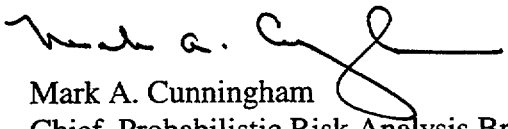
The NRC staff believes that ATHEANA has reached an important stage in its development. ATHEANA is now a thorough process for identifying, analyzing, and documenting human failure events and the contexts that make them more likely. ATHEANA shares a number of elements with current HRA methods (e.g., the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

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

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

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

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



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

ACKNOWLEDGMENTS

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

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

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

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

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

The ATHEANA team:

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

1 INTRODUCTION

1.1 Purpose and Organization of this Report

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

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

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

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

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

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

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

The basic steps in the prospective analysis are:

- integrate the issues of concern into the ATHEANA methodology

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

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

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

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

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

This report is organized in two parts:

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

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

This report also includes five appendices:

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

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

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

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

1.2 Background

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.3 Motivation for a New Approach to Human Reliability Analysis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4 Benefits from Using ATHEANA

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

1.4.1 Overview of the Risk Management Benefits of Using ATHEANA

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4.2 Insights from ATHEANA Regarding Risk Management Using PRA

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

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

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

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

1.4.2.1 Possible Plant-Specific Insights and Subsequent Improvements

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

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

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

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

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

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

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

1.4.2.2 Insights of Possible Value to the NRC and Industry

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

- identification of any new vulnerabilities not found by previous methods

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

- identification of potential changes in operator qualification exams

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

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

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

1.4.2.3 Insights Regarding Additional Qualitative Benefits from Using ATHEANA

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

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

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

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

1.4.3 General Insights

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

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

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

1.5 Other Related HRA Developmental Work

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

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

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

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

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

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

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

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

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

1.6 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2 GENERAL DESCRIPTION OF THE ATHEANA METHOD

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

2.1 The Multidisciplinary HRA Framework

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

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

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

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

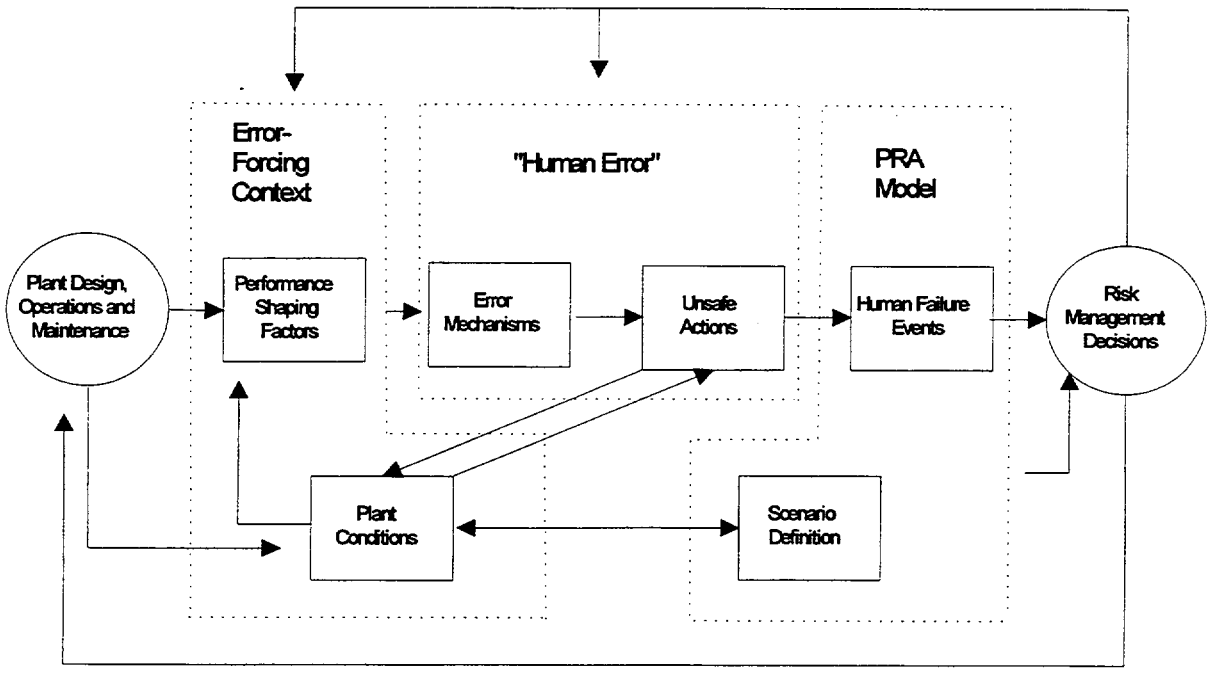


Figure 2.1 Multidisciplinary HRA Framework

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

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

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

2.1.1 Error-Forcing Context

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

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

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

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

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

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

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

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

- unusual or incorrect valve lineups or other unusual configurations

2.1.2 "Human Error"

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

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

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

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

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

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

2.1.3 The PRA Model

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

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

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

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

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

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

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

2.2 The Approach for Analysis using ATHEANA

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3 References

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

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

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

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

3 THE IMPORTANCE OF PLANT CONDITIONS AND CONTEXT IN HUMAN PERFORMANCE

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

3.1 Current HRA and PRA Perspective

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

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

3.2 The Significance of Context

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3.1 ATHEANA Reviews of Events

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

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

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

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

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

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

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

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

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

3.3.2 Other Analyses of Operational Events

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

3.4 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 BEHAVIORAL SCIENCE PERSPECTIVE

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

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

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

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

4.1 Analysis of Operator Cognitive Performance

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

4.1.1 Situation Assessment

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

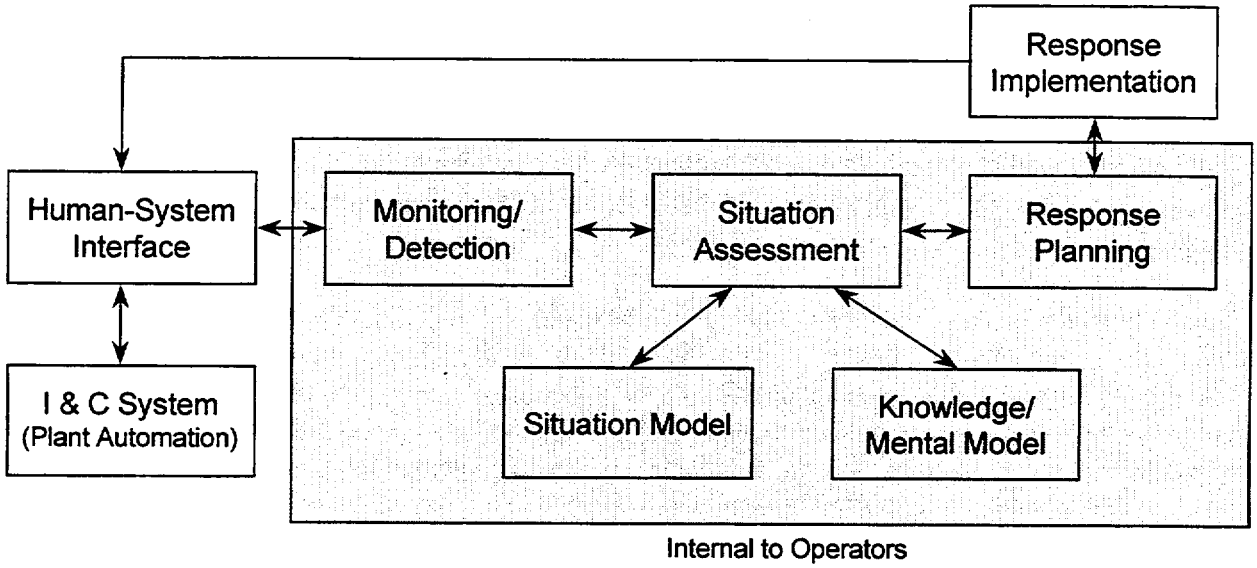


Figure 4.1 Major Cognitive Activities Underlying NPP Operator Performance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1.2 Monitoring and Detection

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

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

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

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

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

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

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

4.1.3 Response Planning

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

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

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

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

4.1.4 Response Implementation

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

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

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

4.2 Cognitive Factors Affecting Operator Performance

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

4.2.1 Knowledge Factors

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

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

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

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

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

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

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

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

4.2.2 Processing Resource Factors

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

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

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

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

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

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

4.2.3 Strategic Factors

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

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

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

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

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

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

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

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

4.3 Failures in Operator Cognitive Activity

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

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

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

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

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

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

4.3.1 Failures in Monitoring or Detection

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

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

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

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

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

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

4.3.2 Failures in Situation Assessment

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

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

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

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

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

There are four types of interpretation failures:

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

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

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

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

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

- poor displays that do not indicate targets, limits, and set points, requiring operators to retrieve and integrate values to determine whether something is normal (These memory retrieval and information integration requirements are subject to memory retrieval, working memory limits, and computational processing limitations.)

- lack of knowledge or incomplete knowledge

- impact of processing limitation factors, exacerbated in situations where the workload is high or alertness level is low

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

- lack of knowledge or incomplete knowledge (In complex accident situations, such as severe accidents, the phenomena may be less understood, and operators may not be familiar with what plant dynamics to expect.)

- limitations on working memory and computational processing that make it difficult for operators to keep in mind all relevant parameters and accurately "compute" what plant behavior should be expected (In complex situations, it may be difficult for them to perform the mental computations required to detect that observed plant behavior deviates either quantitatively or qualitatively from what would be expected.)

- impact of processing limitation factors, which are exacerbated in situations where the workload is high or alertness level is low

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

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

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

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

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

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

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

The following generally account for many human errors:

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

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

4.3.3 Failures in Response Planning

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

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

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

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

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

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

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

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

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

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

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

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

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

4.4.1 Characteristics of Parameters and Scenarios

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

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

4.4.1.1 Parametric Influences

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

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

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

4.4.1.2 Scenario Influences

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

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

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

4.5 Conclusions

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

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

4.6 References

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

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

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

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

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

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

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

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

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

4.7 Bibliography of Cognitive Psychology Literature Relevant to ATHEANA

General Treatment of the Cognitive Basis for Human Error

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

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

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

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

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

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

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

Related Works on the Concepts Discussed in this Section

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 OPERATIONAL EXPERIENCE ILLUSTRATING ATHEANA PRINCIPLES

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

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

This section provides excerpts of selected event analyses to illustrate:

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

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

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

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

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

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

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

5.1.1 Plant Conditions and PSFs

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

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

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

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

5.1.2 Failures in Information Processing Stages

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

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

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

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

5.2 Analysis of Error-Forcing Context

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

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

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

5.2.1 Error-Forcing Context and Unsafe Actions

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

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

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

5.2.1.1 Error-Forcing Context in Detection

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

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

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

Table 5.1 Examples of Detection Failures

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

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

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

5.2.1.2 Error-Forcing Context in Situation Assessment

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

Table 5.2 Examples of Situation Assessment Failures

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

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

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

Table 5.2 Examples of Situation Assessment Failures (Cont.)

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

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

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

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

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

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

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

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

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

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

5.2.1.3 Error-Forcing Context in Response Planning

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

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

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

Table 5.3 Examples of Response Planning Failures

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

Table 5.3 Examples of Response Planning Failures (Cont.)

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

5.2.1.4 Error-Forcing Context in Response Implementation

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

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

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

5.2.2 Performance-Shaping Factors

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

Table 5.4 Examples of Response Implementation Failures

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

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

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

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

5.2.3 Important Lessons from Analyses of Events

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

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

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

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

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

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

Table 5.5 Examples of PSFs on Cognitive and Physical Abilities

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

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

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

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

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

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

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

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

Table 5.6 Characteristics of Serious Accidents and Event Precursors

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

Table 5.7 Factors Not Normally Considered in PRAs

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

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

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

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

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

5.3 An Operational Event Example Illustrating Dependency Effects

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

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

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

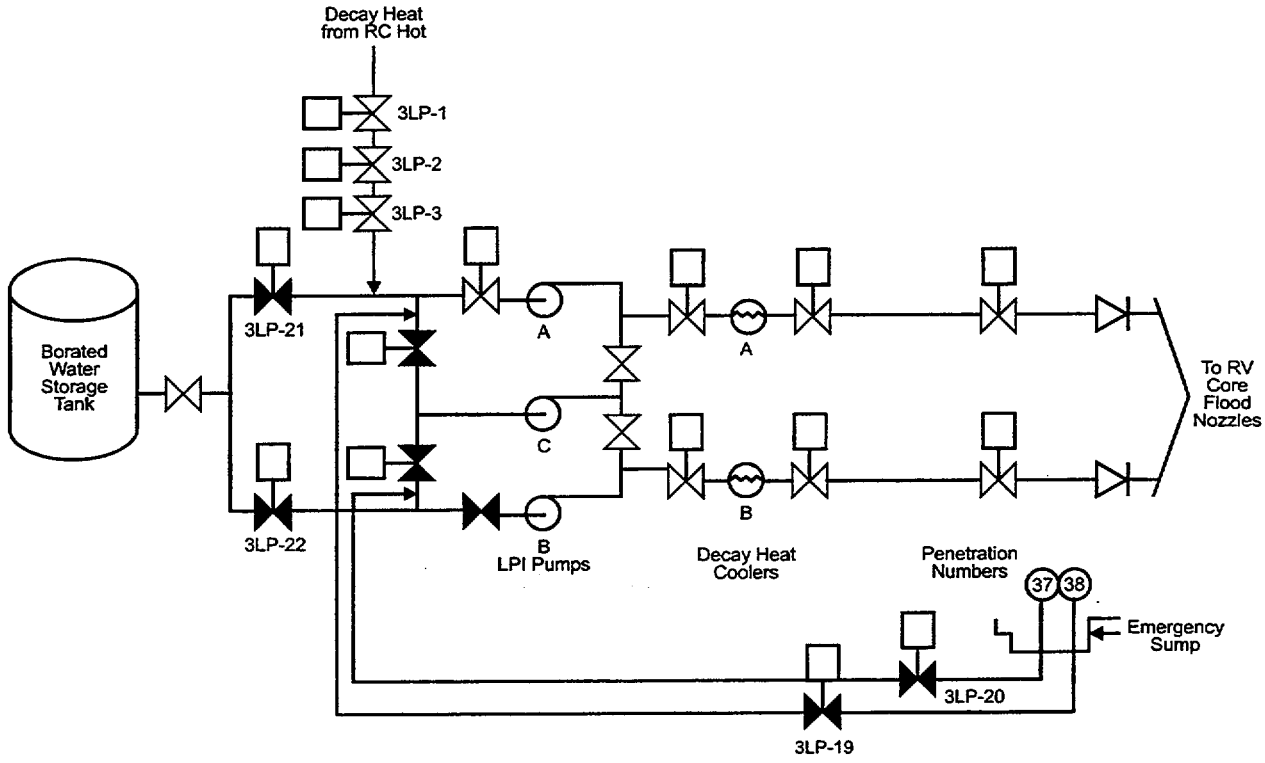


Figure 5.1 Oconee 3 Loss of Cooling

5. Operational Experience Illustrating ATHEANA Principles

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

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

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

INITIAL CONDITIONS

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

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

Plant Configuration:

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

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

ACCIDENT CONDITIONS

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

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

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

Hardware Failures:

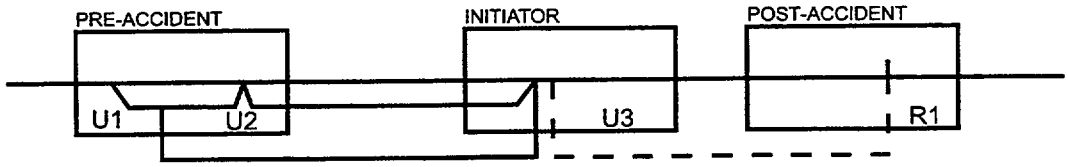
FINAL STATUS SUMMARY

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

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

Figure 5.2a Event Information

Event Timeline:



Unsafe Actions (U):

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

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

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

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

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

Figure 5.2b Summary of Human Actions

5. Operational Experience Illustrating ATHEANA Principles

HARDWARE DEPENDENCIES

System(s) Involved:
LPI

Interfacing Systems:
RCS

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

Spatial Dependencies:

HUMAN DEPENDENCIES

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

ACCIDENT DIAGNOSIS LOG

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

Figure 5.2c Event Dependencies

5.4 Summary

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

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

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

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

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

5.5 References

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

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

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

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

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

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

6 OVERVIEW OF THE ATHEANA PROCESS

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

This section provides:

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

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

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

6.1 Road Map to Part 2

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

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

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

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

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

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

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

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

6.2 Summary of Retrospective ATHEANA Analysis

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

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

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

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

Important features of the detailed retrospective analysis approach include:

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

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

6.3 Summary of Prospective ATHEANA Analysis

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

The ten steps in the prospective ATHEANA process are:

Step 1: Define and interpret the issue

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

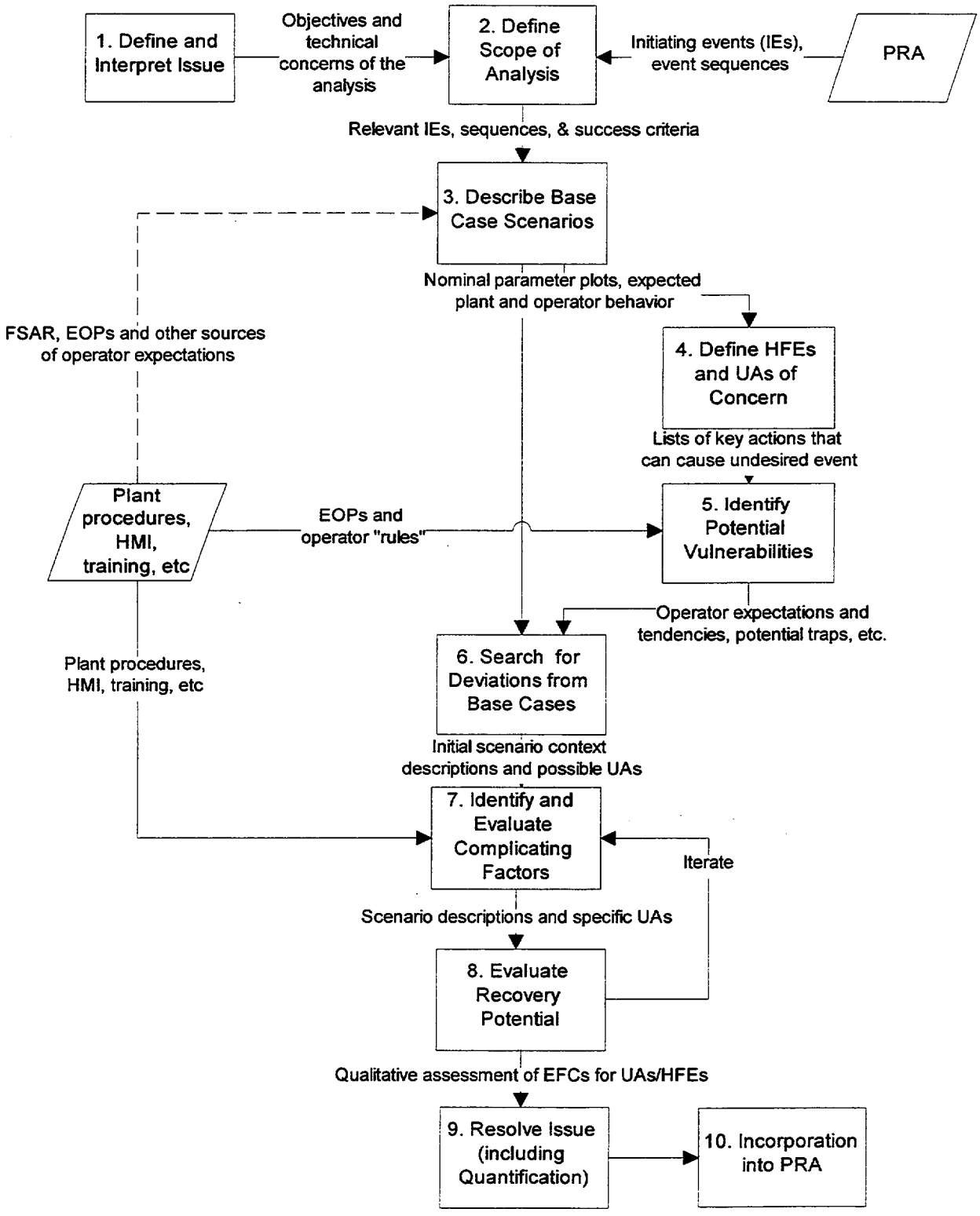


Figure 6.1 ATHEANA Prospective Search Process

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

Step 2: Define the scope of the analysis

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

Step 3: Describe the base case scenario

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

- represents the most realistic description of expected plant and operator behavior for the selected issue and initiator
- provides a basis from which to identify and define deviations from such expectations (which will be performed in Step 6)

In the ideal situation, the base case scenario:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 6: Search for deviations from the base case scenario

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

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

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

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

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

(2) evaluate rules with respect to possible deviations

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

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

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

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

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

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

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

Step 8: Evaluate the potential for recovery

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

Step 9: Quantify the HFE probability

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

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

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

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

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

Step 10: Incorporate the HFE into the PRA

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

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

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

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

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

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

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

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

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

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

Step 3: Describe Base Case Scenarios

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

Step 4: Define HFEs and UAs of Concern

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

Step 5: Identify Potential Vulnerabilities

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

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

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

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

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

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

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

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

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

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

Step 8: Evaluate the Potential for Recovery

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

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

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

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

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

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

---

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

6.4.1 Summary

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

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

6.5 References

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

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

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

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

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

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

7 PREPARATION FOR APPLYING ATHEANA

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

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

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

7.1 Select the Analysis Activity

ATHEANA can be used in the following three activities:

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

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

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

7.2 Assemble and Train the Multidisciplinary Team

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

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

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

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

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

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

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

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

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

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

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

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

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

7.3 Collect Background Information

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

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

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

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

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

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

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

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

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

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

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

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

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

This step yields the following products:

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

7.3.1 Review and Collection of Anecdotal Experience

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

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

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

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

of Nuclear Power Operations (INPO) reports]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The second type of EFC creates situations in which, while the operators' thinking is correct, plant behavior, design, and/or configuration hinder operators from successfully performing their chosen mitigative measures (i.e., execution failures). EFC elements that can create executionally problematic situations include the following examples:

- multiple hardware failures or unavailabilities (including pre-existing failures)

- unusual plant configurations

- plant design features (e.g., interlocks) that are difficult or time-consuming to recover if unintentionally triggered, disabled, etc.

- less than the usual amount of time to perform needed actions (owing to an unusual accident initiator or progression)

- execution requires communication among different locations and multiple operators, consists of many steps; or there are other workload, coordination, or communication burdens

The third type of EFC is, of course, a combination of the first two types.

7.3.2 Additional Plant-Specific Information Needed for ATHEANA

As stated earlier, it is difficult to anticipate the additional plant-specific information that will be needed before the unsafe action and EFC search steps in the ATHEANA process. However, in order to assist in the initial identification of potentially challenging situations for operators, it would

be helpful to identify the following types of plant-specific information:

- equipment with historical or recent problems (e.g., frequent failures, degraded performance, unavailability)
- instrumentation or indicators with historical or recent problems (e.g., frequent failures, miscalibrations or drift, degraded performance, unavailability)
- plant-unique initiators
- uniquely high or low frequencies of specific initiators
- recent history of specific initiators and common accident dynamics and/or progressions,
- plant-unique design features that are potentially troublesome
- "informal rules," developed from operational experience, training, and good practice, that can override or supersede formal rules contained in plant procedures
- operational practices or preferences not obvious from the review of procedures (e.g., preferential use of a particular indicator owing to its perceived historical reliability)

It is admittedly difficult to state what plant-specific sources will be most helpful in providing the above types of information. However, team members who represent training and operations are expected to identify the last two types of information from their knowledge and experience. Operators, trainers, and other operations personnel should also be interviewed.

A variety of possible sources may address the first four information types, including the knowledge and experience of team members; maintenance work records; trip history; plant-specific incident reports; and interviews of maintenance and testing personnel, systems engineers, and field and control room operators.

7.3.3 Other Information Needed Later in ATHEANA

During the course of applying ATHEANA, the need for other information and information sources may surface. However, to the extent possible, the resources needed (both staff support and information) should be identified early in the process. Plant resources that may be needed later include the following:

- consultation with training staff, individually and, perhaps, in groups (in addition to the expertise provided by team member(s) who represent the operator training department)
- simulator exercises and associated debriefing interviews of operators and trainers (see Section 7.4)

As noted earlier, the training staff can assist the analysts in identifying and understanding past or potential situations that have negative impacts on operator performance.

7.4 Prepare to Conduct Simulator Exercises

Simulator exercises and interviews with operators can be used to support the ATHEANA processes associated with identifying unsafe actions, tenable error mechanisms, and EFCs. To the extent that accidents being examined in a retrospective analysis can be simulated, it may possible to get additional insights about why unsafe actions occurred during the event. In general, however, the use of simulators as described below is related to performing a prospective analysis and the analyst team should make arrangements to use the plant simulator to support this process.

The particular roles fulfilled by use of simulator exercises in ATHEANA are as follows:

- a focused opportunity to discuss with teams of operators and other training staff the important characteristics of the context used in the exercise
- an opportunity to observe the styles of teamwork and problem-solving and general operating strategies for operating crews
- an ability to test the extent to which the context appears to be "error-forcing," either as modeled in the exercise or with additional elements as discussed with the operators and trainers
- an opportunity to evaluate the potential failure probability of the crew in the context of the event as modeled

Each of these roles is further discussed below.

As well as the inputs provided by operations trainers during the brain-storming of the ATHEANA process, the walk-through of scenarios in a simulator setting can provide an excellent opportunity to obtain inputs from personnel who are extremely familiar with the plant systems. The simulator can be stopped at key points in the scenario and the operators asked about what they believe is happening and what they expect to see next. They can be asked questions about what effect different kinds of information displays may have, why some information may be discarded, and why they may chose to deviate from a procedure or plant practice. Such discussions can also be held in a post-simulation debriefing with the operators. In either case they can provide insights into how the operators' collective situation assessment and decision-making processes work in the context of the scenario. These insights can be used to identify stronger and more likely EFCs and to provide information about additional ways in which the failures of concern could occur.

It is recognized in the ATHEANA process that the styles of working as a group and problem-solving can vary among crews and among different plants. For example, some facilities place more

emphasis on strict compliance with each step of the early emergency procedures. Such compliance has the considerable merit of systematically addressing each potential problem in turn. However, in highly dynamic events, it also has the potential for delaying responses or for some of the early dynamic characteristics to be overlooked. Therefore, for a plant that follows such a policy, a fast-paced event or an event with complex early dynamics is likely to be possibly more "error forcing." However, for a plant where such strict adherence is not emphasized so much, events that may lead operators to depart from the early procedures are perhaps more error forcing. By observing a crew's performance in the simulator, it is possible to view the style of the crew and decide how a particular scenario might be more error forcing because of the style.

The simulator exercises can be used to test the extent to which the context appears to be "error forcing," either as modeled in the exercise or with additional elements obtained from operators and trainers during the debriefing. By observing how crews transition through the decision-making points in the scenario, it is possible to detect from the discussions typically taking place among crew members where possible points of failure exist. For example, a crew in a simulator may exhibit successful problem-solving at a critical point in a scenario that relies on a unique experience or some highly specialized knowledge (for example, how a particular sensor works). In such cases, it may be judged that other crews without this knowledge may find such a scenario highly problematic, and thus the scenario may be considered error-forcing for most crews.

Given the limitations of generalizing the results of simulator exercises to actual accident conditions, it is suggested that simulators not be used as a direct source for data to quantify the likelihood of failures for a given context. However, the simulator can provide an opportunity to gain insight about the potential failure probability of the crew. In other words, the behavior of the crew and the extent to which they find the context to be problematic can provide qualitative information to help judge the likelihood of errors. For instance, if during an event the crew found no hesitation in taking a UA and the event was accurately simulated within the limits of training simulator technology, this provides empirical evidence to support selection of a comparatively high failure probability. Perhaps more important are the reflections of the crew on the scenario following the exercise. Their view on the difficulty of the scenario, the significance of the context, and possible changes in context that would have made the situation even more error forcing can be invaluable. Such changes in context could include different philosophies of operation and training that exist at other plants, used to exist at their own plant, or are being contemplated.

In conclusion, under the right conditions the use of the simulator allows the analysts to confirm the tendencies predicted in analysis and uncover unforeseen conditions that may alter their conclusions. It also provides some degree of validation that the combinations of plant conditions and PSFs (i.e., the predicted EFCs) are indeed challenging to operators and are likely to result in the predicted HFEs. The tenability of potential error mechanisms, such as operator biases, may be inferred from observing the exercises, and ideas can be obtained for how the EFCs might be altered to provide an even greater tendency to perform the undesired human actions.

In addition, post-simulation discussions with the operators can be used to gain insights about the operators' perceptions, expectations, and thought processes (even when they are successful in

responding to the specific simulated scenario) and may provide guidance for identifying stronger and more realistic EFCs. In particular, when trying to determine whether certain error mechanisms contributed to an operator's responses, strategically asked questions may allow such inferences to be made. Finally, it should also be recognized that the actual responses of the crews during simulations and the accompanying discussions would be very relevant to the quantification of the potential HFEs, given the EFCs.

7.5 Conclusion

Once the above activities are completed or prepared for in the case of simulator exercises, analysts can proceed to either Section 8 for guidance on performing a retrospective analysis or to Section 9 for guidance on performing the ATHEANA prospective analysis. However, before beginning a prospective analysis, it is highly recommended that some experience in performing retrospective analyses be obtained in order to get a better understanding of the ATHEANA perspective and general approach.

7.6 References

7.1 U.S. Nuclear Regulatory Commission, *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance*, Volumes 1, 2, and 3, Division of Systems Technology - Office of Nuclear Regulatory Research, NUREG-1560, Washington, D.C., October 1997.

7.2 U.S. Nuclear Regulatory Commission, *The Use of PRA in Risk-Informed Applications*, Division of Systems Technology - Office of Nuclear Regulatory Research, NUREG-1602, Washington, D.C., June 1997.

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

7.4 AIT Report, Salem Unit 1, April, 7, 1994, *Loss of Condenser Vacuum (and Loss of Pressure Control - RCS Filled Solid)*, Report Nos. 50-272/94-80 and 50-311/94-80, U.S. Nuclear Regulatory Commission, 1994.

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

8 RETROSPECTIVE ANALYSIS

This section provides guidance for applying ATHEANA in a retrospective analysis of actual plant events. The results of the analysis may be formatted to expand the human event database for future HRA use or as the basis for understanding the factors affecting human performance and proposing corrective actions to reduce the likelihood of similar events in the future.

8.1 Overview

The retrospective application of ATHEANA to analyzing actual plant events provides analysts with a tool for augmenting the HRA database for future use in PRAs and for identifying key corrective actions to diminish the likelihood of similar events occurring in the future. The use of ATHEANA for a retrospective analysis is a departure from other methods of analyzing plant incidents because ATHEANA is designed to identify human failure events (HFEs) as modeled in PRAs[1] and their underlying causes.

ATHEANA postulates that unsafe human actions occur within an error-forcing context that can be specifically identified. The PRA must be able to identify these error forcing contexts in order to estimate how likely these conditions are and the likely consequences in terms of inappropriate human actions or inactions. The error forcing contexts are the conditions that plant management and staff can influence. Identifying the contexts will help them control the conditions that lead to unsafe acts (UAs). The ATHEANA retrospective analysis provides a detailed sketch of the error forcing contexts.

The process is iterative and subjective, relying on contemporaneous records of the event as well as subjective recall of the events and its causes. The analysts will find that they may retrace the same information many times before obtaining a cogent and logical description of the event and the human contribution to the failures that occurred during the event.

The elements of the retrospective analysis are similar to the prospective analysis (see Section 9), but the starting place is quite different. Whereas the prospective analysis works from the defined functional failures in the PRA to identify functional failure modes that could be caused by rational human behavior, the retrospective analysis begins with the actual scenario to identify the functional failures that were caused by human behavior. The prospective analysis postulates error-forcing contexts using a rule-based search process, while the retrospective analysis sifts through the event data to uncover the error forcing-contexts.

The following steps comprise the retrospective analysis process:

---

[1] As discussed in Section 1, we must think of a PRA as a general approach for framing, analyzing, and understanding risk and safety, rather than a particular set of tools such as the event tree/fault tree analysis common in the nuclear power industry. By a PRA, we mean examining risk through a process of successive approximations, beginning with a structuring of possible scenarios that could lead to damage and continuing, first with a judgment-based evaluation of the risk, and then with successively more rigorous calculations as dictated by the seriousness of the situation, practice in the associated industry, and available resources. This broad view of a PRA is not new to ATHEANA [see, for example (Ref. 8.1 and Ref. 8.2)].

(1) Identify the undesired event. The act of clearly identifying the undesired event provides a defined scope for the analysis.

(2) Identify the functional failures, the HFEs, and the UAs.

(3) Identify the causes of the UAs, including plant conditions and performance shaping factors (PSFs)

(4) Document the results.

The desired result of the retrospective analysis can be summarized in a flow chart. An example of results from an ATHEANA retrospective analysis is shown in Figure 8.1. The information presented in the Appendix A retrospective analysis A.1 is summarized in the ATHEANA framework in this flowchart. The analysis is performed largely in the reverse direction of the flow, i.e., the HFEs and UAs are identified before the information-processing failure, PSFs, and contributing plant conditions. The representation in Figure 8.1 demonstrates the ATHEANA principle that HFEs are heavily dependent upon plant conditions and PSFs.

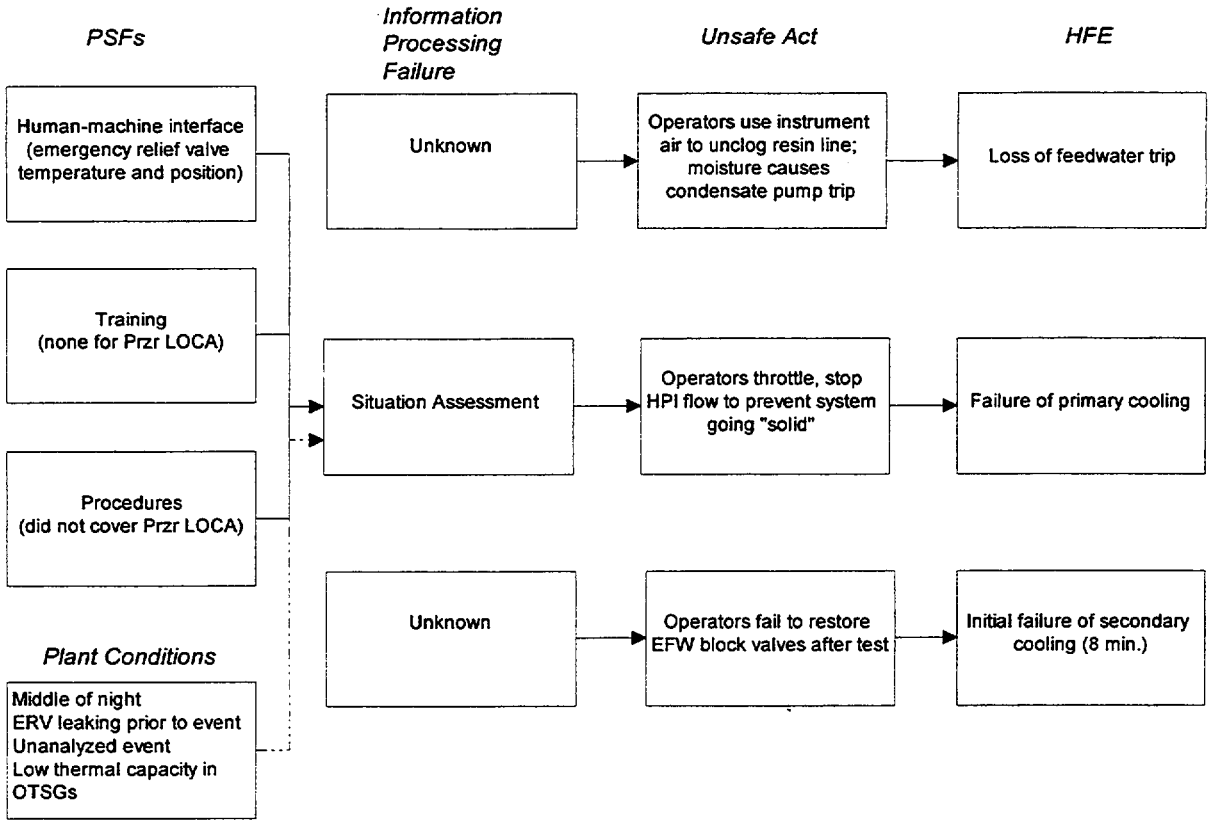


Figure 8.1 TMI-2 Represented in ATHEANA Framework

8.2 Identify and Describe the Undesired Event

The plant event defines the scope of the analysis. Undesired events will typically have the following characteristics:

- severe or potentially severe consequences
- operation outside the boundaries of good operation
- extensive operator control of the plant

The analysts must fully describe the scenario of the event. Any of the event summaries used for the retrospective analyses in Appendix A may be used as an example for this step. This is not a trivial undertaking inasmuch as the background information gathered as described in Section 7 may provide incomplete or conflicting information about the event.

The analysts next list the initial plant conditions and the resultant accident conditions just prior to recovery. These are the key plant parameters that must be controlled for safe operation. Suggested parameters to be included are:

Initial conditions:

- primary or reactor system parameters (power level, system temperature, pressure, water level, chemistry, etc.)
- evolution and activities
- configuration
- preexisting operational problems
- initiator

Accident conditions:

- primary system parameters
- automatic responses
- failures
- human-system interactions
- defeated defenses

To provide further insight as to the unique aspects of the event, it is recommended that the analysts identify the surprises during the event from the analysts' perspective; these are plant or human responses that seem surprising, given the situation. They could be plant response to certain actions, robustness of the plant, speed of response, unexpected operator response, etc.

8.3 Identify the Functional Failures, the HFEs, and the UAs

The analysts next identify the functional failures that occurred during the undesired event. Functional failures are modeled in the PRA and can be function, system, or component failures. Functional failures can occur for many reasons and may be stated generally. Section 9 of this report

provides guidelines for identifying functional failures. The retrospective analysis examples in Appendix A do not specifically identify the functional failures, but it is recommended that the analysts do so to facilitate the identification of the human failure events and uncover the UAs that caused the HFE. For instance, in the Crystal River Unit 3 spray valve failure event, Section A.2, the functional failure is failure of RCS pressure control.

An HFE is a functional failure that is the result of one or more unsafe human actions. UAs are actions inappropriately taken by plant personnel or actions not taken when needed that result in a degraded plant safety condition. The term "unsafe act" does not imply that the human was the cause of the problem. Indeed, the analysis of operational events avoids inference of blame by looking for the circumstances and conditions that set up people to take actions that are unsafe.

Each HFE has associated UAs that define the specific ways in which plant, system, or equipment functions are failed by human actions or inactions. The analysts will examine the information gathered prior to the analysis to understand the human actions taken that lead to the potential HFE. For example, UAs could be:

- turning off running equipment
- bypassing signals for automatically starting equipment
- changing the plant configuration so it defeats interlocks that are designed to prevent damage to equipment
- excessive depletion or diversion of plant resources (e.g., water sources)

If a PRA-related functional failure has occurred that was not previously modeled as an HFE, the event provides an incentive to revise the existing PRA. If no PRA-related functional failure has occurred, the event is not directly risk significant. Nevertheless, its information on the cause of failures in human performance may be useful.

The analysts begin the identification of the functional failures and UAs by constructing an event diagnosis log. The event diagnosis log lists in chronological order the plant conditions and operator actions from the initiation of the event until the recovery and stabilization of the plant at the end of the event. Much of the information gathered prior to the analysis will be brought together to construct this log. The analysts should spend the requisite effort in creating a complete fact-driven diagnosis log, continuing with information gathering until anomalies and gaps in the chronology are filled. The log is the most useful deductive piece of the analysis and will be referred to frequently by the analysts to postulate the causes of the UAs. Examples of the event diagnosis log are provided in Appendix A.

The diagnosis log will provide the information to isolate the plant functional failures, the HFEs, and the UAs that caused the HFE. To isolate these ATHEANA elements, the analysts label key actions and equipment failures in the diagnosis log as follows:

- unsafe acts (U): actions that lead to the HFE
- nonerror, nonrecovery actions (H): normal actions taken by plant staff that neither lead to plant recovery nor contribute to the HFE
- recovery actions (R): actions taken by plant staff to mitigate the event and put the plant in a safe or stable condition
- equipment failures (E): equipment that failed to operate when automatically or manually initiated or equipment that operated incorrectly

Each operator action and equipment failure that appears to contribute to exacerbating or mitigating the consequences of the identified undesired event should be listed in a table and graphically depicted in a chronological relationship of the actions and failures of the event. This relationship is displayed for the events analyzed in Appendix A. Thus, as illustrated in the appendix, the key contributions to the event's outcome are presented on the event timeline, identified in a UAs and other events table, and in the diagnosis log. The analysis of undesired events to this point will usually require iteration. Dependencies among the actions and events are identified in the human dependencies table. Dependent actions and events have a strong influence on error-forcing context (Ref. 8.3).

Figure 8.1 of the TMI retrospective analysis provides one example of the relationship between the HFE and the UAs. A similar presentation constructed for the Crystal River Unit 3 spray valve failure event is shown in Figure 8.2.

8.4 Identify the Causes of the UAs

The key analysis for the ATHEANA process is determining the causes of the UAs by identifying information-processing failures and the error-forcing context composed of the PSFs and significant contributing plant conditions.

8.4.1 Information Processing Failures

The analysts will not be able to precisely determine what the operators were thinking when they took the UAs. When reasonable, the analysts will postulate what caused the operator to take the UA(s) based on the surrounding conditions, statements of the operators, etc. The psychological discussion in Section 4 of this report may be helpful to the analysts in postulating the causes. More often, only the failures in information processing, evidenced by the operators' behavior, can be assessed. The typical ones are listed below:

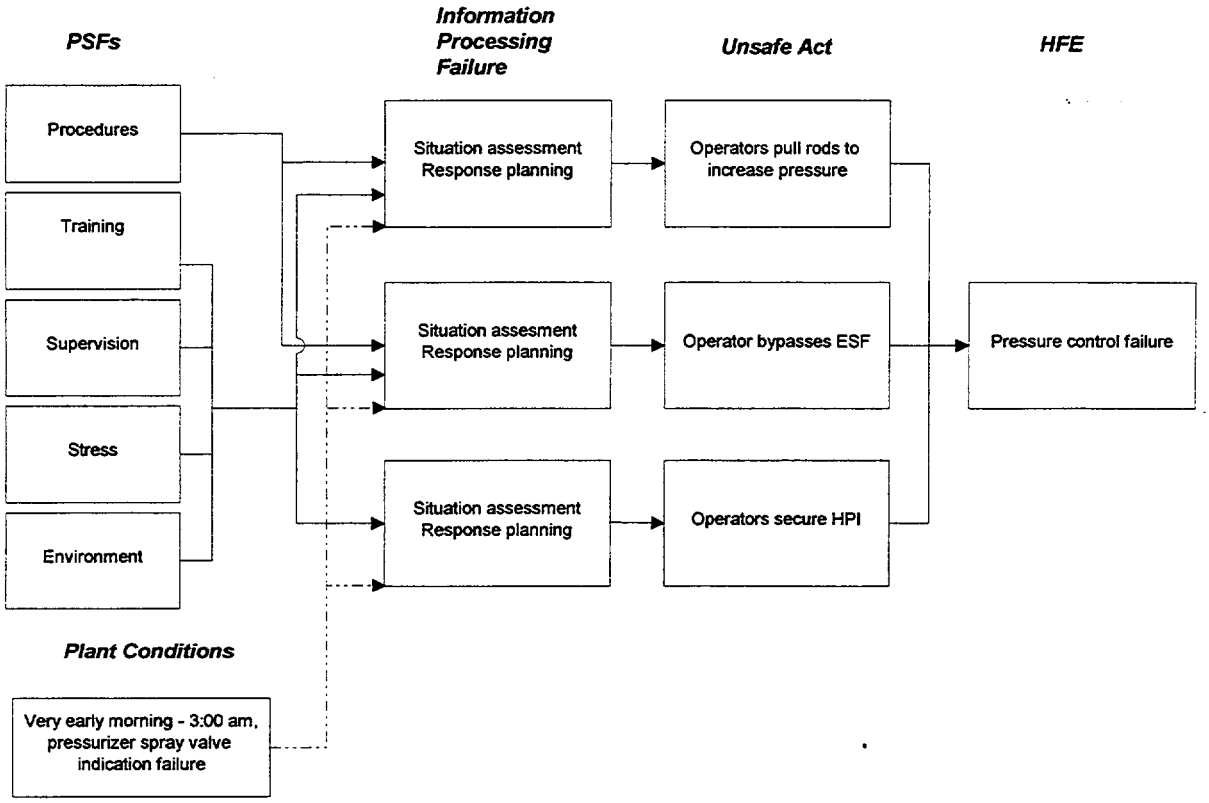


Figure 8.2 Crystal River Unit 1 Represented in ATHEANA Framework

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

- Situation assessment
  - information is erroneous or misleading
  - plant indicators are misinterpreted
  - plant or equipment behavior is misunderstood
  - similarity of the event to other better-known events leads operator to form an incorrect situation model

- Response planning
  - operators select nonapplicable plans
  - operators follow prepared plans that are wrong or incomplete
  - operators do not follow prepared plans
  - prepared plans do not exist, so operators rely upon knowledge-based behavior
  - operators inappropriately give priority to one plant function over another

- Response implementation
  - important procedural steps are missed
  - miscommunication
  - equipment failures hinder operators' ability to respond

Refer to Section 5 for a discussion of these factors applied to the specific events and to Appendix A for completely worked-out examples.

8.4.2 Performance-Shaping Factors

The analysts sift through the event information gathered to identify PSFs that, when combined with plant conditions, might reasonably be expected to cause the error mechanism and a UA. In other words, the analysts look for factors that helped to set up the operator to make an error. Examples of PSFs identified in event analyses include:

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

The underlying causes of the PSFs may be such things as training, poor or incomplete procedures, time of day, organizational factors, or poor human–system interfaces. Section 5.2.2 of this report provides background on PSFs. Based on this analysis, it is useful for the analysts to summarize what the most negative influences on the event actions appear to be or are mentioned by participants in the event, as well as the most positive influences on the event. See Appendix A retrospective analyses for examples.

8.4.3 Significant Plant Conditions

As part of the error-forcing context, the analysts should also summarize the most significant plant conditions that differ from expected plant conditions. These would include, for example:

- extreme or unusual conditions
- contributing preexisting conditions
- multiple hardware failures
- transitions in progress

8.5 Drawing Conclusions

The analysts draw together, for each UA, the plant conditions and PSFs that they believe caused the failure of information processing for the unsafe act. It may turn out that there is more than one error mechanism for each UA act as demonstrated in the analyses in Appendix A.

The analysts' evidence of the error-forcing context, the combination of plant conditions and PSFs, is presented so that an independent reviewer can draw the same conclusion regarding the team's assessment of the cause of the UA. The presentations used in the analyses in Appendix A or summarized as in Figures 8.1 and 8.2 are reasonable ways to present the evidence. For each event analyzed, there could be one or more HFEs identified, each with one or more contributing UAs. The representation of the event may be complex. The analysts have the responsibility of making it as clear and straightforward as possible.

8.6 Document the Results of the Analysis

Using the examples in Appendix A and Figures 8.1 and 8.2 as templates, the analysts document their discussions, rationale, and findings.

8.7 References

8.1 Magee, R.S., E.M. Drake, D.C. Bley, G.H. Dyer, V.E. Falter, J.R. Gibson, M.R. Greenberg, C.E. Kolb, D.S. Kosson, W.G. May, A.H. Mushkatel, P.J. Niemiec, G.W. Parshall, W. Tumas, and J. Wu, *Risk Assessment and Management at Deseret Chemical Depot and the Tooele Chemical Agent Disposal Facility*, Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, National Research Council, National Academy Press, Washington, DC, 1997.

8.2 Isselbacher, K.J., A.C. Upton, J.C. Bailar, K.B. Bischoff, K.T. Bogen, J.I. Brauman, D.D. Doniger, J. Doull, A.M. Finkel, C.C. Harris, P.K. Hopke, S.S. Jasanoff, R.O. McClellan, L.E. Moses, D.W. North, C.N. Oren, R.T. Parkin, E.D. Pellizzari, J.V. Fodricks, A.G. Russell, J.N. Seiber, S.N. Spaw, J.D. Spengler, B. Walker, and H. Witschi, *Science and Judgment in Risk Assessment*, Committee on Risk Assessment of Hazardous Air Pollutants, National Research Council, National Academy Press, Washington, DC, 1994.

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

9 DETAILED DESCRIPTION OF PROCESS

9.0 Introduction

This section provides guidance for applying the ATHEANA prospective search process. Figure 9.1 is a flow diagram showing the major steps in the process. Figure 9.1a provides a key to the meaning of different shaped boxes in Figure 9.1 and in the remaining figures in the section. Because the performance of Steps 9 and 10 (i.e., quantification and interpretation of findings) involves management decisions and is very closely tied to the issue being addressed (see Step 1), these steps are discussed in Section 10.

The ATHEANA prospective process is designed to be used for a wide range of applications, from a complete HRA analysis to support a new PRA, to addressing a particular risk-related issue, as discussed in Section 1. Appendices B through E provide examples of ATHEANA applications for the following initiators:

- loss of main feedwater
- loss-of-coolant accident (LOCA)
- small LOCA
- loss of service water

The guidance given in this section should be used in conjunction with the illustrative examples given in these appendices.

9.1 Step 1: Define and Interpret the Issue

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

ATHEANA may be useful in addressing operator performance concerns in risk-significant situations of many varieties. Since ATHEANA provides both qualitative and quantitative insights, both PRA and non-PRA applications are possible. ATHEANA applications for prospective analysis can, for example:

- provide an HRA to support a new PRA

- assist in the expansion of the original PRA scope to address issues of new concern (e.g., the impact of cable aging)

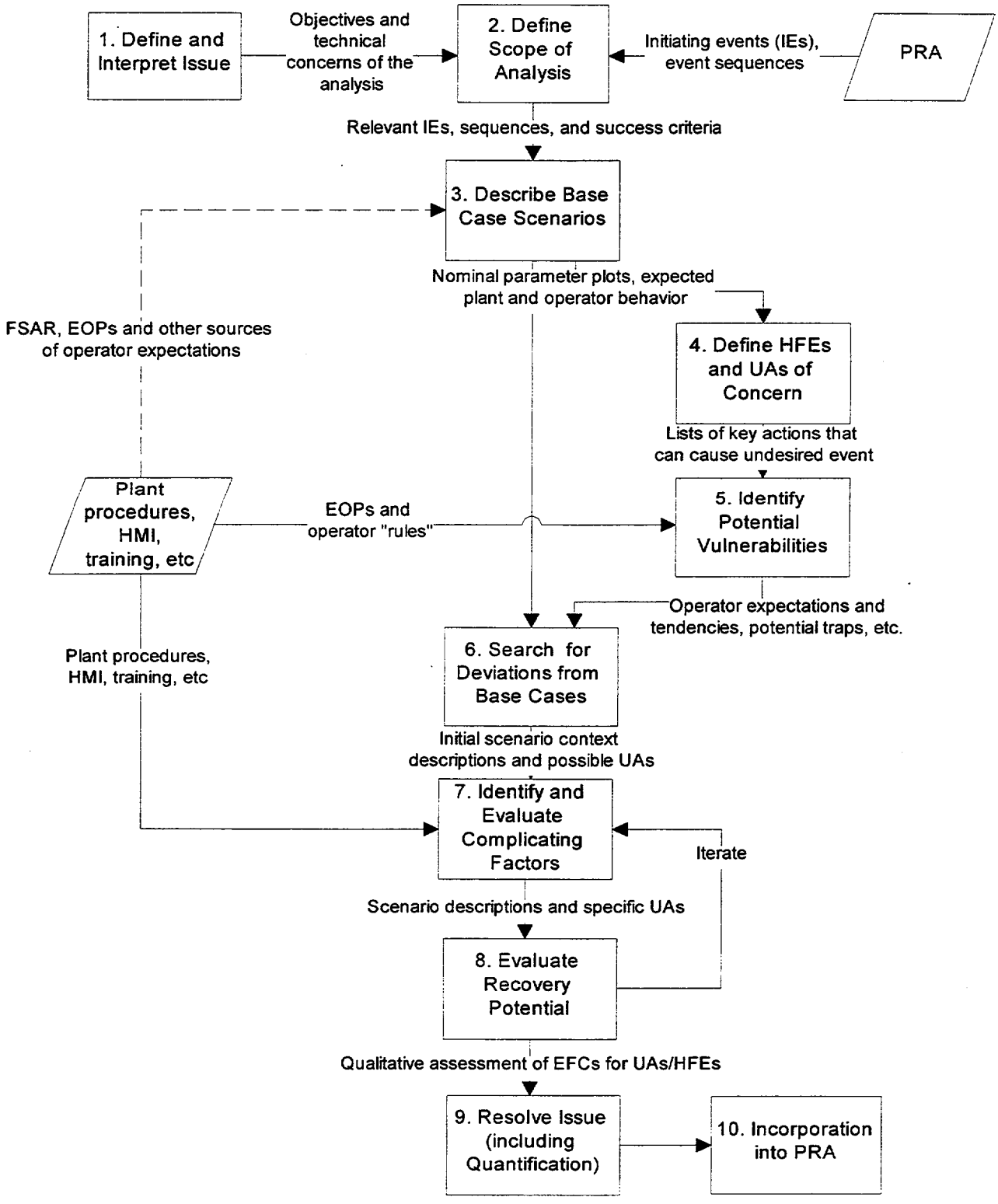


Figure 9.1 ATHEANA Prospective Search Process

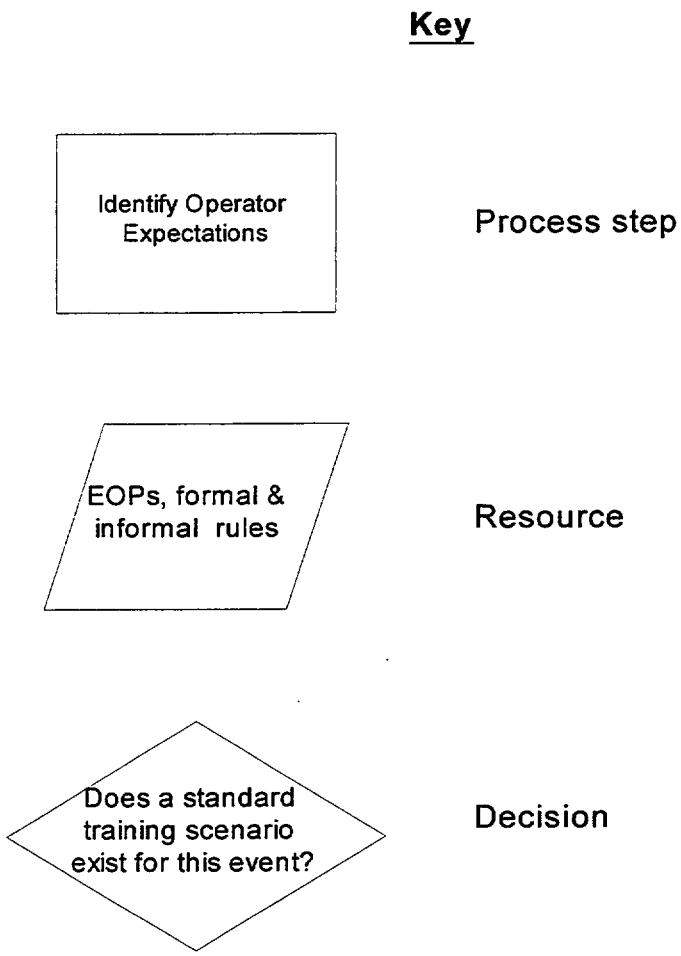


Figure 9.1a Key for the Meaning of the Box Shapes in Figures 9.1- 9.6

- assist in upgrading PRA studies for the purposes of risk-informed regulation (e.g., preparing submittals)
- refine existing PRAs and HRAs (e.g., fire PRAs, low-power and shutdown PRAs, internal events PRAs, especially with respect to errors of commission)

A wide range of such application issues was discussed in Section 1. In addition, Appendices B through E provide illustrative examples of ATHEANA for specific issues. For example, Appendix B investigates potential operator vulnerabilities to inappropriately shutting down AFW pumps in scenarios involving loss or serious degradation of steam generator cooling flow during full-power operation. On the other hand, Appendix C performs a more general investigation of the possible "physics" deviations to a LLOCA that might adversely affect operator response. The four appendices demonstrate that there is a broad range of issues that can be investigated using ATHEANA.

9.1.1 Guidance for Step 1

Sources of Issues. The ATHEANA analysis begins when the analysts are tasked to address specific issues as a result of problems or questions related to the impact of human performance on risk. Sources for the analysis request could include:

- regulators or government officials
- utility management
- utility technical staff, including the PRA/HRA and operating experience groups
- members of the public

Clearly Define the Issue. Questions and issues provided to the ATHEANA analysts for resolution often are phrased in vague or very general terms. To avoid wasted resources and disappointed interest groups, it is essential that the analysts work with the source to reach agreement on a clear, technical statement of the issue in unambiguous terms amenable to analysis.

Interpret the Issue in the Context of a PRA. For the analysis to proceed, the issue should be interpreted in terms of the PRA. This risk-informed interpretation will form the basis for many of the following steps of analysis.

In this risk-informed interpretation, we must think of a PRA as a general approach for framing, analyzing, and understanding risk and safety, rather than a particular set of tools such as the event tree or fault tree analysis common in the nuclear power industry. (References 9.1 and 9.2 provide a discussion of this perspective.) By PRA, we mean examining risk through a process of successive approximations, beginning with a structuring of possible scenarios that could lead to damage and continuing, first with a judgment-based evaluation of the risk, and then with successively more rigorous calculations, as dictated by the seriousness of the situation, practice in the associated industry, and available resources.

9.1.2 Products of Step 1

The output of this step is a succinct description of the issue to be analyzed, indicating, to the extent practicable, the boundaries for the analysis, the overall goal of the analysis, and the relationship of the issue to risk and the PRA, if one is available.

9.2 Step 2: Define the Scope of the Analysis

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

9.2.1 Guidance for Step 2

The flow of the analysis in this step is sketched in Figure 9.2 and described in the following paragraphs.

Scope Limitations Provided by the Issue. The issue itself usually provides the primary scope limitation. In many cases, the issue limits the scope so narrowly that little or no additional restrictions are necessary to permit a manageable ATHEANA analysis. For example, the illustrative case presented in Appendix C limits the analysis to a single initiator, the large LOCA.. In other cases, we may only be interested in:

- certain specific functional failures
- only certain specific human failure events, or
- certain specific unsafe acts

Developing Further Scope Limitations by Setting Priorities. The ATHEANA analysts will decide which initiators, event trees, and human failure events to analyze first. Priorities can be established, either by developing an overall plan or schedule for the analysis, or by determining an analysis scope that represents a significant resolution of the issue and is consistent with currently available resources.

Setting priorities is an iterative process over Steps 2, 3, 4, 6, and 7 and uses information from:

- the PRA (initiators, event trees, plant functions and their associated systems and equipment)
- the emergency operating procedures
- the events or scenarios that concern the plant staff (e.g., operations manager, trainers)

- operational experience
- resources available to perform the analysis

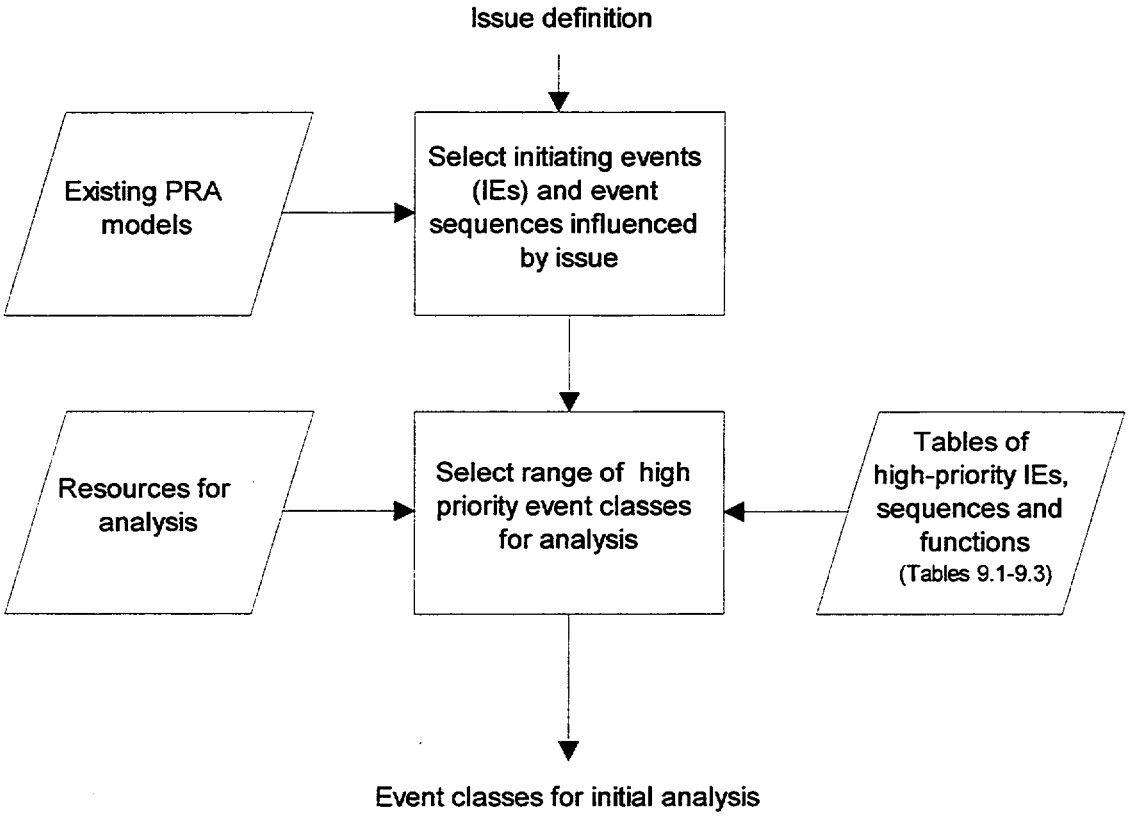


Figure 9.2 Step 2 - Describe the Scope of the Analysis

Because it is always necessary to select the initiating events for analysis, we provide guidance on these events before describing the approach for setting priorities.

Specific Guidance for Selecting the Initiating Event Classes and Relevant Initiators. The issue itself may limit the selection of initiating events. Otherwise, priorities must be developed based on the likely risk significance of the initiating event. It is always necessary to select specific initiating events for analysis. In a nuclear plant PRA, the generally accepted definition of an initiating event is:

> *Any event that perturbs the steady state operation of the plant, if operating, or the steady state operation of the decay heat removal system during shutdown operations, thereby initiating a transient within the plant. (Initiating events trigger sequences of events that challenge plant control and safety systems).*[1]

In this document, classes of initiating events are distinguished from the specific initiator since more than one initiator may trigger a sequence of events that lead to the same initiating event class (e.g., a transient). A generic list of initiating event classes and associated initiators is provided in Table 9.1. Other references for initiator lists include the plant-specific final safety analysis report (FSAR), the plant-specific probabilistic risk assessment (PRA), plant-specific and vendor safety analyses, plant-specific and industry generic event history, and other generic references (e.g., Ref. 9.3).

The ATHEANA process also recognizes two different types of initiating events because of the way they may affect human performance:

- direct initiating events
- indirect initiating events (all of which eventually or immediately lead to one or more direct initiating event, which is the point where steady-state operation is disrupted)

Direct initiating events are those that meet the generally accepted PRA definition given above. The base case scenarios for these initiators are usually straightforward, well documented, and follow a predictable sequence of events. Indications that the event has occurred are reasonably quick, direct, and often easily discernable. Also, they are well supported by emergency procedures and training. The expected and essential associated human actions are generally modeled in the HRA of the PRA.

---

[1] Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, Proposed final draft to be released for public comment, American Society for Mechanical Engineers (ASME) RA-S-1999 Edition Draft #9, January 21, 1999.

Indirect initiating events begin with some *starting event*[2] that causes or starts a sequence of events that lead to a standard initiating event. Sometimes there is substantial delay before steady-state operation is perturbed (i.e., until a standard initiating event occurs). Early indications of these events are often subtle, perhaps misleading, and often it is difficult to determine the extent of the effects of such events. For instance, these events could cause propagating damage to plant equipment before a reactor trip (or other initiator) occurs. These characteristics provide a greater challenge for operators to understand the nature of the event and the resulting plant status. Starting events include many of the support system initiating events (e.g., loss of service water and loss of instrument air) and environmental events (e.g., fires, floods, and earthquakes). By the time a reactor trip actually occurs and the operators enter the EOPs, substantial confusion and conditions causing bias and dependencies may already exist.

In most cases, the issue selected in Step 1 will help determine what initiating event classes and initiators should be selected. For example, if the issue is to analyze the risk from fires, then the analysts should choose the initiators that best represent or are most affected by fire events. It is a typical assumption in PRAs that fires lead to a reactor trip and subsequent loss of feedwater, and in some cases loss of offsite power can be assumed. Unless the ATHEANA analysts can identify other specific initiators because of particular vulnerabilities (for example, support system components), these initiators are a suitable starting point for investigating the risk from fires. If the issue selected does not require or imply which event type(s) should be selected, then the analysts should develop priorities for the initiating event classes.

Table 9.1 Generic List of Initiating Event Classes and Associated Initiators

Initiating Event Class	Example Initiators
Transients (internal) – with and without feedwater available	Loss of offsite power (SBO) Loss of main feedwater Loss of vacuum Turbine trip Reactor trip MSIV closure Loss of circulating water
LOCA	Large Small Medium

[2]Current PRAs are somewhat self-contradictory in using the term "initiating event." They typically define an initiating event as described earlier, then in the initiating event analysis and in the subsequent PRA, they identify starting events (our second class) such as fire and loss of service water as initiating events. Such events clearly fail to meet the definition of initiating event given above: They cause no immediate trip of the turbine and reactor; and they cause no immediate departure from steady-state operation. Because there is no practical significance of this logical inconsistency when plant hardware systems are modeled, the PRA community has largely ignored it. However, the distinction is remarkably significant when modeling human operator response. The two classes of event sequences present very different challenges to the operators.

Table 9.1 Generic List of Initiating Event Classes and Associated Initiators (Cont.)

Initiating Event Class	Example Initiators
Support system failures	Loss of HVAC Loss of service water Loss of instrument air Loss of dc bus Loss of ac bus Loss of instrument bus Loss of component cooling water Loss of reactor building closed cooling water
External events	Fires Seismic disturbance Floods Winds
Other/special	Interfacing systems LOCA Anticipated transient without scram (ATWS) Steam generator tube rupture (SGTR) Feedline break Reactor vessel (RV) failure (e.g., pressurized thermal shock)
Alternative modes	Low power and shutdown

Specific Guidance for Setting Priorities. Priorities for examining different initiators and event trees are used to further restrict the scope of the analysis and focus it on potentially higher-risk events. The existing plant-specific PRA model, including event trees, fault trees, success criteria, initiating events and event frequencies, should be used along with Tables 9.2 and 9.3 to establish plant-specific priorities. The ATHEANA analysts also may find the excerpts from operational experience given in Part 1, Tables 5.6 and 5.7, which together can serve as templates or guidance for defining error-forcing contexts, useful in identifying high-priority initiators and event trees.

Table 9.2 provides a generic list of accident sequence characteristics that have potentially high risk significance from the human perspective. This list is based upon behavioral science principles, operational experience reviews (see, for example, those given in Part 1), and PRA principles. For example, operators can develop expectations regarding the event type (based upon initial accident symptoms) and its likely progression for events that occur relatively frequently (or recently). Operators can develop similar expectations for initiators and accident sequences that have a wide range of possible conditions or trajectories. In addition, the PRA may consider only certain nominal conditions or trajectories out of a broad spectrum. However, if a different event (but with some similar initial symptoms) occurs or if an event follows a significantly different trajectory than expected, then a potentially challenging situation is created for operators that can lead them to take incorrect actions.

Challenging situations also can be created by events that have the potential for creating complex, hidden, or unfamiliar plant conditions. Such conditions may include multiple hardware failures, especially those that are dependent; confusing, contradictory, or remote indications (including those wide-spread problems that can be caused by fires or seismic events); and confusing plant behavior (especially that due to degraded performance, rather than catastrophic failure, support system failures, and unusual plant configurations). If the time to core damage (or failure of a plant function) is relatively short, the ability of operators to break out of their initial mindset (i.e., expectations) and to correct any associated initial actions is limited. The opportunity for operator recovery of initial actions is similarly limited if a single functional failure leads directly to core damage and that function can be failed by operator intervention. Note that the list of ATHEANA-suggested priorities for initiators or accident sequences contains generalized descriptions of error-forcing context elements (e.g., unusual, hidden, or unfamiliar plant conditions).

Table 9.3 takes the analysis one level below that of Table 9.2, identifying the characteristics of plant functions and associated systems that have potentially high risk significance from the human perspective. It is based on the same principles as Table 9.2. The specific priorities the analyst assigns to particular characteristics in Tables 9.2 and 9.3 depend on a number of factors ranging from the particular plant design and how that affects plant response to the way individual members of operating crews interact at the specific plant under analysis. The latter was perhaps the most important lesson learned from observing plant crews in the simulator during the early trials of ATHEANA. The analysts must identify characteristics of the operating practices at the plant that make some kinds of UA-EFC pairs more or less likely, then set priorities to bring forward the more likely failure paths. A key step in this process will be observing crews in action in the simulator. Key factors to consider include teamwork, reliance on and confidence in the procedures and the plant computer, the style of formal and informal communication, the way in which the team keeps track of its progress, and how its members interact to verify the appropriateness of completed and planned actions.

Table 9.2 ATHEANA-Suggested Characteristics of High-Priority Initiators or Accident Sequences

Characteristic of Scenario	Comment/Example
Short time to damage	Large-break loss-of-coolant accident (LLOCA) initiator in the context of PRA
Unfamiliar	Not specifically analyzed in FSAR, not specifically included in operator training
Single functional failure goes to damage	Long-term cooling (e.g., failure of changeover to recirculation mode) in scenarios requiring this function
Distraction that separates control room team	Fire requires someone from the control room staff to function as a fire-fighting crew member
Forces independent action by one member of team	Fast response is required with little time for stepwise communication

Table 9.2 ATHEANA-Suggested Characteristics of High-Priority Initiators or Accident Sequences (Cont.)

Characteristic of Scenario	Comment/Example
Potential for complex and/or hidden or unfamiliar conditions	No salient evidence or reminders; dependencies or dependent failures, especially where cause and effects are far removed from each other; confusing secondary (PWRs) or support system failures; fires; seismic events
Multiple (maybe conflicting) priorities	Operators must select among or use multiple procedures (or other rules).
Wide range of accident responses, plant dynamics/conditions represented	Confusion with similar but less complex situations
Relatively high-frequency events	Transients, small-break loss-of-coolant accident (SLOCA) in the context of PRA

Next the analysts can establish priorities for the plant functions and associated systems and equipment required in response to accident initiators. The ATHEANA analysts should use the existing, plant-specific PRA model and the examples of accident characteristics given in Table 9.2. In addition, they should use the examples of characteristics given in Table 9.3 to identify potentially high priority plant functions and systems that have these characteristics. The analysts also may find the excerpts from operational experience given in Part 1, Tables 5.6 and 5.7, which can serve as templates for error-forcing contexts, useful in identifying high-priority plant functions, systems, or unsafe actions. Later, in Step 4, the high-priority HFEs associated with the high-priority functions and systems can be identified.

Table 9.3 ATHEANA-Suggested Characteristics of High-Priority Systems and Functions

Characteristics	Example
Short time to damage	No injection in a LOCA, failure of boron injection systems in anticipated transient without scram (ATWS)
Single functional failure goes to damage	No injection in a small LOCA, failure to isolate a large interfacing system LOCA
Function needed early in accident response	Inhibit automatic depressurization system (ADS) in BWR ATWS, injection in certain-sized LOCAs, boron injection in ATWS

Table 9.3 ATHEANA-Suggested Characteristics of HighPriority Systems and Functions (Cont.)

Characteristics	Example
Little or no redundancy of systems and equipment that can perform plant function	Pressure-operated relief valves (PORV) and high-pressure injection (HPI) in feed-and-bleed, low-pressure injection or recirculation system for all recirculation modes
Dependencies between redundant systems and equipment that can perform plant function	Effects of loss of reactor building closed cooling water to support high- and low-pressure coolant injection
Paucity of action cues creates high potential for confusion and complications	Events that involve unfamiliar plant conditions; similarity to other plant conditions; wide range of plant conditions and dynamics and accident response represented; cause and effects are far removed from each other; involves instrumentation and control (I&C) (about which operators are often least knowledgeable)
Functional failure has immediate effect and plant impact	Subcriticality
Functional failure can include an irreversible plant or equipment damage that has no easy recovery options or none	Failure to inhibit an emergency and full blowdown using the instrumentation and control ADS during a BWR ATWS; EOCs for inappropriate starts or stops of equipment
Human-intensive accident response important principally for EOCs	Steam generator tube rupture (SGTR) sequences, ATWS sequences

9.2.2 Products of Step 2

The output of this step is a set of selected initiators (or overall classes of initiators, if desirable) for which the issue (from Step 1) is to be analyzed. This provides some boundaries for the analysis and therefore an overall context, as well as a relationship to a PRA. In addition, the development of priorities on scenarios and plant functions is used in Steps 3, 4, and 6 to guide the analysis.

9.3 Step 3: Describe the Base Case Scenario

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

- represents the most realistic description of expected plant and operator behavior[3] for the selected issue and initiator

[3] However, it is recognized that a range of conditions within the definition of the base case scenario is possible.

- provides a basis from which to identify and define deviations from such expectations in Step 6

Figure 9.3 is a process flow diagram that shows the detailed tasks required for this step. An overview of these tasks is provided in Section 9.3.1. Following the overview, more detailed guidance for developing the base case scenario is provided.

9.3.1 Overview of Step 3

As stated above, the purpose of this step is to define and characterize a base case scenario that will be used in later ATHEANA analysis steps. Table 9.4 operationally defines what a base case scenario is. For example, the ideally defined base case scenario:

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

Each of the characteristics of an ideal base case scenario is described briefly below.

Consensus operator model: Operators develop mental models of plant responses to various PRA initiating events through training and experience. If a scenario is well defined and consistently understood among all operators (i.e., there is a consensus among the operators), then there is a consensus operator model. Note that given the current high reliability of operations, with zero to one trips per year at each plant, most operators licensed within the past five years will have no direct experience with even the most common trip scenarios. For more seasoned operators, direct experience is becoming increasingly remote. Therefore, it is likely that the consensus operator model will be that seen routinely in the plant simulator.

Well defined operationally: A scenario is well defined operationally if the scenario has been addressed in procedures, training, operational or simulator experience, and the specific equipment and expected operator responses are well understood.

Well-defined physics: If the plant behavior has been thoroughly analyzed in thermal hydraulics, neutronics, or other calculations, the physics of the scenario is considered well defined. This characteristic, along with the characteristic of being well documented, is termed the "reference analysis" for a scenario.

Well documented: If the scenario (including thermal hydraulic, (T-H) neutronics calculations, etc.) has been fully described in public or proprietary information sources, it is considered to be well documented. Such documentation, often found in plant FSARs or PRA supporting documentation, represents the reference analysis for a scenario.

Realistic: If the scenario description is consistent with how the plant really works, it is considered realistic. However, since the scenario is initially defined at the level of an initiating event, a broad range of plant behavior is represented. Consequently, the scenario description may be realistic for the whole class or for only one example within a class (and not for all of the others within the class).

Table 9.4 shows two situations for defining a base case scenario: the ideal case and less than ideal cases. This table also illustrates that the base case scenario may be defined differently for different cases, depending upon what information resources are available. Table 9.4 also provides the analysts with some options for how to develop the base case scenario when the information available is weak. Choices among these options are value judgments in which management, policy, or resources may be the deciding factors.

Figure 9.3 shows the approach for performing this step. This approach recognizes that there are preferred information sources and that these sources are not always available. The preferences are described below and summarized in Table 9.4.

The first preference is to define the base case scenario so that it corresponds with the consensus operator model. Consequently, the first task is to determine if there is a consensus operator model. If there is a COM, it should be described using appropriate plant-specific resources. If there is no COM because operators have no expectations for this scenario, the analysts should proceed to the task of identifying and describing any reference analyses.

As shown in Figure 9.3, regardless of whether there is a consensus operator model, the next task in this step is to determine if there is a reference analysis for the scenario. This task is needed, for different reasons, in both instances.

A reference analysis is needed if there is a consensus operator model because, from a thermal hydraulic point of view, such scenarios are not always well defined and documented in the open literature. For some initiating event types, a reference analysis will be provided in the plant's FSAR Chapter 14 or 15 safety analysis (although other sources, such as supporting calculations for a PRA, may be available and appropriate). The reference analysis that most closely approximates the consensus operator model should be selected for use in this step. In this instance, as shown in Figure 9.3, the descriptions of the consensus operator model and the reference analysis together comprise the base case scenario.

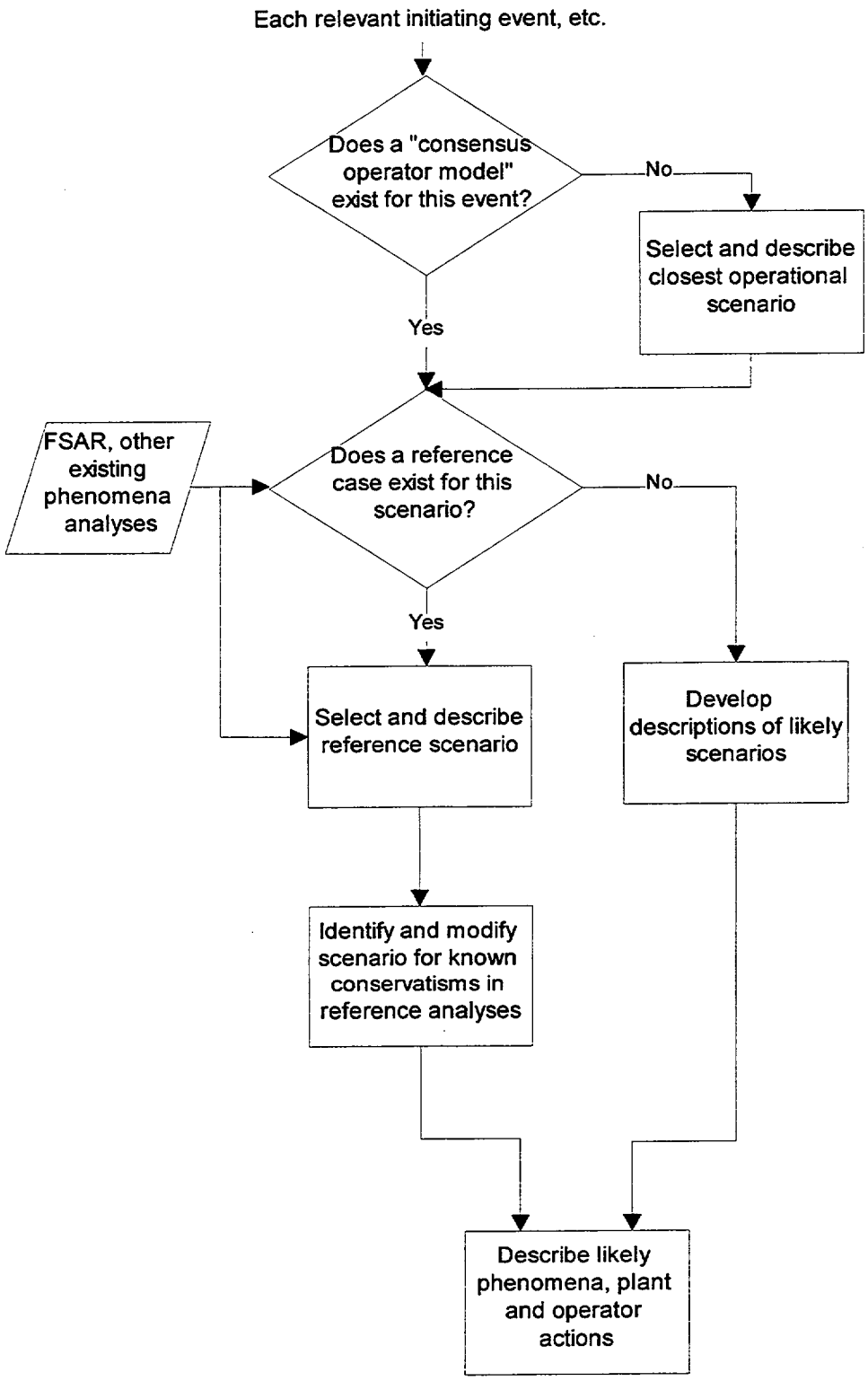


Figure 9.3 Step 3 - Describe Base Case Scenario

Table 9.4 Development of the Base Case Scenario

Example of types of Base Case[a]	Characteristics of a base case scenario					Options for Development when Information is Weak[c]
	Consensus Operator Model (COM)	Well defined Operationally	Reference Analyses		Realistic[b]	
			Well-defined Physics (T-H and neutronics)	Well documented Public or Proprietary Sources		
Ideal	Exists	Yes	Matches COM	Yes, public	Yes	N/A[d]
When the ideal is not available, another type of base case must be developed	In some cases, there may be no COM, or it may not be well-defined operationally. Examples in Appendices B–E describe some specific cases.		There may be no reference analysis that directly applies to the COM. Sometimes analyses will be available to the analysts, but not to others. Some tie to a reference analysis is needed to allow understanding and quantification of deviations from a T-H well-defined condition.		If the COM is not a realistic model of how the plant will actually respond, the operators' situation assessment is obviously flawed.	The project has many choices when the options for the base case do not include the "ideal." These include such possibilities as: 1. Judgmentally adusting the reference case to make it realistic and to make it match the COM 2. Funding additional reference case analysis 3. Selecting likely human activities, if the COM is not well defined 4. Surveying operators and trainers, if the COM is not readily apparent 5. Selecting an arbitrary base case and treating all other identifiable scenarios as deviations

[a] In all cases, a base case must be identified. The deviation analysis of Step 6 will proceed from this base case. The significance of deviations from the base case will involve evaluation of the base case and its relationship to the COM.

[b] "Realistic" should address whether it is realistic for the whole class or only one example in the class (and far off for all others).

[c] Choices among these options are value judgments, i.e., management decisions; resources or policy may be deciding factors.

[d] N/A = Not applicable.

In the instance where there are no operator expectations, reference analyses alone are used to develop the base case scenario.

As shown by the right-hand branching in Figure 9.3, in some cases there may be no FSAR analyses or other referenceable sources to approximate the consensus operator model or otherwise define a base case scenario. This often occurs for the starting events (see Step 2, Section 9.2 for definition) that are indirect causes of plant trips, such as the support system initiators and the external events. (Note that operators may not expect these events either.)

For these situations, it only may be possible to construct a base case scenario from either a most likely scenario or simply an arbitrary scenario. For such situations, the scenario description still should be realistic, based on available knowledge and expert judgment.

9.3.2 Detailed Guidance for Step 3

Figure 9.3 shows that there are five tasks that must be performed in Step 3:

(1) Identify and describe the consensus operator model.
(2) Identify and describe relevant reference analyses.
(3) If necessary, describe modifications to reference analyses.
(4) If there are no reference analyses, describe possible scenarios for the selected initiator.
(5) Describe the resulting base case scenario.

The description of the base case scenario is the end result of these tasks and is developed using existing information sources and an understanding of accident behavior. The principal sources of information needed for the tasks in Step 3 are:

- plant-specific FSAR
- other reports or documents that describe the design basis
- other plant-specific safety analyses (e.g., thermal-hydraulic analyses)
- vendor safety analyses
- plant-specific procedures [especially (EOPs)]
- vendor or generic emergency procedures
- basis documents for procedures (e.g., vendor emergency response guidelines)
- operator experience (both simulator training and actual operations)
- operator training material and its background documentation
- plant staff, especially operations, operator trainers, and those responsible for thermal-hydraulic analyses
- plant-specific and industry generic operating experience

Each of the five tasks in Step 3 is described below.

9.3.2.1 Identify and Describe the Consensus Operator Model

In order to perform this task, the analysts first should collect information from operator trainers and plant-specific operating experience to determine if there are operator expectations for the initiating event selected. Based upon the operator expectations identified, the analysts should determine if there is a consensus operator model.

If there is a COM, then the analysts should develop a description of the model using appropriate plant-specific resources. In some cases, there may be no COM, but multiple operator opinions. If this is the case, then analysts should select and describe the scenario that most closely matches (operationally) these various opinions, or define multiple base case scenarios for investigation. If there is no COM because operators have no expectations for this scenario, the analysts should proceed to the task of identifying and describing any reference analyses.

Input from operator trainers is especially important to this task since they are likely to be knowledgeable about both operational and training experience of the operating crews. If the resources allow them, interviews of operators can yield additional, useful information for this task.

9.3.2.2 Identify and Describe Relevant Reference Analyses

The reference analysis is a detailed engineering analysis of the neutronics and thermal hydraulics of a scenario. The analysts should identify the reference analyses that most closely match the consensus operator model, if one exists. If there is no COM, but multiple operator opinions, then analysts have to identify as many reference analyses as are needed to best represent the scenario or scenarios selected in the previous task. If there is no COM because operators have no expectations for this scenario, a reference analysis should be selected based upon the analysts' judgment, especially with respect to the realism of the scenario.

In describing the reference analyses, analysts should not only describe the applicable scenario but also provide appropriate citations of the referenceable information source in order to facilitate documentation and traceability. For example, if the initiator is included in the FSAR, a description of the reference case should begin by citing the applicable FSAR sections. In the description, direct quotation of the FSAR may be desirable to avoid ambiguity and to facilitate traceability.

9.3.2.3 Describe Modifications to Reference Analyses

If both a consensus operator model and a reference analysis have been identified, they should be compared to determine if the reference analyses should be modified to better represent operator expectations. Whether or not there is a consensus operator model, if the referenceable scenario information contains known conservatisms, such as FSAR analyses, these conservatisms may need to be relaxed in order to help describe an expected and/or more realistic scenario. In addition, more realistic (or likely) plant behavior and equipment interactions should be identified. Recommended

resources for performing the modifications to the reference analyses include operations staff, operator (simulator and classroom) trainers, and staff responsible for thermal-hydraulic calculations.

Particularly where it is based upon safety analyses, such as those documented in the FSAR, the reference analysis will not take credit for, nor account for, the effects of nonsafety, normally operating equipment. Generally, the consensus operator model will assume operability of both safety-related and normally operating systems. Where the operation of this nonsafety equipment does not affect the overall plant response in the scenario of interest, the consensus operator model and the reference analysis will be essentially the same, such as in the large loss-of-coolant accident example given in Appendix C. However, where the continued operability of the normally operating equipment does affect the plant response, at least to some degree, the consensus operator model and the reference analysis can be different, as illustrated in the loss of main feedwater (LMFW) example given in Appendix B. In the latter case, it will be necessary to modify any reference analysis information to fit the consensus operator model. For example, for the LMFW, most other transients, and the small LOCA, the nonsafety control systems (e.g., the condenser and atmospheric steam dumps) control the secondary and primary system thermal-hydraulic responses. The FSAR safety analysis does not include these systems, i.e., it assumes that they are not available. Therefore, in all reference analyses, the primary and secondary system parameters controlled by the steam generator steaming rate (heat removal) may be quite different than those in the consensus operator model. In other words, the base case scenario in these cases is developed from the consensus operator model and a modified version of an associated reference analysis.

9.3.2.4 Describe Possible Scenarios for the Selected Initiator (if no Reference Analysis)

As shown in Figure 9.3, in some cases, there may be no FSAR analyses or other referenceable sources to approximate the consensus operator model or otherwise define a base case scenario. This often occurs for the starting events (see Step 2, Section 9.2 for definition) that are indirect causes of plant trips, such as the support system initiators and the external events. (Note that operators may have no expectations for these events either.) These starting events are causes of standard initiating events (such as turbine trip, reactor, and small LOCA) and they complicate those initiating events by:

- disabling or degrading systems useful in mitigating the initiating event
- creating a slowly and apparently randomly degrading situation that is not part of normal design, training, and procedural expectations
- being one of many possible instances of the starting event, each leading to decidedly different event and parameter progressions, or
- creating other elements of context that can increase the likelihood of the occurrence of an unsafe act

For these situations, it only may be possible to construct a base case scenario from either a most likely scenario (based on plant-specific or generic operational experience, supplemental analysis, and judgment of trainers and analysts, if possible) or simply an arbitrary scenario (if the range of possible scenarios is too broad, as in the loss of service water example given in Appendix E). For such situations, the scenario description still should be realistic, based on available knowledge and expert judgment.

9.3.2.5 Describe the Base Case Scenario

As discussed in Section 9.3.1, the base case scenario is based upon the consensus operator model and relevant reference analyses, if both a COM and reference analysis exist. In the ideal case where both exist, then the description of the base case scenario should include:

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

As indicated above, key functional parameters should be considered in the description of the base case scenario. These are generally those functional parameters found in the EOPs and used by the operators to assess plant status and to make decisions about what actions need to be taken. Note that for a specific issue or initiator, some parameters may not be particularly relevant to identifying and analyzing possible human failure events (HFEs) associated with the issue or event. In such cases, those parameters may be eliminated from the base case description of plant behavior. However, care should be taken in eliminating any functional parameters since an unexpected response in seemingly unrelated parameters could induce interesting HFEs. Examples of key functional parameters are:

- reactor power
- turbine or generator load
- electric power

- instrument air
- service water (and similar systems)
- reactor coolant system (RCS) level and pressure
- core heat removal (e.g., T_{avg}, core outlet temperatures, subcooling margin)
- steam generator level and pressure
- containment pressure and temperature
- radiation
- ventilation
- equipment conditions (e.g., vibration, fluctuating current, high temperature, or other signs of imminent damage)
- other key parameters addressed in plant-specific EOPs

The expected operator behavior for the base case scenario is important for the use of ATHEANA. This can be determined from the plant behavior described above, a review of relevant procedures and training, and the relevant, key functional parameters. Expected operator actions should be part of what is described for the base case scenario.

9.3.3 Product of Step 3

The product of this step is a description of the base case scenario containing the information listed in Section 9.3.2. Table 9.5 illustrates how the base case scenario might be developed for examples of different situations regarding information availability. For instance, Table 9.5 provides three options for developing a base case scenario for the loss of main feedwater example. In Appendix B, the second option of adjusting the reference analyses to be more realistic and better match the consensus operator model was used. Also, Appendices B through E describe more specifically and in more detail some examples of such situations and the resulting base case scenarios.

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

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

Table 9.5 Examples of Base Case Scenario Development

Example of types of Base Case1[a]	Characteristics of a base case scenario					Options for Development when Information is Weak[c]
	Consensus Operator Model (COM)	Well-Defined Operationally	Reference Analyses		Realistic[b]	
			Well-Defined Physics (T-H & neutronics)	Well-Documented Public or Proprietary Sources		
Ideal	Exists	Yes	Matches COM	Yes, (publicly available)	Yes	Not needed
Loss of main feedwater	Exists	Fairly well defined	An FSAR scenario is probably the best choice, but it will differ from the COM	Yes, is the FSAR version used (i.e., public)	Probably not (e.g., missing control systems)	1. Use FSAR as reference case without modification, recognizing problems 2. Adjust the reference (i.e., FSAR) analyses to be realistic and match COM 3. Do new T-H analyses (or use propriety analyses) to serve as the reference
Fires, external events	No COM. Too many open-ended possibilities	No	No	Many mechanistic and PRA analyses of fires, but no single scenario	Many realistic models of fire progression; many bounding analyses of particular fire consequences.	Reasonable base cases, if not COMs: 1. Many fire PRAs assume a loss of feedwater or turbine trip initiator due to fire. 2. Earthquake PRAs often use a turbine trip as their base case, because of the seismic trip. For more severe earthquakes, loss of offsite power and LOCAs are used, depending on specific vulnerabilities.

Table 9.5 Examples of Base Case Scenario Development (Cont.)

Example of types of Base Case1[a]	Characteristics of a base case scenario					Options for Development when Information is Weak[c]
	Consensus Operator Model (COM)	Well-Defined Operationally	Reference Analyses		Realistic[b]	
			Well-Defined Physics (T-H & neutronics)	Well-Documented Public or Proprietary Sources		
Loss of service water	No	No	Partially	Partial information	For a subset of possibilities with a broad range possibilities	1. Survey operators and trainers[d] 2. Make arbitrary choice if no reference case or operator opinions.

[a] In all cases, a base case must be identified. The deviation analysis of Step 6 will proceed from this base case. The significance of deviations from the base case will involve evaluation of the base case and its relationship to the COM.

[b] In other words, the way the plant would really work. However, "realistic" also should address whether it is realistic for the whole class or only one example in the class (and far off for all others).

[c] Choices among these options are value judgments; management or policy may be deciding factors.

[d] This activity is performed as part of Step 5 to identify if there is a consensus operator model.

A "human failure event" is a PRA term that requires PRA concepts for its definition. On the other hand, an "unsafe action" is not specifically tied to a PRA, but allows the analysts to bridge the gap between human behavior and the PRA mode. Definitions for both these terms are:

Human failure event: A basic event that is modeled in the logic models of a PRA (event and fault trees), and that represents a failure of a function, system, or component that is the result of one or more unsafe actions.

Unsafe action: An action inappropriately taken or not taken when needed, by plant personnel that results in a degraded plant safety condition.

9.4.1 Guidance for Step 4

This guidance is written with the assumption that first HFEs will be identified in the ATHEANA process, then UAs. However, as noted above, iterations back to this step may require only one of these identifications. Regardless, the information and approach for the identification of HFEs and UAs, given in separate subsections, remain the same.

HFE definitions are based upon the relevance to the issue or event being addressed and the requirements for plant response to the initiating event. HFEs are typically of a functional nature (e.g., shutdown secondary cooling) and may be sufficient to address the issue identified in Step 1. Other times, it may be more beneficial to define specific unsafe actions [e.g., put LPCI (low-pressure coolant injection) pumps in pull-to-lock] in order to represent the issue of concern. In either case, these are the undesirable operator actions for which the ATHEANA process is being used to determine error-forcing contexts that may make the actions plausible or even likely.

Performance of this step requires the following inputs:

- the issue definition from Step 1
- the plant-specific PRA model, especially event trees and success criteria
- description of the base case scenario from Step 3
- (if necessary) additional knowledge and information regarding accident response, general plant design and operation, and system design and operations

9.4.1.1 Defining HFEs

To the extent the PRA is used to aid in the definition of relevant HFEs or UAs, it may be desirable to transform any systemic event trees into functional event trees if the issue definition is broad and not specific to any one system. When redefining these event trees, functions that are represented both explicitly and implicitly in the event tree should be considered, including passive plant functions. In addition, some plant functions shown as event tree headings represent more than one system (under either an AND or OR gate) and these other systems (and sometimes human actions) also should be identified and noted (or shown explicitly).

The following systematic process leads to the identification of HFEs. Some of these tasks may have been performed in the previous steps (e.g., identify the functional success criteria). Also, the selected issue may allow some of these tasks to be omitted. With these exceptions, HFEs can be identified for each function represented in the event tree for the relevant initiator by:

(1) identifying whether the function is:
- needed, or
- undesired with respect to the accident response requirements for the specific initiator or sequence

(2) identifying the system(s) or equipment that perform the function

(3) identifying the pre-initiator status of the system(s) or equipment (e.g., normally operating, standby, passive)

(4) identifying the functional success criteria for the system(s) or equipment

(5) identifying the functional failure modes of the system(s) or equipment

(6) deciding if either errors of commission, errors of omission, or both types of errors are relevant to the selected issue

(7) identifying applicable descriptions of possible human failures that can be developed into candidate human failure event descriptions

Tables 9.6 and 9.7 serve as guides for the ATHEANA analysts in performing these tasks. However, the guidance given is intended to be illustrative rather than exhaustive. Table 9.6 also contains examples of systems, given in the far right column, that may have the characteristics shown in the other columns of the table. Similarly, examples of human actions that can fail plant systems or equipment by different functional failure modes are shown in Table 9.7. Both tables should be used to trigger ATHEANA analysts' discussions on which of the examples given are applicable and on other possible success criteria, failure modes, and human failures.

Table 9.6 can be used to accomplish the first six tasks listed above. In the first column of Table 9.6, the ATHEANA analysts must identify whether each plant function in each event tree for the relevant initiator is needed or undesired. Next, the systems or equipment that perform these functions must be identified. Then, the tasks associated with the remaining columns are performed for each of these systems. In the third column, the likely pre-initiator status of each system is identified. (However, the ATHEANA analysts should remember that some initiators can change the status of systems. In such cases, the immediate post-initiator status is more relevant than the pre-initiator status.) After having determined the pre-initiator status, the ATHEANA analysts must determine the functional success criteria and functional failure modes that are appropriate for each system. Table 9.6 (fourth and fifth columns) provides examples of PRA functional success criteria and PRA functional failure

Table 9.6 Functional Failure Modes Based upon PRA Requirements[a]

Function Required in PRA? (1)	Systems that Perform Function (2)	Pre-Initiator Status (3)	Functional Success Criteria (4)	Functional Failure Modes (5)	Functional Failure Mode Category[b] (6)	Example Systems
(a) Needed		Standby	Equipment automatically actuates (short mission time)	Equipment fails to initiate or actuate automatically	1	RPS, accumulators
			Equipment automatically actuates and continues to operate for duration of mission time (longer mission times)	Equipment fails to initiate or actuate automatically	2	HPI, LPI, AFW, CS, CI
				Equipment fails to continue to operate for duration of mission time	3	
			Equipment manually actuated and continues to operate for duration of mission time	Equipment fails to be manually initiated or actuated when required	4	HPR, LPR, RHR, SDC
				Equipment fails to continue to operate for duration of mission time	3	
		Standby or Operating	Equipment manually operated as necessary to control plant parameters for duration of mission time	Equipment manually not actuated when required	4	PORVs, ADS
				Equipment fails to continue to operate for duration of mission time	3	MFW, Condesate, AFW, HPI, LPI, RCPs, CVCS, SLC
				Equipment fails to be controlled or operated as required	5	
		Passive	Equipment maintains required status	Equipment status inappropriately changed	6	
(b) Undesired		Operating	Equipment stopped and remains stopped for duration of mission time	Equipment fails to stop automatically	7	RCPs

Table 9.6 Functional Failure Modes Based upon PRA Requirements[a] (Cont.)

Function Required in PRA? (1)	Systems that Perform Function (2)	Pre-Initiator Status (3)	Functional Success Criteria (4)	Functional Failure Modes (5)	Functional Failure Mode Category[b] (6)	Example Systems
		Standby	Equipment maintains pre-initiator (or immediate post-initiator) status	Equipment fails to remain stopped for required duration Equipment fails to be stopped manually Equipment fails to maintain desired status Equipment status changes spuriously and inappropriately	8 9 10 11	SLC, SI, CI, CS

[a] Acronym's: HPI-high pressure injection; LPI-low pressure injection; AFW-auxillary feedwater; CS-core spray; HPR-high-pressure recirculation; LPR-low-pressure recirculation; RHR-residual heat removal; SDC-shutdown cooling; PORVs-power-operated relief valves; ADS-automatic depressurization system; MFW-main feedwater; RCPs-reactor coolant pumps; CVCS-chemical and volume tank coolant; SI-safety injection.

[b] Note that the numbers assigned in column 6 to the functional failure made categories provide a link to the associated rows in Tables 9.7 and 9.9a-3.

Table 9.7 Examples of Likely Human Failures and Human Failure Modes by PRA Functional Failure Mode

PRA Functional Failure Modes (5)	Functional Failure Mode Category (6)	EOC or EOO? (7)	Example Human Failures (8)	Transfer to Unsafe Action Table for Step #7
Equipment fails to initiate/actuate automatically	1	EOC	Equipment inappropriately removed from automatic control Equipment inappropriately removed from armed or standby status	Table 9.9a
	2			
		EOO	Automatic actuation fails, and no backup, manual startup	Table 9.9d
Equipment fails to continue to operate for duration of mission time	3	EOC	Equipment inappropriately terminated Equipment inappropriately isolated or aligned Equipment output and/or resources inappropriately diverted Equipment output and/or resources inappropriately depleted	Table 9.9b
Equipment fails to be manually intiated or actuated when required	4	EOC/EOO	Equipment fails to be actuated when required Equipment inappropriately actuated	Table 9.9c
Equipment fails to be controlled or operated as required	5	EOC/EOO	Equipment fails to be operated or controlled Equipment inappropriately operated or controlled	
Equipment fails to maintain desired status	6	EOC/EOO	Equipment status inappropriately changed Fails to maintain integrity Inappropriately breached integrity	Table 9.9e
	10	EOC	Equipment inappropriately operated	Table 9.9b
Equipment fails to stop automatically	7	EOC	Equipment inappropriately removed from automatic control	Table 9.9a
		EOO	Automatic stop fails, and no backup, manual stop	Table 9.9d
Equipment fails to be stopped manually	9	EOO	Equipment fails to be stopped when required	Table 9.9c
Equipment fails to remain stopped for required duration	8	EOC	Equipment inappropriately restarted (and continues to operate)	Table 9.9b
		EOO	Equipment spuriously restarts, and no backup, manual stop	Table 9.9d
Equipment status changes spuriously and inappropriately	11	EOO	Spurious actuation, with no backup stop of equipment Spurious reconfiguration, with no backup realignment	

modes associated with different types of systems of equipment based upon functional need and pre-initiator status. The ATHEANA analysts should begin by considering those functional success criteria and failure modes represented explicitly in the plant-specific PRA. In order to complete this activity, however, the analysts should try to identify additional important success criteria and failure modes. Such criteria may be implicit in the PRA model, or may be indicated in emergency operating procedures or operating practice. A review of anecdotal experience also may be helpful in these activities. Finally, the ATHEANA analysts should determine the functional failure mode categories (sixth column) applicable to each system.

Since most systems or equipment have multiple operational requirements for success (e.g., automatic actuation, continued operation for required mission time, control of operation during mission time) and therefore multiple opportunities for failure, it is important that ATHEANA users identify all of the functional success criteria and functional failure modes that apply to a specific system or piece of equipment when using Table 9.6. For example, for needed, standby systems, the ATHEANA analysts must consider all of the example functional success criteria associated with a standby pre-initiator status and the functional success criteria associated with a standby or operating initial status. However, since Table 9.6 contains some redundancy in identifying functional failure modes, the specific path for finding applicable functional failure modes is not important.

The results of the sixth column in Table 9.6 are used in Table 9.7 to perform the last two tasks listed above. With the seventh column of Table 9.7, the ATHEANA analysts can focus the remaining analysis steps on either errors of commission or errors of omission.[4] This seventh task is inserted at this point in the analysis since the issue selected for the ATHEANA HRA analysis may be limited to only certain human failure modes (e.g., only EOCs, or only EOCs and nonbackup types of EOOs). By inserting this decision point, the investigation of possible human failures can be limited to only those associated with the human failure modes that are relevant to the selected issue. The eighth column of Table 9.7 provides examples of human failures that are either EOOs or EOCs and that are categorized by the system functional failures shown in the sixth column. The ATHEANA analysts should review the examples provided in Table 9.7 to determine which are applicable for the function and system or equipment being considered. In addition, the example failures in Table 9.7 should be expanded using the ATHEANA analysts' understanding of the system or equipment design and operational features. It also is important that any ideas generated by the ATHEANA analysts regarding specific unsafe actions and associated error-forcing contexts be documented along with the results of ATHEANA steps.[5] (As noted earlier, it is possible that the recovery analysis performed in Step 8 or other steps in the ATHEANA analysis will require a human failure event to

[4]The terms "error of omission" and "error of commission" are PRA terms that are associated with different system failure modes. These terms also are useful in differentiating between human events that may already be modeled in the PRA and those that may not have been considered before. Section 1.4.2.1 provides more discussion on the usefulness of the EOO and EOC classifications.

[5] Experience suggests that the ATHEANA analysts will most easily think at the level of unsafe actions and error-forcing contexts, rather than in terms of HFEs. Consequently, thinking ahead to unsafe actions and error-forcing contexts is not discouraged, but should be documented as it occurs. In this way, such ideas will be preserved for future use while maintaining the systematic nature of the search process, which is desirable.

be decomposed into unsafe actions. If so, this decomposition will be performed in Step 8 if it is not performed in this step.)

The example human failures given in the eighth column of Table 9.7 are used to develop candidate human failure events, as defined for the plant-specific PRA. Based upon the identified, relevant human failures, several candidate HFEs are expected to be identified for each system and equipment. Using the example human failures given in Table 9.7, these HFEs should be defined in the context of the plant-specific PRA. The associated descriptions of these candidate HFEs should have one of the following general formats:

Error of omission:
*Operators fail to (*action verb for functional failure mode*) system X*

Error of commission:
*Operators inappropriately (*action verb for functional failure mode*) system X*

9.4.1.2 Defining Unsafe Actions

Because of possible differing needs for definitions of unsafe actions, multiple approaches for this task must be provided. As in the definition of HFEs, the issue of interest for ATHEANA analysis may specify an unsafe action. If such is the case, no further investigation is required for the identification of an unsafe action. On the other hand, the need for decomposition of HFEs into unsafe actions may not be recognized until recovery analysis or quantification steps are performed. The requirements imposed by these steps may even provide some indications as to what types of unsafe actions are relevant. In this case, an abbreviated process for defining an unsafe action is needed. Finally, the analysts may require a rigorous identification of all unsafe actions associated with an HFE.

For the case in which the abbreviated process is sufficient, Table 9.8 is provided to assist the analysts in identifying and defining unsafe actions. Example unsafe actions are provided for generalized equipment functional failure modes. (Table 9.8 was developed from Tables 9.9a-e which are used in the rigorous UA search approach.) The examples given are not meant to be exhaustive but merely illustrative and may help identify additional unsafe actions or functional failure modes.

Table 9.8 Example Unsafe Actions for Generalized Equipment Functional Failure Modes

Equipment Functional Failure Mode	Example Unsafe Action(s)
Failure of automatic actuation	Operators take equipment out of armed or standby status Operators change equipment configuration from armed, standby, or normal state Operators bypass or suppress automatic signals Operators disable automatic signals or sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators disable or fail equipment Operators reset signal setpoints
Inappropriate actuation	Operators actuate equipment prematurely (i.e., too soon) Operators prematurely release or unsuppress equipment automatic initiation signals Operators manually actuate equipment (when not needed) Operators manually actuate equipment automatic control
Failure to control	Operator control of equipment results in: Underfeeding or filling — Overfeeding or filling Undercooling — Overcooling Underpressure — Overpressure Reactivity decrease — Reactivity increase Integrity breach
Failure of manual initiation or actuation	Operators never actuate equipment Operators actuate equipment too late Operators release or unsuppress equipment automatic initiation signals too late Operators fail to perform backup, manual startup after automatic actuation fails (recovery)
Inappropriate termination	Operators stop (e.g., pumps stopped Operators both stop and disable equipment for future service (e.g., pumps in pull-to-lock) Operators disable or fail equipment (e.g., due to operation outside of design parameters) Operators stop and realign equipment out of required armed or standby configuration or lineup Operators stop equipment and bypass or suppress automatic signals Operators stop eqipment and disable automatic signals or sensors Operators stop equipment and take automatic signals out of armed status Operators stop equipment and reset signal setpoints
Inappropriate isolation	Operators re-align equipment (e.g., valves repositioned) Operators actuate equipment automatic isolation signals Operators actuate equipment automatic reconfiguration signals

Table 9.8 Example Unsafe Actions for Generalized Equipment Functional Failure Modes (Cont.)

Equipment Functional Failure Mode	Example Unsafe Action(s)
Inappropriate diversion or depletion of resources	Operators realign equipment (e.g., valves repositioned) Operators operate equipment outside design parameters (e.g., over RHR design pressure, resulting in flow diversion through lifted relief valves, ISLOCAs, etc.) Operators do not adequately control equipment that competes for resources before or during operation of required equipment Operators do not control equipment early in accident
Failure to terminate	Operators never stop equipment Operators stop equipment too late Operators release or unsuppress equipment automatic initiation signals for stop too late Operators fail to perform backup, manual stop after automatic stop fails (recovery) Operator fail to perform backup, manual stop after spurious start or re-start (recovery)
Inappropriate status change	Operators manually actuate or start equipment Operators manually realign equipment Operators manually override equipment automatic isolation signals Operators manually actuate equipment automatic control Operator actions (e.g., operator fails to operate or control, operator inappropriately operates or controls) from other categories result in failure to maintain integrity , inappropriately breached integrity, etc.

If the analysts cannot describe an HFE at the level of a functional failure mode (such as that given in Table 9.8), then a more rigorous approach to identifying unsafe action should be used. This more rigorous approach is performed using Tables 9.9a-e, along with links to Table 9.7, which concluded the identification of HFEs in the previous task. Tables 9.9a-e (found at the end of Section 9) allow the analysts to identify the different ways in which the operators could produce the effects characterized by the failure modes used to define HFEs. The last column of Table 9.7 guides the analysts to different tables (Tables 9.9a-e) based upon functional failure mode. (Categories of failure modes are used in the tables to make transfers between tables easier for the analysts.) Tables 9.9a-e provide example unsafe actions for different human failures. The examples given in these tables should be used in discussions or brainstorming sessions in conjunction with an understanding of design and operational characteristics of plant systems and with the plant experience (both simulator and operational), industry experience, and plant knowledge of the ATHEANA analysts to identify applicable unsafe actions and generate other possible unsafe actions. Because in some cases more than one category of functional failure mode will lead to the same example of unsafe actions, the analysts should not be overly concerned about what category leads them to the applicable examples.

Most of the example human failures and UAs result directly in a functional failure. However, the control failures (i.e., functional failure mode category 5) addressed in Table 9.9c more often involve the effect of equipment failures on plant functions. For example, undercooling in the context of the high-pressure injection (HPI) system can be the result of too little HPI flow (e.g., too few trains operated or overthrottling) or of the HPI pumps being turned off or not operated frequently enough. The dependent effects between systems and support systems (including shared resources) also must be considered. Consequently, the ATHEANA analysts also should use the following sets of guide words in identifying indirect effects of failure modes:

Examples of key plant parameters to be controlled:

- Temperature
- Pressure
- Level
- Volume
- Flow or flow rate
- Reactivity
- Subcooling margin (PWR)

Example control failures:

- Too much or little (e.g., throttling, quantity)
- Too soon or late (timing)
- Too fast or slow (rate)
- Too many or few times (frequency)
- Too short or long (duration)
- Too many or few trains (quantity and rate)
- Under or overthrottling (quantity and rate)

The ATHEANA analysts should keep in mind that there may be many different ways in which a failure mode may be activated. For example, the operator can take the following inappropriate actions:

- not use (e.g., fail to start) a system
- make it difficult to use a system (e.g., put pumps in pull-to-lock or deplete system resources)
- damage (even permanently) system equipment

The reasons an operator may do these things and the potential for eventual recovery also are different. Later steps in the process that lead to the identification of the error-forcing context address these reasons. However, as in previous steps, the analysts should document for later use any ideas generated during this step regarding reasons for UAs and EFCs.

9.4.2 Products of Step 4

The products of Step 4 include:

- a list of HFEs, and their associated descriptions relevant to the issue and for each event tree (or selected initiator) in the PRA
- (possibly) UAs associated with each candidate HFE

9.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

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

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

As illustrated by Figure 9.4, potential traps inherent in the ways operators may respond to the initiating event or base case scenario can be identified through the following:

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

Guidance for identifying potential traps using each of these approaches is given below. The individual trap searches are discussed separately, although some of these searches overlap. Finally, all of the identified potential vulnerabilities are summarized and aggregated.

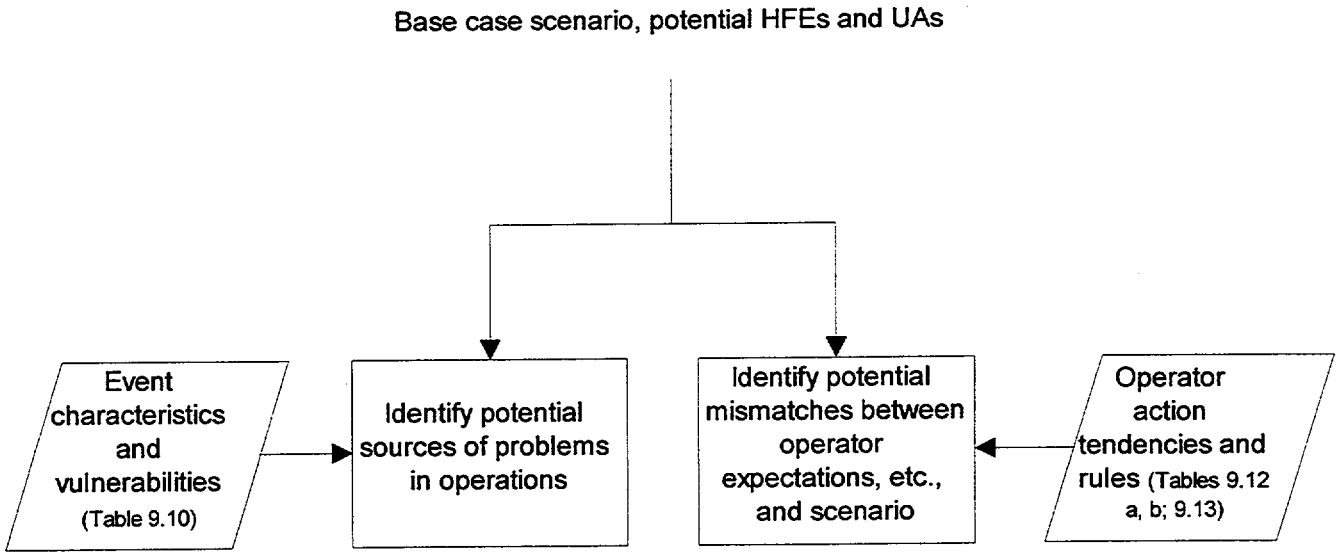


Figure 9.4 Step 5 - Identify Potential Vulnerabilities

9.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

Potential vulnerabilities in operator expectations can be anticipated by examining the characteristics of the initiating event in two different ways:

(1) with respect to operator biases that may triggered
(2) with respect to whether the initiating event is categorized as a direct or indirect initiator

Reason (Ref. 9.4) has identified two particular kinds of *heuristics*[6] having particularly powerful effects on people when they must make decisions about events, which in turn can affect the kinds of choices operators make during abnormal conditions. These are the *representativeness heuristic* and the *availability heuristic* (see the glossary for further explanations). These two heuristics lead to specific biases that affect the choices people make. The three most common biases associated with these heuristics that relate to control-room operations during abnormal conditions are:

[6]A *heuristic* is a way of mentally taking a shortcut in recognizing a situation and taking an action. Heuristics normally allow people to quickly select the most plausible choices first and the less plausible choices later.

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

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

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

In later steps, these biases can be used to help identify, for example, the more likely incorrect situation assessments where operating crews may overlook or become preoccupied with particular parameters.

Different initiating events differ with respect to how recently and frequently they are encountered and how similar they may be to recent or frequent events. As a result, different operator biases, expectations, and behaviors will be more likely than others for a specific initiating event.

Table 9.10 incorporates this recognition by indicating what potential vulnerabilities may result from different event characteristics. To use Table 9.10, analysts first should review the base case scenario defined in Step 3 and the general event or initiator type for the scenario. (Examples of general event types are shown in the right-hand column of Table 9.10.) Then, the general event type for the base case scenario should be compared with the event characteristics shown in the left-hand column of Table 9.10. More than one event characteristic may apply to a specific scenario. Next, the analysts should identify the potential vulnerabilities associated with the event characteristics that apply to the base case scenario's general event type. Potential vulnerabilities include mismatches between the actual event and operator expectations for the event, mismatches between the actual event and the rules that operators expect to apply for the event, and events for which operator knowledge is limited and rules or training do not apply. Analysts should identify possible deviations from the base case scenario that would tend toward the vulnerabilities identified from the table. Finally, the analysts should describe the vulnerabilities and possible deviations as specifically as possible, so these descriptions can help guide the deviation analysis in Step 6.

In Step 2, direct and indirect initiating events were defined and discussed. For direct initiating events, the base case event sequences that follow the initiator are generally analyzed in the FSAR with an additional failure, and other conservatisms, and thermal-hydraulic analysis may be performed in support of the plant PRA. These scenarios are straightforward, following a predictable sequence of events if there are no additional failures or interventions. Therefore, they are well supported by emergency procedures and training. The expected and essential associated human actions are generally modeled in the HRA of the PRA. These events by themselves do not pose any

difficulties in operator responses. In order for scenarios involving HFEs that are triggered by direct initiating events to become significant contributors, some significant deviation in the physics of the base case must occur. The next step in the ATHEANA analysis examines a wide range of possible deviations. Those deviant scenarios that both introduce challenging cognitive situations and have potentially reasonable frequencies of occurrence (not negligible) are passed on for further ATHEANA analysis.

Indirect initiators, on the other hand, including support system initiating events (e.g., loss of service water and loss of instrument air) and environmental events (e.g., fires, floods, and earthquakes) often have four very troublesome characteristics:

- lack of specificity as to the cause and effects of starting events
- lack of detailed engineering analysis
- ill-defined dynamic progression
- lack of directly applicable EOPs that account for the systems and dependencies introduced by such events

For example, while there are extensive analyses of seismic capacity, fire protection, cooling water requirements, etc., they are all based on design rules. That is, if an earthquake produces no greater acceleration than the designed amount, the structures, systems, and components (SSCs) are assumed to function as designed. Or, if any single active failure occurs, a sufficient amount of equipment will have sufficient cooling to provide required safety functions. Also, unlike the direct initiating events, indirect events are more stochastic in nature. Because the accident progression following indirect initiators can be ill defined and dynamic, formal procedures may not provide complete operator guidance for responses to accidents. These types of events (e.g., failures of support systems that lead to initiators) can be outside the design basis, and associated procedural guidance often does not address the underlying cause(s) of the failure. Furthermore, operators are likely to expect the most benign of scenarios following an indirect initiating event (on a frequency basis) and therefore might be unaware or unwilling to believe the severity of a serious indirect initiating event. For indirect initiators, the operators may not have any expectations, or even if they do, there are so many possibilities that there is a good chance that their expectations will not be correct. This makes these types of events troublesome and such events should be investigated further in the next step. Although the base case scenario may already be outside operator expectations, a systematic process for identifying the characteristics of important deviations should be performed in the next step to define these scenarios.

Table 9.10 Event Characteristics and Potential Vulnerabilities

Event Characteristic	Potential Vulnerabilities	Example Event Types
General event type occurs relatively frequently.	Mismatch between actual event and what operators expect; mismatch between actual event and the informal and formal rules that the operators expect to apply; because event occurs frequently, a conditioned response is possible; or, response may become routine and may not account for deviations from expected scenario	Transients
General event type is trained for relatively frequently.	Mismatch between actual event and what operators expect; mismatch between actual event and the informal and formal rules that the operators expect to apply; because event occurs frequently, response may become routine and may not account for deviations from expected scenario	Transients, LOCAs
General event type represents a wide range of possible plant behavior.	Mismatch between actual event and the informal and formal rules that the operators expect to apply; operator expectations may be different than actual event.	Transients, LOCAs, support system failures, external events
General event type is rare and/or is trained for infrequently.	Rules and training may not apply or exist; operator knowledge and experience are limited.	Support system failures, external events
General event type is rare and/or cannot be trained for realistically (i.e., no simulator training).	Rules and training may not apply or exist; operator knowledge and experience are limited	Fires, low power and shutdown.
Event type encompasses a plant-specific operational problem that occurs relatively frequently over a period of time.	Mismatch between actual event and operator expectations; because event occurs frequently, conditioned response is possible; mismatch between actual event and the informal and formal rules that the operators expect to apply (because the rules do not provide guidance in the case of an event with the operational problem).	Examples of plant-specific operational problems: feedwater control, seasonal grass intrusions in service water intake structure.
General event type often involves initiator-induced or mode-induced dependent failure of equipment response.	Rules provide limited guidance on alternatives to and how to restore needed equipment.	Fires, other external events, shutdown operations, support system failures.

Table 9.10 Event Characteristics and Potential Vulnerabilities (Cont.)

Event Characteristic	Potential Vulnerabilities	Example Event Types
General event type typically or often requires ex-control room actions (beyond alignment of shutdown cooling with RHR, etc.).	Rules may require coordination and communication of multiple people in multiple locations under adverse and unfamiliar conditions; rules provide limited guidance on alternatives to and how to restore needed equipment.	Fires, other external events, shutdown operations, support system failures, low power and shutdown events.

9.5.2 Time Frames of Interest

A review of the reference case analysis will generally reveal natural time frames for the scenario with respect to plant behavior, plant symptoms, system response, and operator response. These usually align with the following phases of the scenario:

- initial conditions or pretrip scenario[7]
- initiator and nearly simultaneous events
- early equipment initiation and operator response
- stabilization phase
- long-term equipment and operator response

A concise presentation of these natural time frames can be helpful, exposing the bases for many of the equipment success criteria and clearly identifying periods of minimal and maximal vulnerability to inappropriate human intervention. Table 9.11 presents a useful display of the time frames associated with the base case scenarios of the loss of main feedwater and large LOCA examples of Appendices B and C. A comparison of the two examples makes it clear that the actual timing of the natural phases are scenario specific and, likewise, the likelihood of HFEs in these phases.

After the analysts have prepared a table of their own time frames of interest, similar to our Table 9.11, it should be posted on their blackboard, available for constant reference during the prospective analyses of Step 6. It will be especially useful in keeping in mind the base case sequence of events, their timing and possible vulnerabilities in equipment success criteria and human responses as deviations from the base case are considered, as well as the potential for particular contexts disrupting information processing by the operators. After deviant scenarios are identified in Step 6, a comparison with the respective base case time frames will point the way to fruitful selection of HFEs, unsafe acts and error-forcing contexts.

[7] For starting event initiators, the pretrip phase may be a complex scenario itself.

Table 9.11 Relevant Time Frames for the Examples of Appendices B and C

Time Frame	Loss of Main Feedwater (MFW) Scenario, Appendix B		Large LOCA Scenario, Appendix C	
	Major Occurrences	**Influences on/by Operators**	**Major Occurrences**	**Influences on/by Operators**
Initial conditions	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention
Initiator or/ simultaneous events	Loss of MFW Reactor scram or turbine trip	Operators may identify MFW problems and manually trip the plant.	Reactor power prompt drop Pressure drops below safety injection (SI) initiation point	These events are over before the operator even recognizes what is happening
Early equipment initiation and operator response	0-2 minutes Auxiliary Feedwater (AFW) start SG pressure control per blowdown Other auto equipment responses	Operators verify initial responses per EOPs; particularly, AFW start in this case. Operators may even manually start AFW before it auto starts.	0-20 seconds Break flow is complete Pressure drops to essentially zero Containment pressure has peaked and is falling ECCS flow begins Accumulator flow occurs	During this time frame the operator is checking parameters and ensuring that appropriate standby equipment has started. Some early decisions in the EOPs may have occurred.
Stabilization phase	2 minutes - 1 hour Heat sink restored (SG levels and pressure) Plant conditions restabilize Some throttling and shutting down of equipment (e.g., AFW) begins	Operators likely to throttle and even shut down some AFW pumps to avoid overcooling or respond to lack of cooling (& enter other EOPs) if heat sink apparently not restoring. Perform other actions as necessary (e.g., pressurizer heater on or off) to keep plant stabilized.	1-3 minutes Core reflood begins at about 30 seconds and has reached stable conditions Fuel temperatures have peaked and are falling	During this time, the operators have moved into the LOCA EOP and have passed a number of decision points.
Long-term equipment and operator response	>1 hour Unnecessary equipment shutdown Achieve hot or cold shutdown	Operator shuts down unnecessary equipment and transitions plant to hot or cold shutdown.	Isolation of the accumulators Shift to cold leg recirculation cooling Shift to hot leg recirculation cooling Repair and recovery	During the 20 minutes until switchover to cold leg recirculation cooling, the operators are occupied with confirmatory steps in the EOPs. Any complications beyond the base case scenarios can affect their performance. This longer time frame extends to days and months. There are no critical operations concerned with the base case scenario. Problems during this phase would be the concern of a low-power and shutdown PRA.

9.5.3 Operator Tendencies and Informal Rules

Tables 9.12a and 9.12b show the typical, required types of actions (called "operator action tendencies") for off-normal conditions of key functional parameters typically used to determine plant status. These operator action tendencies are based on the formal emergency and abnormal operating procedures and related training that is received, as well as informal practices and rules that are also part of the operator psyche. In Table 9.12a, a representative summary is provided, based on a review of typical pressurized water reactor (PWR) emergency procedures. The table should be useful for most PWRs. Table 9.12b provides a similar summary for boiling water reactors (BWRs). However, since the operator action tendencies shown in these tables should be considered generic, plant-specific rules should be reviewed to verify and supplement these actions.

In considering operator tendencies, the analysts should identify those tendencies that may lead to the HFEs or UAs of interest and the corresponding plant conditions that may lead to those tendencies. The plant conditions can therefore potentially set up the operators to follow the tendencies and so should be examined as part of the next step in the ATHEANA process.

In addition, in this step, the analysts should identify any informal rules that may be relevant as possible contributing factors to inducing the HFEs or UAs of interest. For example, an informal rule may exist among the operating staff that a certain indicator should not be trusted since it often sticks and thus reads incorrectly during dynamic situations. If the analysts can identify a way that following this or other informal rules could contribute to an error-forcing context that might induce an HFE or UA, this should be identified as a potential vulnerability and examined further in the next step of the process.

Table 9.13 provides examples of informal rules to assist the analysts in identifying such rules for their specific plant. The examples are broken down into three categories of possible operator activity: plant interventions (e.g., selection of unsafe actions), information processing (e.g., monitoring), and understanding of plant conditions and configurations (e.g., equipment status). The possible source of the informal rule (e.g., training, experience) is shown. The examples indicate what aspects of the operators' knowledge base may be the source of an informal rule. Consequently, the possible sources can guide analysts in discovering (probably through interviews of operators and operator trainers) what informal rules may be used.

9.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

The evaluation of formal rules and emergency operating procedures begins by tracking those elements of the EOPs (or other formal rules) that are most relevant to the scenario. (See Ref. 9.5 for a related approach.) A flowchart or logic diagram format can be used to accomplish this tracking, distinguishing between procedure steps in which decisions are made and steps where actions,

Table 9.12a Summary of Operator Action Tendencies (PWRs)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Plant Level: Reactor power	Too high or increasing	Rods in or Emergency borate (inject)
Turbine/generator load	Not tripped	Trip / Run back /close main steam valves
Key Supports: Electric power	Partial or total loss	Restore (use emergency diesels if necessary) or realign
Instrument air	Partial or total loss	Restore or realign
Cooling water systems	Partial or total loss	Restore/realign/augment
Reactor Coolant System (RCS) (primary): Pressurizer (RCS) level	Too low or decreasing	More RCS injection or less letdown
	Too high or increasing	Less/stop injection or more letdown
Pressurizer (RCS) pressure	Too low or decreasing	More RCS injection / isolate possible LOCA paths / stop pressurizer sprays and turn on heaters / decrease cooldown
	Too high or increasing	Turn on pressurizer sprays and turn off heaters / increase cooldown / provide relief with pressure operated relief valves ((PORVs), vents)
Core heat removal (e.g., T_{avg}, core outlet temps, subcooling)	Too low or decreasing (insufficient)	Increase RCS forced flow (unless voiding evident) / more RCS injection / increase cooldown
	Too high or increasing (overcooling)	Decrease RCS forced flow / less/stop injection / close any open PORVs/vents / decrease cooldown
Steam Generators - S/G (secondary): S/G Level	Too low or decreasing	More S/G feed (i.e., increase cooldown) / use feed and bleed
	Too high or increasing	Less S/G feed (i.e., decrease cooldown) / possible isolation of main steam
S/G Pressure	Too low or decreasing	Decrease steam dump (i.e., decrease cooldown) / isolate (especially if high radiation indicative of tube rupture)
	Too high or increasing	Increase steam dump or provide main steam relief (i.e., increase cooldown)
Containment: Containment pressure	Too high or increasing	Increase fan cooling / isolate containment / containment spray
Containment temperature	Too high or increasing	Increase fan cooling / isolate containment / containment spray
Radiation	Indicating	Isolate source or area

Table 9.12a Summary of Operator Action Tendencies (PWRs) (Cont.)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Ventilation	Too little or rising temperature	Regain / open doors/ use portable equipment
Other: Equipment condition	Signs of imminent damage (vibration, fluctuating current, high temperature)	Shut down or isolate

[a] This is defined relative to what is expected at the time in the scenario when the operator is responding to the functional parameter of interest. Note that the operator may respond to a parameter early in the event and again later in the event and so forth. The expected absolute reading or trend of the parameter could be different for the early and later responses. The off-normal condition is defined relative to each expectation at each time.

[b] It is recognized that the specific actions will depend on the absolute reading and rate of change in the parameter and the specific procedural guidance for the conditions observed. These are, however, the typical types of actions that are called out to be performed, depending on the specific circumstances.

Table 9.12b Summary of Operator Action Tendencies (BWRs)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Plant Level: Reactor power	Too high or increasing	Rods in / emergency borate/ level-power control
Turbine or generator load	Not tripped	Trip / Run back / close steam valves
Key Supports: Electric power	Partial or total loss	Restore (use emergency diesels if necessary)/realign
Instrument air	Partial or total loss	Restore or realign
Cooling water systems	Partial or total loss	Restore/realign/augment
Reactor Pressure Vessel: Level	Too low or decreasing	More vessel injection / depressurize /vessel flooding/ isolate containment / containment flooding
	Too high or increasing	Reduce feedwater or less-stop injection
Pressure	Too high or increasing	Provide relief (turbine bypass, safety relief valves (SRVs)...)

Table 9.12b Summary of Operator Action Tendencies (BWRs) (Cont.)

Key Functional Parameter(s)	Off-Normal Condition[a]	Operator Action Tendencies[b]
Containment: Suppression pool temp.	Too high or increasing	Suppression pool cooling sprays or depressurize
Suppression pool level	Too high or increasing	Use pool drains / terminate external injection / depressurize
	Too low or decreasing	Provide pool makeup or depressurize
Drywell pressure	Too high or increasing	Isolate LOCA and containment / drywell spray / venting / depressurize
Drywell temperature	Too high or increasing	Increase drywell cooling / drywell spray / depressurize
Radiation	Indicating	Isolate source/area / depressurize
Ventilation	Too little and/or rising temp	Regain / open doors/ use portable equipment
Other: Equipment condition	Signs of imminent damage (vibration, fluctuating current, high temperatue)	Shutdown / isolate

[a] This is defined relative to what is expected at the time in the scenario when the operator is responding to the functional parameter of interest. Note that the operator may respond to a parameter early in the event, and again later in the event, and so forth. The "expected" absolute reading or trend of the parameter could be different for the early and later responses. The off-normal condition is defined relative to each expectation at each time.

[b] It is recognized that the specific actions will depend on the absolute reading and rate of change in the parameter and the specific procedural guidance for the conditions observed. These are, however, the typical types of actions that are called out to be performed depending on the specific circumstances.

monitoring, or verification is performed. Examples of such flowcharts are contained in Appendices B through E. Note that this simplified flowchart is not meant to duplicate the EOPs. However, it does highlight:

- the location of branch points from the most applicable procedure to other procedures
- where specific steps exist that call for stopping equipment that is particularly germane to the scenario
- where a major reconfiguration of equipment is called out

The EOPs or other formal rules define the expected responses the operators will take, depending on the scenario progression. However, the above points in the EOPs could be particularly vulnerable to operator error so that a "wrong" procedure is entered, or equipment is shut down or reconfigured inappropriately. Therefore, at each decision point or where otherwise deemed beneficial, information is provided that summarizes the following to provide clues as to possible pitfalls:

Table 9.13 Examples of Informal "Rules" Used by Operators

How operators use rules	Informal[a]	
	Training	**Other Sources of Informal Rules**
Plant Interventions		
Selection and justification of unsafe action(s)	Keep core covered Always follow your procedures Don't go solid in pressurizer	Good Practice Protect pumps (e.g., stop if no lube oil pressure, no cooling, runout, deadheaded, cycling) Old Practice Safety injection (SI) on low pressurizer level Folklore A good operator always beats autoactuation Never feed water into an overheated vessel Conflict Alternatives have negative consequences Success seems imminent
Information Processing		
Monitoring[b] (i.e., what indications to monitor, when to monitor, etc.)	Which instruments to use Which (and in what order) to respond to alarms Check redundant indications (especially alarmed conditions)	Experience Which instruments to use (may not be all that are available)
Interpretation (part of situation assessment)	Believe your indications	Good practice Question diagnoses (e.g., if unexpected response, restore your last action) Experience (plant-specific) Some indications are more reliable than others. Some indications always give false readings. Recent history of plant/equipment/instrument performance
Understanding Plant Conditions and Configurtions		
Equipment status	Indications of performance. Believe your tagout system	Folklore Pumps in runout overspeed Multiple failures in one system are not possible

Table 9.13 Examples of Informal "Rules" Used by Operators (Cont.)

How operators use rules	Informal[a]	
	Training	Other Sources of Informal Rules
Instruments/indications	Instruments are very reliable	Folklore Indication readings correspond directly with actual plant state or behavior Indications are independent

[a] Including training, guidance for good operating practice, old practice (i.e., previous operating practice), experience, invented rules of thumb (referred to as "folklore").

[b] Including both data-driven and knowledge-driven monitoring.

- actions to be taken
- potential for ambiguity
- a judgment on the significance of taking the wrong branch or inappropriate action.

Existing EOP flowcharts may be used or extended for the purposes of this activity. For example, some vendor emergency guidelines, which form the basis for emergency operating procedures, contain procedure flowcharts. Also, similar diagrams may have been developed as part of previous PRA or HRA efforts (e.g., Refs. 9.5, 9.6). Since development of these flowcharts may be time-consuming, use of existing work is preferable. Unless the procedures are changed, the flowcharting has to be done only once.

9.5.5 Product of Step 5

The product of Step 5 is a summary or aggregation of the information collected in this step. As we proceed into the searches of Step 6, the analysts keep all of this information at hand, i.e., on their blackboard, available for ready reference at each stage of the searches. Using this information, the analysts can identify potential vulnerabilities. In turn, the analysts can use these potential vulnerabilities as guides to the more fruitful aspects to search when developing deviations from the base case scenario in the next step.

9.6 Step 6: Search for Deviations from the Base Case Scenario

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

9.6.1 Overview of Step 6

The search schemes in this step guide the analysts in finding physical or "physics" deviations. These are real deviations in plant behavior and conditions. In contrast, deviations in perceived plant behavior and conditions, whether due to indicator failures or failures in operator perception, are addressed in Step 7. Analysts may identify performance-shaping factors (PSFs) and explanations for human behavior (e.g., error mechanisms) along with these plant conditions. The combination of plant conditions (including the deviations), along with resident or triggered human factors concerns, defines the error-forcing context (EFC) for a human failure event that is composed of one or more unsafe actions. The next step, Step 7, builds upon or refines this initial EFC definition by identifying other possible complicating factors (including possible hardware failures) and resident or triggered human factors concerns (e.g., mismatches between deviant plant behavior or conditions and procedures or other job aids).

There are three possible outcomes from this and the next step that would result in scenarios and EFCs that are passed on for further analysis in the recovery and quantification steps:

(1) The EFC is strongly defined by physical deviations (i.e., Step 7 is not needed to define the EFC).

(2) The physical context is reasonably strong, but the frequency is low. However, there are similar scenarios with higher frequencies.

(3) The physical context is not severe enough to make the HFEs or UAs likely, but additional factors (such as additional hardware or indications failures identified in Step 7) could create an EFC.

Figure 9.5 illustrates the tasks and task flow for this step. Four search schemes are used to identify characteristics that should be contained in a deviation scenario:

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

(2) Evaluate rules with respect to possible deviations

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

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

After each of the search schemes has been exercised, the analysts should review and summarize the characteristics of a deviation scenario (or potentially important deviations) that were identified in the searches. With these combined results, the analysts then develop descriptions of deviation

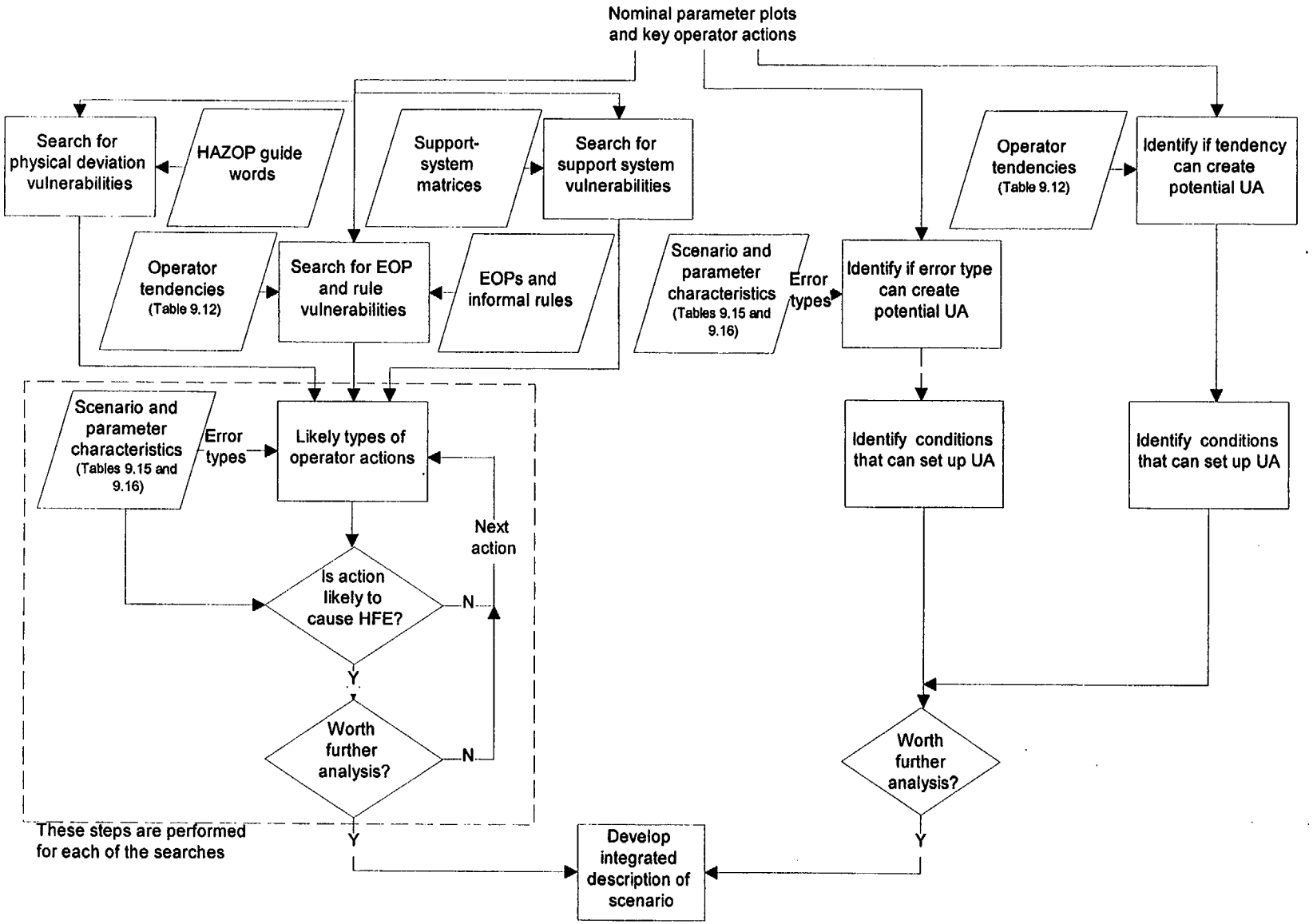


Figure 9.5 Step 6 - Search for Deviations from Base Case Scenario

scenarios and associated HFEs or UAs. These deviations also become the initial error-forcing contexts for the HFEs or UAs.

The search schemes are not wholly independent. In general, all search schemes should be tried, and in the order given above. However, the different schemes are not equally fruitful for different classes of initiating events (or for direct versus indirect initiating events). Because of built-in redundancies in the search schemes, the fourth search, or "operator tendencies and error types" search, can be viewed as a sort of catch-all search that may identify deviations that eluded the previous searches. Also, the first three searches identify plant conditions and rules (i.e., aspects of the plant) that are deviation characteristics first, then try to identify possible error types or operator tendencies (i.e., aspects of the human) that are associated with these characteristics. In the fourth search, the approach is reversed; possible error types and operator tendencies that could cause HFEs or UAs of interest are identified first, then the plant conditions and rules associated with such inappropriate operator responses are identified. A happy consequence of the redundancies in the search schemes is that analysts should not be surprised if the same deviation characteristics are identified using different search schemes or if different analysts find the same or similar deviations using different search schemes.

Each of the four search schemes for identifying physical deviations is described below. However, the common tools or resources that underlie these schemes are described first.

9.6.2 Tools Underlying the Search Schemes

As noted above, the four search schemes for identifying physical deviations are not independent. Part of this dependency, or redundancy, is by design to help the analysts in identifying significant deviations. Variations in how the search schemes are applied (see Appendices B through E for examples) also account for some of this dependence. Finally, the same tools or information underlie all four schemes, although they are used differently in the different schemes.

These tools or information resources are:

- the identified potential vulnerabilities from Step 5
- EOP flowcharts
- operator tendencies
- informal rules
- support system dependencies
- human information processing tendencies or characteristics
- familiarity with thermal-hydraulic response

The use of EOP flowcharts, operator tendencies, and informal rules was introduced in Step 5. The identification of physical deviations performed in this step expands upon those tasks. Understanding of plant thermal hydraulics also was important to the performance of previous steps (as well as

previous PRA studies). The two other tools are new to the process. The investigation of support system dependencies is an extension of that which has been performed for many PRAs already. The investigation of human information processing tendencies allows the potential for human vulnerabilities to guide the analysts to physical deviations that may be particularly troublesome for operators.

9.6.3 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

Three tasks are performed in this first search:

(1) Guide words are used to identify and define how the scenario may deviate from the base case.

(2) Relevant EOPs are checked for technical validity for the identified deviations.

(3) Possible error types or inappropriate operator response are identified by matching the plant conditions associated with identified deviations.

The example analyses given in Appendices B through E can be used as a guide for performing this search.

This first search begins by using guide words to identify and define how the scenario may deviate from the base case, thereby causing complexities that may contribute to EFCs. While the focus of this search is on deviations from the initiator in the base case, the analysts should not limit this search if deviations associated with subsequent accident responses are discovered. The use of guide words is common in other types of safety investigations, especially HAZOPs (HAZard and OPerability studies) performed in the chemical processing industry (see, for example, Ref. 9.7). Since the guide words are used only to stimulate the analysts' thinking, it is not particularly important how or by what guide words deviations are identified.

The following is a list of suggested guide words that seem appropriate for the identification of physical deviations and a very basic interpretation of each guide word:

Guide Word	Meaning
No or not	A deviation that negates the base case scenario
More	A deviation that represents a quantitative increase
Less	A deviation that represents a quantitative decrease
Late/never/early	A deviation that represents a change in expected timing
Inadvertent	Same as "as well as"
Too quick/slow	A deviation that represents a change in the expected speed or rate
Too short or long	A deviation that represents a change in the expected duration
As well as	A deviation in which something in addition to the base case occurs
Part of	A deviation in which only some of what is expected occurs

Reversed	A deviation that is the logical opposite of the base case
Repeated	A deviation that represents a repetitiveness of what is expected

Note that this list is degenerate for some scenarios (e.g., under LLOCA IE "more" = "early" = "quick" = "short"). Also, the analysts are likely to find that a short set of guide words is easiest to use.

Considering the potential vulnerabilities identified in Step 5 (Section 9.5.1), the analysts should apply the suggested guide words to the initiating event or the scenario as a whole to determine whether changes in the initiator or scenario (i.e., deviations) could result in operator actions relevant to the HFEs or UAs of interest. Illustrations of how these guide words are applied are shown in the example analyses in Appendices B through E. In applying each guide word, the analysts identify how the initiator or overall scenario could be different from the base case (i.e., a possible deviation) as suggested by the guide word, as well as the potential significance of each deviation. Based on their reasonableness and potential significance, those deviations that could seemingly contribute to an overall context that might induce the HFEs or UAs of interest are reviewed even further.

For the physical deviations that are identified, the analysts then should ask if the deviation could be caused by a single operator activity, particularly a "slip"or "lapse" that is difficult to recover or is unrecoverable.[8] Such actions may be caused by traditional human factors problems (e.g., human–system interface) or by operators misreading or misinterpreting indications. Regarding the misreading or misinterpretation failures, such misperception failures should not occur unless:

- the scenario progression is fast or confusing
- something about the misperception breaks down the team concept, encouraging independent action
- some other aspect of context has already broken down team communication
- confusion about the current state of the plant exists and one operator's misperception (or misdiagnosis) is accepted by all team members (see, for example, the Crystal River 3 event in Appendix A)

In addition, analysts may find the examples of psychological reasons for response implementation failures given in Table 9.14 generally helpful. The discussions given in Sections 4.1.4 and 4.3.4 also may be helpful in identifying possible slips or lapses and their justifying causes.

[8] Equipment can be defined as unrecoverable if it cannot be actuated in the time available because it is locked out, disabled, irreparably damaged by the operator action, or otherwise precluded from operation by conditions following the operator action. The identification of unrecoverable failures will rely upon the analysts' knowledge of scenario timing and hardware and system design, dependencies between systems and equipment, operator controls, etc.

After the characteristics of deviations have been identified using the guide words, the analysts should evaluate these, characteristics against relevant procedures to identify whether strict compliance with the procedures and the formal rules (rules defined in training as part of the expected response strategy for the scenarios) will lead to any HFEs because of timing or parameter-value mismatches with the assumptions in the procedures. If no mismatches are identified from the evaluation, then the procedures are technically correct. If mismatches are identified, the procedures are **not** technically correct. Such mismatches should be analyzed in a later step as an initial EFC (although analysts should complete the remaining searches in this step to identify other potentially significant deviations).

Finally, the analysts should identify which UAs and HFEs of interest are supported by the deviation characteristics identified. For each deviation characteristic identified with the guide words, the analysts should review Tables 9.12a or 9.12b (from Step 5), Tables 9.15a and b (scenario characteristic tables), and Tables 9.16a and b (the parameter characteristic tables). While the results obtained using these tables are similar, the structure and content of the tables are different. Consequently, the reviews of Tables 9.12, 9.15, and 9.16 are described separately below. Note that Tables 9.15 and 9.16 are found at the end of Section 9. A discussion of the underlying basis for the use of these tables is presented in Section 4.4.

Table 9.14 Failures in Response Implementation

Failures in Response Implementation	Search Questions to Identify EFC elements
Operators use incorrect indications, displays or controls	
• Displays separated from controls	Under what plant conditions must operators use controls that are separated from the related parameter displays and indications?
• Relevant displays and controls not easily identifiable (particularly ex-control room)	Under what plant conditions must operators use displays or controls that are not easily identifiable, such as being limited to a small number of CRTs or using poorly labeled local indicators or controls? Under what conditions are operators called on to use indicators or controls where the labels are unclear or wrong?
• Controls normally used in other contexts with other displays	Under what conditions must operators use indicators or controls that are located among similar-looking groups? Can the operators be required to use controls that are usually used in different operational contexts? In these cases it is possible for operators to inadvertently use the controls in the way that is normal for these other contexts but that is inappropriate under the accident conditions.

Table 9.14 Failures in Response Implementation (Cont.)

Failures in Response Implementation	Search Questions to Identify EFC elements
Operators use controls or read displays incorrectly • Controls operate in nonstandard manner • Displays have non-standard scales or display modes	Under what plant conditions must the operators use controls that have non-stereotypical operating modes? • "On" or "open" to the left • "Up" or "increase" to the left Under what plant conditions must the operators use displays that have nonstereotypical indicating modes? • "Up" or "increase" to the left Under what plant conditions must the operators use displays that have multiple display ranges? Under what plant conditions must the operators use displays that have multiple display modes (e.g., CRT displays)?
Multiple operators unable to perform task • Operators not available • Coordination not available or ineffective • Communications not effective between operators	Under what plant conditions can there be insufficient operators available to perform all the necessary tasks? • Operators performing other tasks Under what plant conditions can the response coordinator be preoccupied with performing other tasks? For what plant conditions can the coordinator be insufficiently trained? Under what conditions can the communication system be inoperable? Under what plant conditions can the communication system be unavailable? Under what conditions can the communication system be ineffective? • Blackout spots • High ambient noise Under what conditions can nonstandard or ineffective language pose a particular problem in operations (e.g., similar-sounding names and equipment numbers)?

In Tables 9.12a and 9.12 b (for PWRs and BWRs, respectively), key functional parameters and off-normal conditions in these parameters are related to operator action tendencies. The analysts should match each deviation characteristic with the affected functional parameters and off-normal conditions that best describe the deviation. Once a match is identified, then the tables show the analysts what operator tendencies are possible. Finally, the analysts should determine if the identified operator tendencies represent HFEs or UAs that are relevant to the issue of interest.

In Table 9.15a, descriptions of the scenario are related to categories of scenario characteristics. The analysts should match each deviation characteristic identified earlier in this step with the scenario descriptions that best describe the deviation. If a match is identified, then the analysts can use Table 9.15b to identify what error types are possible. In turn, the analysts should determine if any of the identified error types correspond to any of the HFEs or UAs that are relevant to the issue of interest.

Finally, the analysts should identify what error mechanisms are associated with the relevant error types. From the possible error mechanisms, the analysts should try to determine which error mechanisms might be applicable for the HFE or UA, associated plant conditions, and specific plant. (The analysts may find themselves thinking ahead to additional plant conditions, PSFs, informal rules, or other plant-specific features that might activate certain error mechanisms. Step 7 specifically addresses consideration of PSFs and additional plant conditions. As always, such thinking ahead is encouraged.)

Similarly, in Table 9.16a, questions to identify parameter characteristics relevant to the scenario are provided for three of the four information processing stages.[9] These parameter characteristics could have particular influences on operators and whether a UA may result. The analysts should review the parameter characteristics and associated questions for all three of the information processing stages addressed in Table 9.16a to determine which parameter characteristics or information processing stage best describes the above-identified deviation characteristics. If a match is identified, then the analysts can use Table 9.16b to identify possible error types for the parameter characteristic and associated information processing stage. Next, the analysts should determine if the identified error types correspond to any of the HFEs or UAs that are relevant to the issue of interest. Finally, the analysts should identify what error mechanisms are associated with the relevant error types. From the possible error mechanisms, the analysts should try to determine which error mechanisms might be applicable for the HFE or UA, associated plant conditions, and specific plant. Several aspects of Tables 9.15a and b and 9.16a and b should be noted. These tables provide analysts with a set of error types and mechanisms that may be relevant, given certain scenario characteristics, and provide some guidance for identifying (in Step 7) which PSFs may be particularly relevant when certain scenario characteristics and error mechanisms are likely to be operative. There is no assumption that the tables are all encompassing or that there are necessary and precise relationships among their elements. For example, it is not necessarily the case that a particular error mechanism will be associated with an identified characteristic or that a particular PSF will be related to a certain error mechanism. Thus the tables are to be used as guidance for possible factors and relationships to be considered rather than a specification of the precise relationship among factors.

9.6.4 Search of Relevant Rules

Paralleling the first search, three tasks are performed in this second search:

(1) Decision points in relevant formal and informal rules are evaluated against the deviations identified in the first step.

(2) Relevant EOPs are checked for technical validity for the identified deviations.

[9] It is assumed that the impact of parameter characteristics on the operators would be negligible during the fourth stage, response implementation.

(3) Possible error types or inappropriate operator responses are identified by matching the plant conditions associated with identified deviations.

Because the second and third tasks in this second search are identical to those performed in the first search, a description is not repeated here. The example analyses given in Appendices B through E can be used as a guide for performing this search.

This second search begins by duplicating the evaluation performed in Step 5, Section 9.5.4. However, in this case, decision points in relevant formal and informal rules are evaluated against the deviation characteristics identified in the first search of Step 6, rather than the base case scenario. The analysts also should identify plant conditions that represent deviations from the base case scenario that might trigger the use of formal or informal rules in ways that would lead to unsafe actions.

9.6.5 Search for Support System Dependencies

Paralleling the first two searches, three tasks are performed in this third search:

(1) Dependency matrices are reviewed and expanded to identify support system failures that also could lead to the deviation characteristics identified in the previous searches.

(3) Relevant EOPs are checked for technical validity for the identified deviations.

(3) Possible error types or inappropriate operator responses are identified by matching the plant conditions associated with identified deviations.

Because the second and third tasks in this search are identical to those performed in the first search, a description is not repeated here. The example analyses given in Appendices B through E can be used as a guide for performing this search.

The accident record has shown that serious events can be influenced by support system dependencies. For example, the event at TMI-2 was initiated by the closure of FW valves which, in turn, was caused by moisture intrusion in the instrument air system. Consequently, one potentially useful method of searching for plant conditions that produce error-forcing contexts is to investigate dependencies between support systems and both frontline safety systems and normally operating systems.

The significance of such dependencies is twofold:

(1) If the system or function failure that resulted in the reactor trip also is required post-trip, a complicated or unexpected support system dependency influence may complicate or delay operator response.

(2) The support system failure that ultimately caused the reactor trip may cause additional failures in responding systems (e.g., safety systems) that are complicated, unexpected, and difficult to diagnose, thereby affecting operator response.

Many IPEEEs and PRAs included dependency matrices as part of their documentation. Using and expanding upon these dependency matrices may be an effective way for investigating support system dependencies. For front-line safety systems, such dependency matrices may be sufficiently complete if they go down to the component level. However, dependencies between support systems and normally operating systems may not be addressed. So the analysts would need to expand the existing dependency matrix to include those component failures in normally operating systems that could be caused by support system failures. Probably the only normally operating systems that need to be added are those that, if failed, would require the reactor to trip.

Once the support system dependencies are identified, the analysts investigate what possible events might have resulted in the support system failure. In particular, the analysts should identify those failure causes that could have widespread effects on not only the system that failed and caused the reactor trip but also on frontline safety systems that are required for accident response.

As in the physics search described in Section 9.6.3, the analysts should investigate if there are any unrecoverable slips or lapses that could cause the plant conditions associated with the deviation characteristics identified through this search.

9.6.6 Search for Operator Tendencies and Error Types

As mentioned in Section 9.6.1, this fourth search is conducted essentially in reverse, compared with the first three searches. In other words, the first three searches identify plant conditions and rules (i.e., aspects of the plant) that are deviation characteristics first, then try to identify possible error types or operator tendencies (i.e., aspects of the human) that are associated with these characteristics. In this fourth search, the approach is reversed; possible error types of operator tendencies that could cause HFEs or UAs of interest are identified first, then the plant conditions and rules associated with such inappropriate operator responses are identified. This fourth search also can be considered a sort of catch all for deviation characteristics that might have eluded the previous searches.

This fourth search consists of two tasks:

(1) Operator tendencies that match HFEs or UAs of interest are identified
(2) error types that match HFEs or UAs of interest are identified.

In both tasks, the final activity is to identify the plant conditions and rules that can lead to the relevant tendencies and error types that are identified.

In addition, this search uses the tendencies and vulnerabilities uncovered in Step 5 and searches for deviations that would trigger those tendencies that would result in unsafe actions for the scenario.

As in the previous searches, the example analyses given in Appendices B through E can be used as a guide for performing this search.

First, the operator tendencies shown in Tables 9.12a or 9.12b (for PWRs or BWRs, respectively) should be reviewed. The tendencies that are relevant to HFEs or UAs of interest should be identified. For the relevant tendency (or tendencies), then look at Table 9.12a or 9.12b to find what key functional parameters and associated off-normal condition(s) correspond with the tendency (or tendencies). The analysts may need to translate these functional parameters and off-normal conditions, which are stated in generalized plant terms, into more specific conditions that relate to the scenario being examined. Then the analysts should try to identify how the plant conditions could be created so that the operator tendency (tendencies) is activated. The plant conditions specific to the scenario being investigated, and how these conditions are created, describe a deviation from the base case scenario that could lead to the tendency (or tendencies) of interest.

The search for error types is conducted in a similar way. First, the error types column in Tables 9.15b and 9.16b are reviewed. This review should focus on identifying any error types that match any of the HFEs/UAs of interest and that have not already been identified in the previous deviation searches in Sections 9.6.3, 9.6.4, or 9.6.5. For matches, the error mechanisms associated with the relevant error types should be identified. Next, the associated description of plant behavior (in the leftmost column of Tables 9.15b and 9.16b) should be identified. In the case of Table 9.15a, the generalized plant behavior is categorized by scenario characteristics. For Table 9.16b, generalized plant behavior is categorized by parameter characteristics. In both cases, the analysts should use these categories of characteristics in Tables 9.15a and 9.16a, respectively, to identify a general description of the scenario deviation. In Table 9.15a, a scenario description is used to generally describe the important scenario deviation. Using these general descriptions, the analysts should try to identify what realistic deviations from the base case scenario (in terms of both plant conditions and rules) could cause the plant behavior described in the leftmost column of Table 9.15a.

Such deviations also must lead to the associated error type given in Table 9.15b. In Table 9.16a, questions associated with the parameter characteristics are provided to lead the analysts to relevant deviations. The analysts should use these questions try to identify what realistic deviations from the base case scenario (in terms of both plant conditions and rules) could cause the plant behavior described in the leftmost column of Table 9.16a and the associated error type given in Table 9.16b. If plant conditions are identified, then the analysts should try to identify which of the possible error mechanisms might be activated for the relevant error types. (As in Section 9.6.3, the analysts may find themselves thinking ahead to what additional plant conditions, performance-shaping factors, etc. might activate error mechanisms, as well. Such thinking ahead is encouraged.) Table B-6 illustrates how this search for error types might be documented.

9.6.7 Develop Descriptions of Deviation Scenarios

In this task, descriptions of deviation scenarios are developed from the characteristics of deviation scenarios found in the four searches described above and guided by the potential vulnerabilities

identified in Step 5 (i.e., the information on the blackboard).

The analysts first should summarize all of the characteristics found in the four searches. These represent elements of error-forcing contexts (i.e., plant conditions, perhaps some PSFs, and supporting explanations for operator behavior associated with contextual elements).

Then the analysts should develop a scenario description that significantly deviates from the base case scenario and that would lead to the HFEs or UAs of interest. In order to develop the deviation scenario, the analysts should look at the summary of all the deviation characteristics identified and the vulnerabilities identified in Step 5, then ask the following questions:

- Which vulnerabilities identified in Step 5 are well supported by deviation characteristics?
- Can a reasonable scenario be developed that embodies as many of the deviation characteristics as possible?
- Are there any dependencies between the characteristics of the scenario?
- If there aren't any dependencies, is this scenario (thinking of the scenario as a chain of occurrences) so improbable as to be nonrisk significant (and therefore probably unrealistic)?
- If so, are fewer characteristics sufficient to define a deviation scenario?

Development of the deviation scenario requires knowledge about plant operations and thermal hydraulics so that the analysts can think up the chain of occurrences that will cause the parameter and equipment responses and timing of responses that match the deviation characteristics. The development of a deviation scenario also may be similar (although perhaps without the risk perspective) to that process used to develop simulator exercises by operator trainers. Consequently, the assistance of operator trainers and the plant simulator, if available, could be invaluable to this process. In earlier trials of the ATHEANA process, the operator training staff at a cooperating PWR plant assisted in the development of a deviation scenario. The plant's operator training staff used their knowledge, experience, and the plant simulator to develop, refine, and test the deviation scenario developed.

As indicated by the questions above, to the extent possible, analysts should try to incorporate multiple deviation characteristics that support the likely occurrence of the HFEs or UAs of interest. However, the analysts should try to avoid making up a deviation scenario that is so improbable that the HFE probability (that will be quantified in Section 10) is reduced to the point of insignificance. HFE probability can be reduced by the nature of or multiple characteristics. Consequently, the analysts may have to think ahead to the quantification task when developing a deviation scenario.

The analysts may find that multiple integration steps are required for developing the deviation scenario from the characteristics being used. For example, error mechanisms may have been

identified for each of the deviation characteristics, but the mechanisms identified may be degenerate, or only one or two mechanisms may be especially relevant in the global sense. As discussed in Section 9.6.3, the analysts may think ahead to what performance-shaping factors might be relevant or might be activated by the plant conditions. (Step 7 specifically addresses consideration of performance shaping factors.) If so, the analysts should try to identify which error mechanisms might be activated by these plant conditions and performance-shaping factors that define the deviation scenario.

In addition, the analysts may find that they have included some complicating factors (see Step 7) in the deviation scenario developed in this step. Such thinking ahead should not be discouraged. However, Step 7 still should be performed rigorously since the systematic search in this step may reveal factors that might not otherwise be thought of. An example of helpful ways to capture the results of Step 6 can be found in Section B.6.5 of Appendix B.

9.6.8 Products of Step 6

The products of Step 6 include the summary of the deviation characteristics found in the four searches and descriptions of deviation scenarios developed from the characteristics. The deviation scenario descriptions serve as an initial EFC that will be refined further in the next step.

9.7 Identify and Evaluate Complicating Factors and Links to PSFs

This step expands and further refines the EFC definition begun in Step 6. As shown in Figure 9.6, the analysts consider the following in this step:

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

Like the previous section on developing the deviation scenario and EFC, this step may need to be performed iteratively with quantification (Step 10). In particular, the judgments that analysts will need to make regarding how many complicating factors to add to the EFC are best based upon quantification considerations (see Section 10.2).

If the EFC context identified in the previous step (i.e., Step 6) is judged to be sufficiently strong, then only PSFs triggered by this context (which, therefore, do not reduce the frequency or probability of the context) are identified in this step. If, on the other hand, the context identified in the previous step requires additional factors, then both categories of complicating factors are identified. Each category is discussed further below.

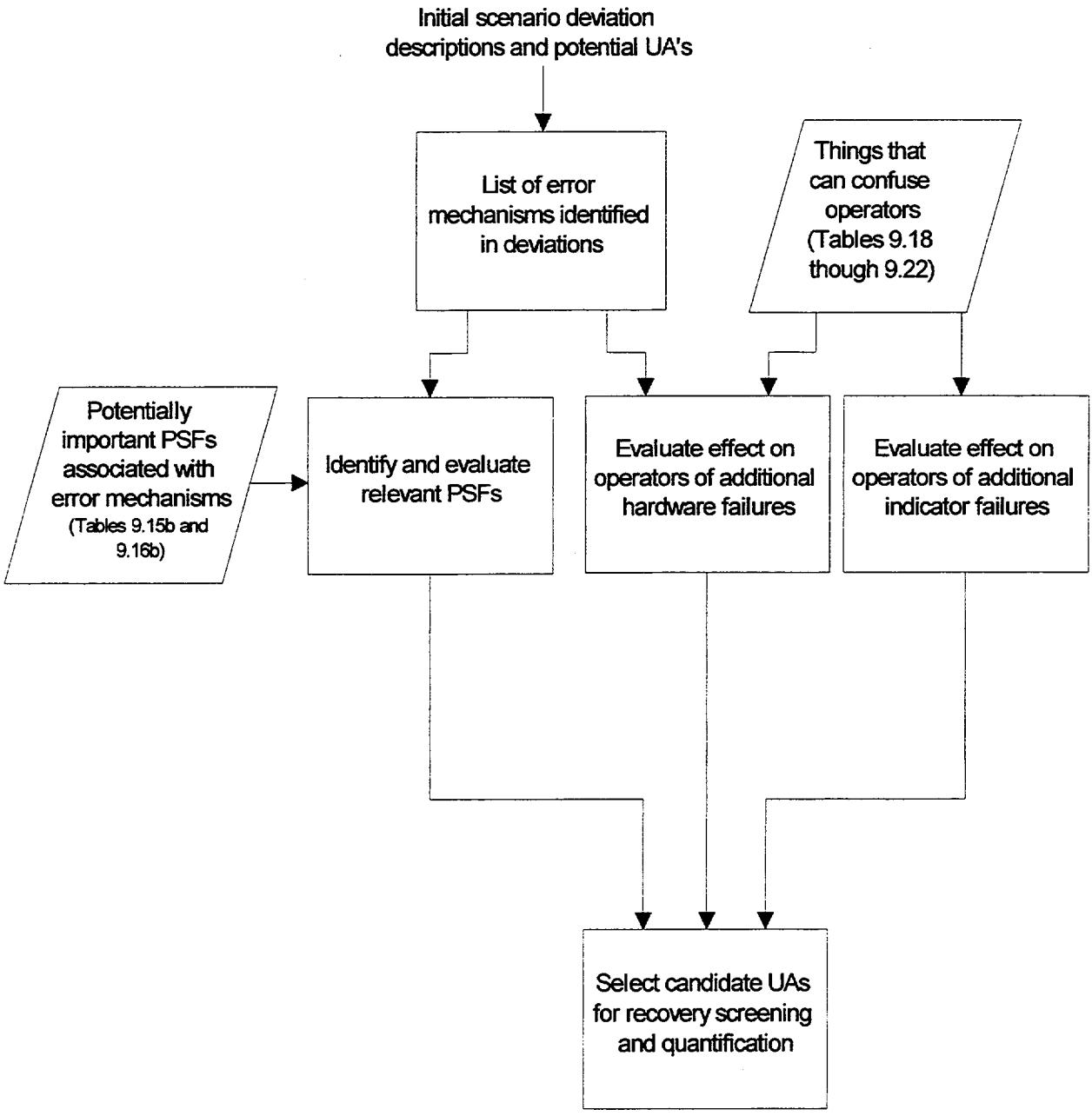


Figure 9.6 Step 7 - Evaluate Complicating Factors

9.7.1 PSFs

Because of the requirements of the various quantification methods that may be used in applying ATHEANA (see Section 10.2.2.2), the identification of relevant PSFs is an iterative step with quantification (if the issue of interest requires quantification). These are two types of PSFs that can add to the EFC initially defined in Step 6. These two types are:

- PSFs that are triggered by the already-defined context
- additional PSFs that are not specific to the context

PSFs that are triggered by the context identified in Step 6 include those that are linked to specific plant conditions and those associated with error types or mechanisms. Examples of triggered PSFs include:

- any relevant PSFs shown in the far right-hand column of Tables 9.15b and 9.16b that are associated with an identified error type or mechanism

- procedures that do not apply to the specific deviation scenario or are otherwise difficult to implement

- control panel layouts that make it difficult for operators to monitor plant status or perform required tasks in response to deviation scenarios (e.g., distributed control panels with shorter than the usual amount of time available)

- high operator workload because of multiple hardware failures, etc. in the deviation scenarios

In some cases, such as for the operator tendencies search in Section 9.6.6, the results of Step 6 may include only plant conditions and not error mechanisms. For these cases, analysts should look more globally for PSFs, using resources provided, such as the PSF list given above and the plant conditions that are used to describe the deviation scenario.

Additional examples can be found in Appendices B through E. Also, Section 5 provides examples of PSFs from operational experience in tabular form. Tables 5.1 through 5.4 provide a mixture of plant conditions and PSFs, while Table 5.5 provides principally PSF examples.

PSFs that are linked to specific plant conditions must be identified using knowledge of plant-specific design and operations as well as the description of the base case and deviation scenarios developed in the previous steps. In addition, the following is a list of commonly used PSFs and strategic factors that analysts can use to prompt their search for applicable PSFs:

- procedures
- training
- communication

- supervision
- staffing
- human–system interface
- organizational factors
- stress
- environmental conditions
- strategic factors such as multiple conflicting goals, time pressure, limited resources (see Section 4.2.3 for a discussion)

PSFs that are linked to error types or mechanisms specific to the deviation scenario context can be identified by reviewing Tables 9.15b and 9.16b. The far right-hand column in these tables provides lists of PSFs that are applicable for specific error types and mechanisms, given the context of the scenarios. If applicable error types or mechanisms were identified in Step 6 for the deviation scenario, the analysts should review the list of PSFs that apply to these error types or mechanisms. During this review, the analysts should determine if the PSF is applicable to the specific deviation scenario and the specific plant design and operation. Also, analysts should recall the note regarding the purpose and limitations of Tables 9.15a and b and 9.16a and b. For example, a particular PSF will not necessarily be related to a certain error mechanism. To repeat, the tables are to be used as guidance for possible factors and relationships to consider, as opposed to a specification of the precise relationship among factors.

In some cases, such as for the operator tendencies search in Section 9.6.6, the results of Step 6 may not include error mechanisms. For these cases, analysts should look more globally for PSFs, using resources provided such as the PSF list given above and the plant conditions that are used to describe the deviation scenario. PSFs identified in this way are context specific but have not been focused by an identified error mechanism.

The second type of PSF is identified through consideration of the deviation scenario definition and review of the list of PSFs. Examples of such PSFs (that are not specific to any deviation, although they can be plant specific) are:

- the impact of time of day on operator performance
- stress or workload (of nonspecific origin)
- general management directives or other guidance

The analysts are cautioned to be restrictive in adding PSFs that are not triggered or activated by the specific EFC. The point of addressing PSFs in this step is not to pile on a lot of PSFs or to address all possible PSFs. Rather, analysts should search for only those PSFs that might represent vulnerabilities that could contribute significantly to the EFC. For example, suppose the analysts identify for the specific plant being considered that operating crews are not yet using formalized communication as much as trainers would like. In addition, this deficiency seems to be a factor in somewhat challenging scenarios that the operating crews have faced in simulator training. In this

case, the judgment of the analysts (especially the input from operators and trainers) would be to add such a negative PSF to the existing EFC.

Another reason for being very restrictive in adding non-triggered PSFs is that such additions may lower the EFC probability. Initially, the analysts should focus on adding only those PSFs that are judged to increase the conditional probability of the unsafe action(s) associated with the HFE [i.e., increase the likelihood that the operators will take the associated inappropriate action(s)]. In fact, analysts may want to defer adding such PSFs until after some initial consideration of HFE quantification, including perhaps consultation with those who will provide the expert judgments needed in quantification. After this initial consideration of quantification, analysts can iterate back to this step to add PSFs, if necessary.

9.7.2 Additional Physical Conditions

Like the additional PSFs discussed above, more physical conditions can be added to the initial error-forcing context identified in Step 6. It is possible that if Step 6 is done very thoroughly, no new additional physical conditions (except those extraneous conditions that complicate the scenario and required operator response) may be found with this search. Also, if analysts desire, the additional resources (i.e., Tables 9.17 through 9.21) used in this search can be used earlier in the process (e.g., Step 6).

Also, like additional PSFs, such additional physical conditions may lower the probability or frequency of the HFE. Consequently, analysts should try to add only those plant conditions that are judged necessary to sufficiently strengthen the error-forcing context in order to increase the likelihood of unsafe operator actions. The addition of plant conditions also can be revisited after initial consideration of quantification, if necessary.

As illustrated by the summaries of event analyses in Section 5 and Appendix A, past operational experience has shown that serious events typically involve contextual elements falling into more than one of the following major categories of deviations in plant conditions: physics, information, hardware, and plant configuration. Physics deviations were identified in Step 6. Consequently, analysts should consider the following types of additional plant conditions:

- additional hardware failures, configuration problems, or unavailabilities
- indication failures
- plant conditions that can confuse operators
- factors not normally considered in PRAs

Each of these is discussed briefly below. As in the physics search described in Section 9.6.3, the analysts should investigate if there are any unrecoverable slips or lapses (both operator interactions with equipment and misreading or misinterpretation of indicators by operators) that could cause the plant conditions associated with the additional factors identified in this search.

Table 9.17 provides example causes of hardware failures, configuration problems, or unmodeled unavailability issues. Analysts should focus first on those conditions that are supported by or are extensions of the context already defined in Step 6. For example, if certain hardware failures already are part of the deviation scenario in Step 6, these failures could be explained by common-cause or other dependent failures. Also, if this is a plausible explanation for the failures defined in the deviation scenario, then additional failures may be plausible for the same reason. Knowledge of plant-specific systems design and operations is crucial in identifying such plausible extensions or links to the previously defined context. By identifying additional conditions that are related to (even dependent upon) the initially defined EFC, the initial EFC is strengthened with minimal reduction in the HFE probability.

For indicator failures, analysts can refer to Table 9.18 for prompts of different types of indicator failures and their causes.

The accident record has shown that certain kinds of plant conditions can confuse operators. The analysts should refer to Tables 9.19 through 9.21 for examples of such conditions. As for the other tables provided in this section, the examples given in these tables should be viewed as prompts for analysts' thinking and discussion, rather than as an exhaustive list of possibilities.

The accident record also shows that there are some factors that may be important to operator performance that are not normally considered in PRAs. In Section 5, Table 5.7 provided examples of such factors that analysts could consider in deciding what additional plant conditions should be added to the error-forcing context initially defined in Step 6.

9.7.3 Reintegration of the Deviation Scenario Description

If elements are added to the deviation scenario description (or EFC) in this step, then the analysts should reintegrate the scenario description in a way similar to that described in Section 9.6.7 for Step 6. In particular, new plant conditions or performance-shaping factors should be integrated into the scenario description. Also, these new plant conditions or PSFs might activate different or additional error mechanisms.

Table 9.17 Examples of Hardware Failures, Configuration Problems, or Unavailabilities

Plant Condition Type	Examples
Hardware response	Random failures (including multiple failures, spurious actuations)
	Initiator-induced failures
	Mode-induced failures (e.g., equipment inoperable or unavailable during shutdown conditions)

Table 9.17 Examples of Hardware Failures, Configuration Problems, or Unavailabilities (Cont.)

Plant Condition Type	Examples
	Common-cause failures
	Other dependent failures (e.g., support system failures, other cascading effects, human-induced, etc.)
	Preexisting operational problems
	Degraded operation
	Beyond design limits
	Human-induced (both latent and active failures)
Plant configuration	Concurrent activities (as they affect operator actions required for accident response)
	Latent failures (as they affect operator actions required for accident response; see also Hardware response, human-induced above)
Unavailabilities	Realistic unavailabilities (e.g., two trains out for maintenance simultaneously)

9.7.4 Products of Step 7

The completion of Step 7 results in the explicit addition of PSFs and other physical conditions to the descriptions of the deviation scenarios so that the EFC is now considered sufficiently strong to make the likelihood of the HFEs or UAs worth concern.

9.8 Step 8: Evaluate the Potential for Recovery

In this step, the definitions of HFEs and the associated EFCs are completed by considering the opportunities for recovering from the initial error(s) (or more precisely not recovering from initial errors). Performance of this step, perhaps even more so than previous search steps, is linked to issues considered in quantification (see Section 10.2). Consequently, some iteration between this step and the quantification step is possible. Also, since the consideration of the opportunities for recovery will involve extending the context defined in previous deviation search steps, recovery analysis also is iterative with Steps 6 and 7. If an HFE can be ensured to be recovered, the analysis stops and proceeds to issue resolution. If recovery cannot be ensured, then the analysis proceeds according to the discussion below.

9.8.1 Guidance for Step 8

The definition of the HFE or UA and the associated context (represented by the description of the deviation scenario) corresponds to an initial error(s). Given this initial error in responding to a specific deviation scenario, it is possible that later in the accident sequence the operators will recognize their error and be able to correct their initial actions before core damage or functional failure(s) occurs. Since the definition of HFEs modeled in the PRA includes both the initial unsafe action and the failure to correct this action, the analysts should investigate what opportunities for successful correction do exist, given the definition of the unsafe action and its explanation developed through the last step.

In evaluating the potential for recovery, the analysts should consider the following five main elements in analyzing the potential for recovery actions:

(1) definition of the possible recovery action(s) if the HFE/UA has been performed

(2) time available to perform the recovery actions so as to prevent a serious outcome (e.g., core damage)

(3) the existence and timing of additional cues that would alert the operators to the need to recover and provide sufficient information to identify the applicable recovery action(s)

(4) the existence and timing of additional resources (e.g., personnel) that could assist in recovery

(5) an assessment as to the strength of the recovery cues with respect to the initial EFC (i.e., plant conditions, PSFs, associated error mechanisms) and hence the likelihood of successful recovery (Section 10 provides some discussion on how to make such assessments)

To consider the above, the analysts should first decide on the necessary recovery action(s). This is based largely on the underlying understanding of what safety function(s) and equipment are failed or otherwise jeopardized as a result of the plant conditions and the HFE and UAs making up the deviation scenario. In addition, the time by which the recovery action(s) needs to be performed should also be identified based on the deviation scenario and an understanding of its related thermal hydraulics.

With the above knowledge, the analysts then develop the deviation scenario progression beyond the initial loss or degradation of the safety function or equipment [i.e., after the initial unsafe action(s) in the defined HFE]. One way to identify additional cues for recovery and understand plant behavior following the initial unsafe action(s) is to continue the mapping of trends in key plant parameters that was begun in Steps 5 and 6. Then development of a scenario progression log, similar to the diagnosis log created for the event analyses documented in Appendix A, can help analysts in structuring and assessing this new information. Appendices B through E provide illustrative examples of such scenario progression logs, using the headings of timing, plant symptoms, and

operator actions. The scenario progression log should highlight expected changes in key plant conditions and parameters, as well as any new relevant cues (indications, alarms, plant personnel observations) that are likely to occur as a result of the scenario progression. The new cues and resources that are identified will form the basis for defining additional contextual elements that are associated with nonrecovery.

Analyst judgment is the basis for the assessment of the importance of new cues and resources. However, the amount of time available for correction is an overriding factor. In other words, if little or no time is available to recover from the initial error, then the chance for recovery will be small. After time available, the analysts look for potential dependencies between the deviation scenario description (i.e., EFC) for the initial unsafe action and the failure to correct the initial action. Also, the analysts should recognize that initial mindsets (i.e., situation models) can be very difficult to break. (See the Oconee 3 example, especially the scenario progression log, given in Section 5 as well as the more detailed analysis given in Appendix A.) Also, operators can be distracted (or be too busy) with other activities, thereby missing cues and opportunities for action. Finally, operators often can justify the delay of actions beyond their criteria for performance, especially if plant hardware is almost fixed or returned to service (or initially failed by operator slips or lapses) and the consequences of the action are considered extreme. (See, for example, the Davis Besse loss of feedwater event in 1985 in Appendix A.) When considering these possible reasons for not performing the recovery action, the analysts should note the number, timing, and nature of the new cues (e.g., alarm, indicator change) and decide on how compelling the new cues are relative to these possible reasons for failing to recover. Any resulting new EFC elements that are associated with the recovery action should be added to the EFC identified for the initial unsafe action in order to complete the EFC for the HFE that will be modeled in the PRA.

Finally, the ATHEANA analysts should compare the EFC context developed with the characteristics of serious accidents listed in Table 5.6 and the complicating factors not usually modeled in PRAs given in Table 5.7. Both of these tables can be considered templates for error-forcing contexts.

9.8.2 Reintegration of the Deviation Scenario after Recovery

Because recovery analysis may add elements to the deviation scenario description (or error-forcing context), just as in Step 7, the analysts should reintegrate the scenario description after recovery analysis also. This reintegration should follow the general guidance given in Section 9.6.7 for Step 6. As in Step 7, elements of the error-forcing context that are added through recovery analysis might activate different or additional error mechanisms.

9.8.3 Product of Step 8

The product of Step 8 is the finalization of the EFC for the HFE and UAs of concern as part of the overall deviation scenario description. However, as stated at the beginning of Section 9.8, iteration between this step and quantification (Step 9) may be required.

Table 9.18 Examples of Information (i.e., Transmit) Problems

Hardware/Software Failures (i.e., information wrong, including instrument, sensor, switch, computer, and calculated parameter failures) (failures may be known, undiscovered, or masked by other activities) Hardware/software may be: Randomly failed (including spurious indications, failures to respond, intermediate indications) Unavailable due to testing or maintenance Disabled by personnel Failed due to operator actions Outside operating range due to plant conditions Provide conflicting indications Failed due to design flaws (e.g., redundant parameters not independent)
Display Failures (i.e., information misleading) Display may: Be failed (e.g., a broken meter or alarm) - either known or undiscovered Lack global cues Lack reference context Have hidden indications (e.g, on back panels) Have distributed locations for displays or controls Have noisy interfaces Have design flaws (e.g., indicated valve position not connected with stem position) Have delayed indication (e.g., trends not noticeable due to recorder scale and event timing) Have only temporary indication (e.g., parameter or trend not noticeable because only temporarily displayed due to event timing or other factors)
Other Human Factor Problems (i.e., information wrong and/or misleading) Information may be wrong or misleading because of: Communication failures (wrong, misleading, ambiguous) (field operators, personnel in containment, I&C or maintenance technicians) Design flaws Lack of redundant instruments or other information sources Requirements for interpretations or hand calculations of parameters (e.g., due to operations outside normal conditions in Prairie Island 2 shutdown event)

Table 9.19 Physics Algorithms in Instruments that Can Confuse Operators

Indicator/Algorithm or Actual	Example
Valve position indicator	Drive vs. stem position Stem disk separation Switch on solenoid Motor operated valve drive screw
Level indicator	Flashing in reference leg P_{pzr} uncompensated for temperature Sensor leaks Sensor isolation
Pressure indicator	Indicated parameter can be time history algorithm Improper sensor location
Temperature indicator	RTDs: linearity limits, ambient temperature compensation T/C: linearity limits, reference temperature drift
Any indicator	Indicated parameter can be calculated from others rather than measured directly Plant behaves in a way to make algorithm generate wrong information or story

Table 9.20 Examples of Plant Conditions in Which the Plant Physics or Behavior Can Confuse Operators

Plant Conditions or Physics	Examples
Reaching saturation, then repressurizing	Steam bubbles will have formed in hot spots, possibly interfering with flow or reflooding)
Positive temperature coefficient	Can result in unanticipated overpower
Operation of electrical equipment	Effects of grounds Speed control and power in 3-phase induction (and synchronous) machines Breaker and controller lockout circuits Selective tripping
Transient effects beyond those analyzed and addressed in training	LOCAs other than 2-inch and double-ended guillotine)
Multiple evolutions (which confound expected physics)	Ramping up or down in power while equipment is being tested or bought back on-line after maintenance
Net positive suction head	Draining down to midloop while other tests, washdown activities, etc. are being performed during shutdown

Table 9.21 Other Plant Conditions that Can Confuse Operators

Plant Conditions	Details
Plant radios	Results in garbled communications
Multiple equipment failures	Common causes failure Combinations of degraded functions, unavailability, human-induced failures, and/or "random" failures
Partial degraded, rather than failed instrument or control air pressure	Can result in increasing combinations of failed equipment
Failures in selective tripping of electrical breakers	
Ambient temperature-induced failures of electrical or electronic equipment	Can result in increasing combinations of failed equipment
Multiple problems	Combinations of any of the above or conditions indicated on other tables

9.9 References

9.1 Magee, R.S., E.M. Drake, D.C. Bley, G.H. Dyer, V.E. Falter, J.R. Gibson, M.R. Greenberg, C.E. Kolb, D.S. Kosson, W.G. May, A.H. Mushkatel, P.J. Niemiec, G.W. Parshall, W. Tumas, and J. Wu, *Risk Assessment and Management at Deseret Chemical Depot and the Tooele Chemical Agent Disposal Facility*, Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, National Research Council, National Academy Press, Washington, DC, 1997.

9.2 Isselbacher, K.J., A.C. Upton, J.C. Bailar, K.B. Bischoff, K.T. Bogen, J.I. Brauman, D.D. Doniger, J. Doull, A.M. Finkel, C.C. Harris, P.K. Hopke, S.S. Jasanoff, R.O. McClellan, L.E. Moses, D.W. North, C.N. Oren, R.T. Parkin, E.D. Pellizzari, J.V. Fodricks, A.G. Russell, J.N. Seiber, S.N. Spaw, J.D. Spengler, B. Walker, and H. Witschi, *Science and Judgment in Risk Assessment*, Committee on Risk Assessment of Hazardous Air Pollutants, National Research Council, National Academy Press, Washington, DC 1994.

9.3 J.P. Poloski, D.G. Marksberry, C.L. Atwood, and W.J. Galyean, *Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995*, NUREG/CR-5750, Idaho National Engineering and Environmental Laboratory, February 1999.

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

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

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

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

Table 9.9a Possible EOCs for Systems or Equipment that Automatically Start or Stop

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to initiate or actuate automatically	1 and 2	Inappropriately removed from automatic control	Operators take equipment out of armed or standby status (e.g., pumps put in pull-to-lock) Operators change equipment configuration/lineup from armed, standby, or normal status
		Inappropriately removed from armed or standby status	Operators bypass or suppress automatic signals Operators disable automatic signals/sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators reset signal setpoints Operators disable or fail equipment
Equipment fails to stop automatically	7	Inappropriately removed from automatic control	Operators bypass or suppress automatic signals Operators disable automatic signals or sensors Operators take automatic signals out of armed status Operators remove or disable motive and/or control power Operators reset signal setpoints Operators disable or fail equipment

Table 9.9b Possible EOCs for Continuation of Operation or No Operation of Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to continue to operate for duration of mission time	3	Inappropriately terminated	Operators stop equipment (e.g., pumps stopped) Operators both stop and disable equipment for future service (e.g., pumps put in pull-to-lock) Operators disable or fail equipment (e.g., due to operation outside of design parameters) Operators stop and realign equipment out of required armed or standby configuration or lineup Operators stop equipment and bypass or suppress automatic signals Operators stop equipment and disable automatic signals/sensors Operators stop equipment and take automatic signals out of armed status Operators stop equipment and reset signal setpoints
		Inappropriately isolated or aligned	Operators realign equipment (e.g., valves repositioned) Operators actuate equipment automatic isolation signals Operators actuate equipment automatic reconfiguration signals
		Output and/or resources inappropriately diverted	Operators realign equipment (e.g., valves repositioned) Operators operate equipment outside design parameters (e.g., over RHR design pressure, resulting in flow diversion through lifted relief valves, ISLOCAs, etc.)
		Output and/or resources inappropriately depleted	Operators do not adequately control equipment that competes for resources before or during operation of required equipment Operators do not control equipment early in accident (Also considerations with ...resources diverted above)
Equipment status inappropriately changed	10	Inappropriately operated	Operators manually actuate or start equipment Operators manually realign equipment Operators manually override equipment automatic isolation signals Operators manually actuate equipment automatic control
Equipment fails to remain stopped for required duration	8	Inappropriately restarted (and continues to operate)	

Table 9.9c Possible EOCs or EOOs for Manual Actuation and Control of Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to be manually intiated or actuated when required	4	Fails to be actuated when required (EOO)	Operators never actuate equipment Operators actuate equipment too late Operators release or unsuppress equipment automatic initiation signals too late
		Inappropriately initiated or actuated (EOC)	Operators actuate equipment prematurely (i.e., too soon) Operators release or unsuppress equipment automatic initiation signals prematurely
Equipment fails to be stopped manually	9	Fails to be stopped when required (EOO)	Operators never stop equipment Operators stop equipment too late Operators release or unsuppress equipment automatic initiation signals for stop too late
Equipment fails to be controlled or operated as required	5	Fails to be operated or controlled (EOO) Inappropriately operated or controlled (EOC)	Operator control of equipment operation results in: Underfeeding or filling — Overfeeding or filling Undercooling — Overcooling Underpressure — Overpressure Reactivity decrease — Reactivity increase Integrity breach

Table 9.9d Possible EOOs for Backup (i.e., Recovery) of Failed Systems and Equipment

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment fails to initiate or actuate automatically	2	Fails to perform backup, manual startup (after automatic actuation fails)	Operator fails to manually start/stop Operator fails to manually isolation/alignment Operator fails to manually open/close Operator fails to manually lockout/trip Operator fails to manually insert/withdraw Operator fails to manually transfer
Equipment fails to stop automatically	7	Fails to perform backup, manual stop (after automatic stop fails)	
Equipment fails to remain stopped for required duration	8	Fails to perform backup, manual stop (after spurious re-start)	
Equipment status changes spuriously and inappropriately	11	Fails to perform backup, manual stop (after spurious actuation) Fails to perform backup, manual re-alignment (after spurious re-configuration)	

Table 9.9e Possible EOCs or EOOs for Failures of Passive Systems and Components

PRA Functional Failure Modes	Category of Functional Failure Mode	Example Human Failures	Example Unsafe Actions
Equipment status inappropriately changed	6	Fails to maintain integrity (EOO)	Operator actions (e.g., operator fails to operate/control, operator inappropriately operates/controls) from other categories that have these consequential effects
		Inappropriately breached integrity (EOC)	

Table 9.15a
Scenario Characteristics and Description

1. **Situation Assessment** - If a scenario can be described by any of the characteristics below, go to the corresponding scenario characteristics for *failures in situation assessment* presented in Table 9.15b to identify Potential error mechanisms, possible unsafe actions (UAs), and relevant performance-shaping factors (PSFs).

Scenario Characteristics	Description
Garden path problems	Conditions start out with the scenario appearing to be a simple problem (based on strong but incorrect evidence) and operators react accordingly. However, later correct symptoms appear, which the operators may not notice until it is too late.
Situations that change, requiring revised situation assessments	Once operators have developed a situation assessment and have started acting on it, it is often very difficult for them to recognize that there is new information or new conditions that requires them to change their situation assessment
Missing information	Key indicators may be missing due to failed sensors, lack of sensors, or lack of informants in the plant.
Misleading information	Misleading information may be provided due to inherent limitations of reports (e.g., stale information, inherent limitations of predictions, distortions resulting from indirect reports, secondary sources, translations) or explicit intent to deceive through misinformation.
Masking activities	Activities of other agents, or other automated systems may cover up or explain away key evidence.
Multiple lines of reasoning	Situations can occur where it is possible to think of significantly different explanations or response strategies, all of which seem valid at the time, but which may be in conflict (or a source of debate and disagreement by the operating crew).
Side effects	Situations can arise where the effects of human or automated system actions, or effects of the initial failure, have side effects that are not expected or understood.

Table 9.15a
Scenario Characteristics and Description (Cont.)

2. **Response Planning** - If a scenario can be described by any of the characteristics below, go to the corresponding scenario characteristics for *failures in response planning* presented in Table 9.15b to identify potential error mechanisms, possible UAs, and relevant PSFs.

Scenario Characteristics	Description
Impasses	The scenario contains features where, at some point, it is very difficult for the operators to move forward, such as when procedures or the operators' situation model no longer matches the conditions, or assumed personnel or resources are not available.
Late changes in the plan	The scenario is being managed according to a prepared plan, and then for some reason changes are required late in the scenario. Operators can become confused as to next steps; the plan is no longer well tested and can contain flaws, or the whole "big picture" gets lost by those managing the event.
Dilemmas	Ambiguity in the plan or in the situation (the event looks somewhat like two or more different accidents) can raise significant doubt in the operators' minds about the appropriate next steps.
Trade-offs	Operators must make impromptu judgments about choices between alternatives, such as when to wait to see if a problem develops (and may get out of control) versus jumping in early before it is clear what has caused the problem (just one of many examples).
Double binds	Conditions exist where operators are faced with two (or more) choices, all of which have undesirable elements.
High tempo, multiple tasks (Sub- or related categories are escalating events, cascading problems, and interacting problems)	The operators simply run out of resources (mental or physical) to keep up with the task demands. In escalating events, the problem keeps getting harder and harder or more complex. Cascading problems are those where the effects of one problem (or an attempt to solve it by the operators) create new problems. In interacting problems two or more faults interact to create complex symptoms that may have never been foreseen.
Need to shift focus of attention	As the scenario unfolds, the operators may need to move attention from one particular aspect of the problem to another, yet they remain focused on the initial problem area, which may be minor.

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors

1. **Failures in Situation Assessment** - When particular characteristics in Table 9.15a are identified as relevant descriptors of a scenario, this table is used to identify potential human error mechanisms that may facilitate *failures in situation assessment.* Possible generic unsafe actions (UAs) and potential performance-shaping factors (PSFs) that could contribute to the occurrence of a UA are also presented. *(Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.)*

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Garden path problems Situations that change, requiring revised situation assessments	1. Simplifying 2. Recency 3. Frequency 4. Familiarity 5. Fixation 6. Tunnel vision 7. Confirmation bias 8. Complacency	1. Initial application of incorrect procedure step 1 - 8. Operators defer action on the changes indicated by other parameters 5 - 8. Fail to recognize a serious situation in time 1 - 8. Take an inappropriate action, take a correct action too soon, fail to take a needed action 5 - 8. Miss a decision point	1 - 4. Training/practice - Initial event is used repeatedly in training or was addressed in training, or is one about which a lot of attention is given in training All. Human-machine interface (HMI) - Later-occurring correct or complete indicators are located where they can be easily seen by one or more crew members. All. HMI Are the later - occurring indications compelling? All. Workload - Would the operators have to work hard to identify and understand the later occurring information? Could the workload become excessive? Could the situation not seem important enough to induce them to search for verification? 5 - 8. Procedures - Are there any warnings or items in the procedures that might alert operators to the importance of the later-occurring information?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Situation Assessment) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Missing information	1. Displayed parameters lead to entry into wrong procedure step or may not lead to entry into procedure 2. Displayed parameters match incorrect mental template (similarity matching) 3. Existing pattern of information directs operators' attention away from redundant sources 4. Complacency 5. Overly eager to respond 6. Simplifying	1,2,&3. Application of incorrect procedure step or no response. 1 - 6. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1, 2 & 3 HMI - Are there indicators that might help the crew discover the existence of the missing information? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 3. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 1 - 3. Training/practice - Lack of discipline or trained practice in searching for other relevant parameters 2. Training/practice - Similar event is used repeatedly in training or was addressed in training, or is given a lot of attention in training 1 - 6. Workload - Would the operators have to work hard to identify other sources of information that could help them detect the absence of the missing indications? Could the workload become excessive or could the situation not seem important enough to induce them to search for verification?
Misleading information	Same as above	Same as above	Same as above

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Situation Assessment) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Masking activities	1. General pattern of existing information seems normal enough that operators do not detect or understand important changes in some parameters 2. Simplifying 3. Apathy - Lack of urgent consideration of parametric behavior as displayed 4. Overeagerness (inclination to respond too soon)	1,2&4. Selection of wrong or less relevant procedure 1,2,3&4. Incorrect situation assessment due to hidden information 1,2,&3. Operators defer action on the basis of the parameters as displayed 1,2,&3. Fail to recognize a serious situation in time 1,2,3,&4. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1,2,&3. Miss a decision point 4. Anticipate an incorrect situation and take an action too soon.	1- 4. Training/practice - Lack of discipline or trained practice in monitoring all parameters and cross-checking against other information 1- 4. HMI - Are there other indicators that might help the crew detect the existence of the hidden information? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 4. Training/practice - Operators have learned to focus on restricted set of available information sources 1,2 & 4. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately considering other relevant indications?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Situation Assessment) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Multiple lines of reasoning	1. Simplifying 2. Satisfying 3. Polarization of thinking 4. Expectation biases (familiarity, recency, primacy, frequency, confirmation bias) 5. Delays (due to crew disagreements) 6. Reluctance, cautiousness 7. Anxiety, stress 8. Lack of deep technical knowledge	1 - 8. Lack of, or reduced, attention paid to other parameters and their changes 1 - 8. Competing or inconsistent responses taken 1 - 8. Application of incorrect procedure step or no response 1 -8. Take an inappropriate action, take a correct action too soon, fail to take a needed action in time	1 - 8. Training - Lack of training or practice for off-normal accident conditions 1 - 8. Procedures - Inadequate information for correct discrimination between lines of reasoning 1 - 8. HMI - Are there other indicators that might help the crew verify or determine the correct line of reasoning ? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters make the conflicting interpretations harder to resolve?
Side effects	1. Lack of deep technical knowledge 2. Reduced vigilance given expected success (overconfidence) 3. Tunnel vision 4. Fixation on initial diagnosis and directly relevant results	1. Take an action that induces both desired and undesired consequences 1 - 4. Fail to take a needed action in time 1 - 4. Take an inappropriate action given the presence of the undesired side effects	1 - 3. Training - Lack of training or practice for off-normal accident conditions 1 - 3. HMI - Are there other indicators that might help the crew detect the undesired side effects ? Are they located where they can be easily seen by one or more crew members most of the time? Are they compelling? 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring make the undesired effects harder to detect?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Cont.)

2. **Failures in Response Planning** - When particular characteristics in Table 9.15a are identified as relevant descriptors of a scenario, this table is used to identify human error mechanisms that may facilitate *failures in response planning.* Possible generic UAs and potential PSFs that could contribute to the occurrence of a UA are also presented . *(Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.)*

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Impasses	1. Lack of deep technical knowledge 2. Operators' expectations or current situation model begins to conflict with the indications and/or what the procedures dictate 3. Anxiety about taking a wrong action	1 - 2. Fail to take a needed action in time	1 - 2. Training - Lack of training or practice for off-normal accident conditions 1 - 2. Procedures - Inadequate information for how to proceed 1 - 2. HMI - Are there other indicators that might help the crew verify or determine the correct response ? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 2. Workload - Could the operators' workload make the impasse about how to proceed more difficult to resolve? 2 - 3. Organizational factors Could fear of retribution or other aspects of the organizational climate at the plant contribute to making it more difficult to solve the impasse? 2 - 3. Organizational factors Does the plant have strict guidelines regarding adherence to procedures?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Response Planning) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Late changes in the plan	1. Lack of deep technical knowledge 2. Fixation on initial diagnosis and initial response plan 3. Anxiety about taking a wrong action	1 - 3. Fail to take a needed action in time 1 - 3. Take an inappropriate action	1 - 3. Training - Lack of training or practice for off-normal accident conditions 1 - 3. Procedures - Is there adequate information for how to proceed if the new indicators are accepted? 1 - 3. HMI - Are there other indicators that might help the crew tease out the correct response plan ? Are they located where they can be easily seen by one or more crew members most of the time? Are they compelling? 1 - 3. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring make it difficult to derive the correct response plan? 2 - 3. Organizational factors Could fear of retribution or other aspects of the organizational climate at the plant contribute to making it more difficult to change the plan late in the scenario? 2 - 3. Organizational factors Does the plant have strict guidelines regarding adherence to procedures?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Response Planning) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
Dilemmas Trade-offs Double binds	1. Lack of deep technical knowledge 2. Anxiety about taking a wrong action	1 - 2. Fail to take a needed action in time 1 - 2. Take an inappropriate action	1. Training - Lack of training or practice for off-normal accident conditions 1. Procedures - Inadequate information or guidance for how to proceed 1. HMI - Are there other indicators that might help the crew verify or determine the the correct response ? Are they located where they can be easily seen by one or more crew members most of the time? 1. Workload - Could the operators' workload make the dilemma, trade-off, or double bind more difficult to resolve? 2. Organizational factors Could fear of retribution or other aspects of the organizational climate at the plant contribute to making it more difficult to solve the dilemma, trade-off, or double bind? 2. Organizational factors Does the plant have strict guidelines regarding adherence to procedures?

Table 9.15b
Scenario Characteristics and Associated Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors (Failures in Response Planning) (Cont.)

Scenario Characteristics	Error Mechanisms	Error Types	PSFs
High tempo, multiple tasks (sub- or related categories are escalating events, cascading problems and interacting problems)	1. Lack of deep technical knowledge 2. Inadequate cognitive resources	1 - 2. Fail to take a needed action in time 1 - 2. Take an inappropriate action 1 - 2. Take an action that simply complicates the problem	1. Training - Lack of training or practice for off-normal accident conditions. 1. Procedures - Inadequate information or guidance for how to proceed 1. HMI - Are there other indicators that might help the crew verify or determine the correct response ? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 2. Workload - Could the operators' workload make the situation more difficult to resolve?
Need to shift focus of attention	1. Simplifying 2. Satisfying 3. Polarization of thinking 4. Expectation biases (familiarity, recency, primacy, frequency, confirmation bias) 5. Delays (due to crew disagreements) 6. Reluctance, cautiousness 7. Anxiety, stress 8. Lack of deep technical knowledge	1 - 8. Lack of, or reduced, attention paid to other parameters and their changes 1 - 8. Competing or inconsistent responses taken 1 - 8. Application of incorrect procedure step or no response 1 -8. Take an inappropriate action, take a correct action too soon, fail to take a needed action in time	1 - 8. Training - Lack of training or practice for off-normal accident conditions 1 - 8. Procedures - Inadequate information for correct discrimination regarding where to focus attention 1 - 8. HMI - Are there other indicators that might help the crew verify or determine where to focus attention? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 5. Workload - Could the operators' workload make it more difficult to determine where to focus attention or realize that they need to shift attention?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics
(Table to be used with Table 9.16b)

1. **Failures in Detection -** If answers to any of the questions are yes, go to the corresponding parameter characteristics for *failures in detection* presented in Table 9.16b to identify potential error mechanisms, possible UAs, and relevant PSFs)

Parameter Characteristics	Question
No indication	Does this scenario involve failed indicators? Does this scenario involve indications calculated from other failed instruments (e.g., subcooling based on RCS pressure)?
Small change in parameter	Within this scenario and with the existing human-machine interface design, is there a relevant parameter change small enough that it might be overlooked (i.e., not detected)?
Large change in parameter	Within this scenario and with the existing human-machine interface design, is there a relevant parameter change so large or out of range that it might be overlooked (e.g, indicator pegged at the top or bottom of a meter and not noticed).
Lower or higher than expected value of parameter	Does this scenario involve indications that are lower or higher than would be expected? Does this deviation correspond with expected values for nonaccident conditions, so that the deviation might not be detected as anomalous?
Low rate of change in parameter	Does this scenario involve significantly slower than expected changes in any indication? Within this scenario and with the existing human–machine interface design, is it likely that the slow rate of change might be overlooked?
High rate of change in parameter	Does this scenario involve rapid changes in any parameter that, with the existing human-machine interface design, may be overlooked (e.g., fleeting changes, briefly appearing alarms or indications, or an indicator pegged at the top or bottom of a meter and not noticed)?
Changes in two or more parameters in a short time	Does this scenario involve changes in two or more indications that are significantly different from expected? Do they involve rapid changes in any parameters that, with this interface design, may be overlooked (such as fleeting changes or briefly appearing alarms or indications)?
Delays in changes in two or more parameters	Does this scenario involve changes in two or more indications that are significantly delayed from what is expected? Do they involve late changes in parameters that, with this interface design, may be overlooked?
One or more false indications	Does this scenario involve false indications that, together with the genuine indications, resemble a situation that is expected (i.e., consistent with other on-going activities that could lead operators to ignore or not attend carefully to the indications)?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Cont.)

2. **Situation Assessment** - If answers to any of the questions are yes, go to the corresponding parameter characteristics for *failures in situation assessment* presented in Table 9.16b to identify potential error mechanisms, possible UAs, and relevant PSFs)

Parameter Characteristics	Question
No indication	Does this scenario involve failed indicators? Does this scenario involve indications calculated from other failed instruments (e.g., subcooling based on RCS pressure)?
Small change in parameter	Does this scenario involve small or significantly smaller-than-expected changes in any indication? Can the operators be led to a state of complacency by this small change? Within this scenario and with the existing human-machine interface design, is it likely that the operators will be misled by a small change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
Large change in parameter	Does this scenario involve a large or significantly larger-than-expected changes in any indication? Can the operators be led to a state of anxiety by this large change? Within this scenario and with this interface design, is it likely that the operators will be misled by a large change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
Lower or higher than expected value of parameter	Does this scenario involve indications that are lower or higher than expected? Does this deviation correspond with expected values for other (different) accident conditions?
Low rate of change in parameter	Does this scenario involve slow or significantly slower-than-expected changes in any indication? Can the operators be led to a state of complacency by this slow change? Within this scenario and with this interface design, is it likely that the operators will be misled by a slow change as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
High rate of change in parameter	Does this scenario involve rapid or significantly more rapid-than-expected changes in any indication? Can the operators be led to a state of anxiety by this rapid change? Does this scenario involve rapid changes in any parameter that, with this interface design, may be discounted or assumed to be anomalous (such as fleeting changes or briefly appearing alarms or indications)? If overlooked or ignored, is the absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Situation Assessment)(Cont.)

Parameter Characteristics	Question
Changes in two or more parameters in a short time	Does this scenario involve changes in two or more indications that are significantly different from expected or inconsistent? If observed, will these indications cause operators to be significantly uncertain or confused as to the situation in the plant? Does this scenario involve rapid changes in any parameters that, with this interface design, may be overlooked (such as fleeting changes or briefly appearing alarms or indications)? If overlooked, is their absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)?
Delays in changes in two or more parameters	Does this scenario involve two or more indications that are significantly delayed from what is expected? If observed, will these delayed indications cause operators to be significantly uncertain or confused as to the situation in the plant? Does this scenario involve changes in two or more indications that are significantly delayed from what is expected? Do they involve late changes in parameters that, with this interface design, may be overlooked? If overlooked, is their absence likely to confuse the operators as to the kind of situation they face (e.g., does it now resemble another scenario that is more familiar)? Delayed information can be ignored or reinterpreted to match earlier (premature) assessments of the plant situation (such as being dismissed as "instrument error").
One or more false indications	Does this scenario involve false indications that, together with the genuine indications, resemble a situation that is "expected" (i.e., consistent with other on-going plant activities that could "explain" their presence)? Will these false indications cause operators to be significantly uncertain or confused as to the situation in the plant?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Situation Assessment)(Cont.)

Parameter Characteristics	Question
Direction of change in parameter(s) over time is not what would be expected (if the base case scenario was operative vs. the deviant) Direction of change in parameters over time, relative to each other, is not what would be expected (if the base case scenario was operative vs. the deviant) Relative rate of change in two or more parameters is not what would be expected (if the base case scenario was operative vs. the deviant)	Does this scenario involve changes in one or more parameters over time that are significantly different than what would be expected if the base case scenario was operative as opposed to the existing deviant scenario. If observed, will these changes cause operators to be significantly uncertain or confused as to the situation in the plant?
Behavior of apparently relevant parameters is actually irrelevant and misleading	Does this scenario involve the occurrence of one or more parameters that are actually irrelevant and misleading given the deviant scenario being examined. If observed, could these parameters cause operators to be significantly mislead. Would they be similar to patterns that would occur in base case scenario.

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics(Cont.)

3. **Response Planning** - If answers to any of the questions are yes, go to the corresponding parameter characteristics for *failures in response planning* presented in Table 9.16b to identify potential error mechanisms, possible UAs, and relevant PSFs)

Parameter Characteristics	Question
No indication	N/A
Small change in parameter	Does this scenario involve smaller-than-expected changes in an important parameter used as a cue or caution in the procedures, or used in training as a basis for actions? What is the likely effect of the operators misapplying this cue or caution? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of complacency or forgetfulness by this small change?
Large change in parameter	Does this scenario involve larger-than-expected changes in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of stress or anxiety by this large change?
Lower or higher than expected value of parameter	Does this scenario involve lower or higher-than-expected values in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of complacency or forgetfulness by the lower change or a state of anxiety by the higher change?
Low rate of change in parameter	Does this scenario involve slower-than-expected changes in an important parameter used as a cue or caution in the procedures? What is the likely effect of the operators mis-applying this cue or caution? Can the operators be led to apply informal rules by this slower deviation? Can the operators be led to a state of complacency or forgetfulness by this slower change?
High rate of change in parameter	Does this scenario involve faster-than-expected changes in an important parameter used as a cue or caution in the procedures? Can the operators be led to apply informal rules by this deviation? Can the operators be led to a state of stress or anxiety by this faster change?
Changes in two or more parameters in a short time	Does this scenario involve changes in two or more indications that are significantly different from the procedural expectations? If observed, will these indications cause operators to be significantly uncertain or confused as to how the procedures should be applied to the plant?
Delays in changes in two or more parameters	Does this scenario involve significant delays in two or more indications compared with the procedural expectations? Will these delays cause operators to be significantly uncertain or confused as to how the procedures should be applied to the plant?

Table 9.16a
Questions to Identify Scenario Relevant Parameter Characteristics (Response Planning)(Cont.)

Parameter Characteristics	Question
One or more false indications	Does this scenario involve false indications that mislead the operators into believing that the required actions are no longer necessary or are not possible (e.g., false indication of a caution or prohibition)? Does this scenario involve false indications that require inconsistent actions by operators (e.g., both depressurize and repressurize the primary system)?
Parameters indicate response for which insufficient resources are available or indicate more than one response option	Does this scenario involve a situation where the unavailability of resources make the response difficult to execute? Are there competing options or options with trade-offs?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Table to be used following Table 9.16a)

1. **Failures in Detection** - When particular parameter characteristics in Table 9.16a are identified as relevant descriptors of critical parameters in a scenario, this table is used to identify human error mechanisms that may facilitate *failures in detection.* Possible generic error types and potential performance-shaping factors (PSFs) that could contribute to the occurrence of an unsafe action (UA) are also presented. *[Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.]*

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
No indication	1. Displayed parameters lead to entry into wrong procedure step or may not lead to entry into procedure 2. Other indications or parameters alone are benign, leading to complacency 3. Existing pattern of information directs operators' attention away from redundant sources	1,2,&3. Application of incorrect procedure step or no response	1. HMI - Are there other indicators that might help the crew detect the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 1. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 1. Training/practice -Are monitoring strategies such that operators would be unlikely to detect the absence of the indication on the basis of other indicators? 3. Training/practice - Operators have learned to focus on a restricted set of available information sources.

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Small change in parameter	1. Limited discrimination - Imperceptible change in display or functionally imperceptible given competing demands 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias	1 - 5. Lack of awareness that the parameter is changing; operators assume that the value is static. 1- 5. Application of incorrect procedure step or no response	1. HMI- Lack of trending displays (e.g., use of analog meter display only) 1. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 1. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1. HMI -Other indicators whereby operators could be led to monitor or detect the small change in the parameter 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting the small change? 1 - 4. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Large change in parameter	1. Limited discrimination (display design inadequate for detecting large change) 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias	1 - 5. Failure to take account of changes in parameter in creating situation model 1 - 5. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting a large or "out-of-normal range" change in this parameter? 1 - 5. HMI - Are the indicators located where they can be easily seen by one or more crew members most of the time? 1 - 5. HMI. Is the instrument designed so that large changes might be more difficult to detect than more normal changes, e.g., indicator pegged at the top or bottom of a meter and not noticed? 1 - 5. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Lower or higher than expected value of parameter	1. Tunnel vision 2. Confirmation bias 3. Expectation bias 4. Recency bias	1 - 4. Failure to take account of changes in parameter in creating situation model. 1 - 4. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 - 4. Training/practice - Is the operators' training such that they might make assumptions about what the value of this parameter would be in this context and therefore not carefully monitor it? 1 - 4. Procedures - Are there any aspects of the procedures called for by the other parameters that could lead operators to ignore this parameter?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Low rate of change in parameter	1. Insufficient attention to processes in time? 2. Limited discrimination - Imperceptible change in display or functionally imperceptible given competing demands 3. Tunnel vision 4. Confirmation bias 5. Expectation bias 6. Recency bias	1 - 6. Failure to take account of changes in parameter in creating situation model. 1 - 6. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 -2. HMI- Lack of trending displays (e.g., use of analog meter display only) 1 - 2. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 1 - 2. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1 -2. HMI - Other indicators whereby operators could be led to monitor or detect the small change in the parameter. 1 - 2. HMI - Instrument designed so that gradual changes are not easily detectable 1 - 6. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting the small rate of change? 1 - 6. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
High rate of change in parameter	1. Insufficient attention to processes in time? 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias	1 - 5. Failure to take account of changes in parameter in creating situation model 1 - 5. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1 - 5. HMI - Are there other indications whereby operators could be led to monitor/detect the high rate of change in the parameter 1. HMI - Instruments designed so that a high rate of change might not be noticed (e.g., digital display) or they are located where they cannot be easily seen by most of the crew 1 - 5. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from detecting the small rate of change? 2 - 5. Training/practice - Similar, but different event is used repeatedly in training or was addressed in training, or is given a lot of attention in training
Delays in changes in two or more parameters	1. Insufficient attention to processes in time? 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias 6. Satisfied with limited set	Same as above	Same as above

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Detection)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Changes in two or more parameters in a short time	1. Saliency 2. Primacy 3. Recency 4. Availability (The above EMs may relate to detecting one indication over another or to failing to detect either because of earlier occurring indications) 5. Tunnel vision 6. Confirmation bias 7. Expectation bias	Same as above	Same as above and: 1 - 4. HMI - Indicators located close together so that detection of changes in one might facilitate (or in some cases interfere with) detection of changes in the other. 1 - 4. Training/Procedures - Are there any aspects of the procedures called for by one of the parameters that could lead operators to ignore the other?
One or more false indications	1. General pattern of false and genuine indications seems normal enough that operators do not detect important changes in some parameters 2. General pattern of false and genuine indications are benign enough that operators become complacent and fail to detect important changes 3. Indications misleading to the extent that operators do not monitor other important parameters	1 - 3. Failure to take account of changes in parameter in creating situation model 1 - 3. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1 -3 . HMI - Are there other indicators that might help the crew detect the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 1 - 3. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 1 - 3. Training/practice -Are monitoring strategies such that operators would be unlikely to detect the failed indicator on the basis of other indicators? 1 - 3. Training/practice - Operators have learned to focus on a restricted set of available information sources

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics

2. **Failures in Situation Assessment** - When particular parameter characteristics in Table 9.16a are identified as relevant descriptors of critical parameters in a scenario, this table is used to identify possible human error mechanisms that may facilitate *failures in situation assessment.* Possible generic UAs and potential PSFs that could contribute to the occurrence of a UA are also presented. *[Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.]*

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
No indication (or no change in the indication) for an important parameter	1. Displayed parameters lead to entry into wrong procedure step 2. Displayed parameters match incorrect mental template (similarity matching) 3. Complacency 4. Overly eager to respond 5. Simplifying 6. Recency bias	1. Application of incorrect procedure step 2, 5, 6. Incorrect SA due to missing information 3. Operators defer action on the changes indicated by other parameters 3. Fail to recognize a serious situation in time 2,4,5,&6. Take an inappropriate action, take a correct action too soon, fail to take a needed action. 1,2,3,5,&6. Miss a decision point	1& 2 HMI - Are there other indicators that might help the crew discover the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 1.& 2 - Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 3. Training/practice - Lack of discipline or trained practice in responding to all parameters 6. Training/practice - Similar event is used repeatedly in training or was addressed in training, or is given a lot of attention in training? 1,2,3,5&6. Workload - Would the operators have to work hard to identify other sources of information that could help them detect the presence of the faulty indications? Could the workload become excessive or could the situation not seem important enough to induce them to search for verification?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Small change in parameter	1. Limited discrimination - Imperceptible change in display 2. Apathy - Lack of urgent consideration of parametric change 3. Overeagerness (inclination to respond too soon)	1. Lack of awareness that the parameter is changing; operators assume that the value is static 2. Operators defer action on the changes in the parameter until other parametric needs are addressed 2. Operators disbelieve or discount a small change in this context 1 & 2 . Fail to recognize a serious situation in time 1 & 2. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1 & 2. Miss a decision point 3. Anticipate a situation and take an action too soon.	1. HMI- Lack of trending displays (e.g., use of analog meter display only) 1. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 1. Training/practice - Lack of discipline or trained practice in monitoring all parameters 1 & 2. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately considering the small change? 2. Training/practice - Lack of discipline or trained practices in responding to all parameters 2 & 3 HMI - Other indicators whereby operators could determine the significance of the small change in the parameter 2 & 3. Training/practice - Trained to cross-check this parameter?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Large change in parameter	1. Fixation - Preoccupation with parameter 2. Incredulity - Disbelief in displayed changes (sensor or instrument error) 3. Overeagerness 4. Displayed parameters match incorrect mental template (similarity matching) 5. Simplifying 6. Recency bias	1. Lack of, or reduced, attention paid to other parameters and their changes 1. Stress from concern that parameter is approaching a critical value much earlier than expected (may not match procedure). Stress may result in an inappropriate action, the taking of a correct action too soon, failure to take a needed action) 2. Failure to take account of changes in parameter in creating situation model 3,4,5,&6 . Take an inappropriate action, take a correct action too soon, fail to take a needed action	1. Training/practice - Lack of discipline or trained practice in responding to all parameters 1. Training - Lack of training or practice for off-normal accident conditions (use of FRG procedures) 1. Procedures - Omission of guidelines for unexpected plant conditions 2. Training - Lack of training in responding to "failed" parameters 2. HMI - Experience of unreliable performance of the relevant parameters 2,4,5,&6. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 2,3,4,.5,&6. HMI - Are there other indicators that might help the crew verify the accuracy of the large change in the parameter? Are they located where they can be easily seen by one or more crew members most of the time? 2,4,5,&6. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately considering a large or "out-of-normal range" change in this parameter?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Lower or higher than expected value of parameter	1. Tunnel vision 2. Confirmation bias 3. Expectation bias 4. Recency bias + all in row immediately above	1 - 4. Failure to take account of changes in parameter in creating situation model. 1 - 4. Take an inappropriate action, take a correct action too soon, fail to take a needed action + all in row immediately above	1 - 4. Training/practice - Is the operators' training such that they might make assumptions about what the value of this parameter would be in this context and therefore not carefully consider it? 1 - 4. Procedures - Are there any aspects of the procedures called for by the other parameters, that could lead operators to ignore this parameter? + all in row immediately above
Low rate of change in parameter	1. Limited discrimination - Imperceptible change in display or functionally imperceptible given competing demands? 2. Tunnel vision 3. Confirmation bias 4. Expectation bias 5. Recency bias 6. Apathy - Lack of urgent consideration of parametric change	1 - 5. Lack of awareness that the parameter is changing; operators assume that the value is static 6. Operators defer action on the changes in the parameter until other parametric needs are addressed	1. HMI- Lack of trending displays (eg., use of analog meter display only) 1. Procedure/policy/ practice - Lack of logging of parameter (to compare values over time) 6. Training/practice - Lack of discipline or trained practice in responding to all parameters

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
High rate of change in parameter	1. Fixation - Preoccupation with parameter 2. Incredulity - Disbelief in displayed changes (sensor or instrument error)	1. Lack of, or reduced, attention paid to other parameters and their changes 1. Stress from concern that the parameter is approaching a critical value much earlier than expected (may mismatch procedure). Stress may contribute to an inappropriate action, the taking of a correct action too soon, failure to take a needed action) 2. Failure to take account of changes in parameter in creating situation model	1. 1 Training/practice - Lack of discipline or trained practices in responding to all parameters 1.2 Training - Lack of training or practice for off-normal accident conditions (use of FRG procedures) 1.2 Procedures - Omission of guidelines for unexpected plant conditions 2. Training - Lack of training in responding to failed parameters 2. HMI - Experience with unreliable performance of the relevant parameters
Changes in two or more parameters in a short time	1. Need to search for a single common explanation for multiple changes	1. Delay in response while search is made for common explanation 1. Generation of false theories to explain coincidental changes in parameters	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Delays in changes in two or more parameters	1. Need to search for a single common explanation for existing changes. 2. Displayed parameters lead to entry into wrong procedure step 3. Displayed parameters match incorrect mental template (similarity matching) 4. Anticipation or confusion, overly eager to respond	1. Delay in response while search is made for common explanation 1. Generation of false theories to explain existing changes in parameters 2 & 3. Application of incorrect procedure step 3. Incorrect SA due to missing information 1 - 4. Take an inappropriate action, take a correct action too soon, fail to take a needed action.	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of delayed changes 2&3. HMI - Are there other indicators that might help the crew discover the existence of the failed instruments? Are they located where they can be easily seen by one or more crew members most of the time? 2 &3 - Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters.

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
One or more false indications	1. Displayed parameters lead to entry into wrong procedure step. 2. Displayed parameters match incorrect mental template (similarity matching). 3. Complacency 4. Overly eager to respond 5. Simplifying 6. Indications misleading to the extent that operators do not consider other important parameters.	1. Application of incorrect procedure step 2, 5, 6. Incorrect SA due to missing information. 3. Operators defer action on the changes indicated by other parameters. 3. Fail to recognize a serious situation in time 2,4,5,&6. Take an inappropriate action, take a correct action too soon, fail to take a needed action.. 1,2,3,5,&6. Miss a decision point	1& 2 HMI - Are there other indicators that might help the crew discover the existence of the false indications? Are they located where they can be easily seen by one or more crew members most of the time? 1.& 2 - Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 3. Training/practice - Lack of discipline or trained practices in responding to all parameters 6. Training/practice - Similar event is used repeatedly in training or was addressed in training, or is given a lot of attention in training 1,2,3,5&6. Workload - Would the operators have to work hard to identify other sources of information that could help them detect the presence of the faulty indications? Could the workload become excessive or could the situation not seem important enough to induce them to search for verification?

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Direction of change in parameter(s) over time is not what would be expected (if the base case scenario was operative vs. the deviation scenario) Direction of change in parameters over time, relative to each other, is not what would be expected. (if the base case scenario was operative vs. the deviation scenario) Relative rate of change in two or more parameters is not what would be expected (if the base case scenario was operative vs. the deviation scenario).	1. Expectancy bias or fixation (has been setup). 2. Operators are mislead by initial information (the information may or may not be incorrect) and fail to notice or appropriately consider later information (e.g., garden path problems, situations that change, red herrings) 3. Incredulity - Disbelief in displayed changes 4. Multiple lines of reasoning are created (conflicting choices, double binds, red herrings, dilemmas). 5. Reluctance to accept implication of later changes influences situation assessment (double binds)	1, 2,3,&4. Failure to take account of changes in parameters or fail to attend to more relevant parameters in creating situation model 13,4,&5. Generation of false theories to explain coincidental changes in parameters 1, 2,3,&5. Fail to recognize a serious situation in time 1, 2,3,4,&5. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1, 2,3,4,&5. Miss a decision point	1, 2,3,4,&5. Training - lack of training or practice for off-normal accident conditions. 1,2,3,4,&5 HMI - Are there other indicators that might help the crew discover the existence or importance of the more recent information? Are they located where they can be easily seen by one or more crew members most of the time? 1,2, & 3. Training/practice - The event indicated by the initial parameters is used repeatedly in training or was addressed in training, or is given a lot of attention in training? 1,2,&3. Training - lack of training for unexpected conditions and problem-solving

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Situation Assessment)(Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Behavior of apparently relevant parameters is actually irrelevant and misleading	1. Expectancy bias or fixation (has been set up). 2. Operators are mislead by initial information (the information may or may not be incorrect) and fail to notice or appropriately consider later information (e.g., garden path problems, situations that change, red herrings) 3. Incredulity - Disbelief in displayed changes 4. Multiple lines of reasoning are created (conflicting choices, double binds, red herrings, dilemmas) 5. Reluctance to accept implication of later changes influences situation assessment (double binds)	1, 2,3,&4. Failure to take account of changes in parameters or to attend to more relevant parameters in creating situation model 13,4,&5. Generation of false theories to explain coincidental changes in parameters 1, 2,3,&5. Fail to recognize a serious situation in time 1, 2,3,4,&5. Take an inappropriate action, take a correct action too soon, fail to take a needed action 1, 2,3,4,&5. Miss a decision point	1, 2,3,4,&5. Training - Lack of training or practice for off-normal accident conditions. 1,2,3,4,&5 HMI - Are there other indicators that might help the crew discover the existence or importance of more relevant recent information? Are they located where they can be easily seen by one or more crew members most of the time? 1,2, & 3. Training/ practice - The event indicated by the initial parameters is used repeatedly in training or was addressed in training, or is given a lot of attention in training 1,2,&3. Training - Lack of training for unexpected conditions and problem-solving

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Cont.)

3. Failures in Response Planning - When particular parameter characteristics in Table 9.16a are identified as relevant descriptors of critical parameters in a scenario, this table is used to identify human error mechanisms that may facilitate *failures in response planning.* Possible generic UAs and potential PSFs that could contribute to the occurrence of a UA are also presented. *[Note that the numbers listed with the items in the error type and PSFs columns provide a link to the error mechanism(s) to which they are expected to be related.]*

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
No indication (or no change in the indication) for an important parameter	N/A		
Small change in parameter	1. Apathy - Lack of urgency in considering response to parametric change 2. Reluctance 3. Over eagerness 4. Forget about small change when developing response plan	1 & 2. Operators defer action on the changes in the parameter until other parametric needs are addressed. 1. Take an inappropriate action or fail to take a needed action due to discounting of small change 1 & 2. Fail to develop a response to a serious situation in time or develop a faulty response plan 1 & 2. Miss a decision point 3. Anticipate a situation and take an action too soon 3. Develop a faulty response plan	1. Training/practice - Lack of discipline or trained practice in appropriately responding to all changes in parameters 1 & 2. Workload - Could the operators' workload, pre-occupation with other parameters, or expectations about what is occurring on the basis of the other parameters keep them from appropriately responding to the small change? 1 & 2. HMI - Are there other indicators whereby operators could determine the significance of the small change in the parameter 1. Training/practice - Trained to cross-check this parameter? 2. Training/practice - Operators are aware of negative consequences associated with the indicated response. 3. Training/practice - Changes in this parameter usually indicate a serious problem and a needed response

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Response Planning) (Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Large change in parameter	1. Fixation - Preoccupation with parameter 2. Incredulity - Disbelief in displayed changes (sensor or instrument error) 3. Over eagerness, over-rapid response 4. Displayed parameters match incorrect mental template (similarity matching). 5. Simplifying 6. Recency bias	1. Lack of, or reduced, attention paid to other parameters and their changes 1. Stress from concern that parameter is approaching a critical value much earlier than expected (may mismatch procedure). Stress may result in an inappropriate action, the taking of a correct action too soon, failure to take a needed action) 1,3. Rush to response overlook cautions, missteps in planning, con't question applicability, don't question conflicting information, don't wait for feedback 2. Failure to take account of changes in parameter in creating situation model 3,4,5&6. Take an inappropriate action, take a correct action too soon, fail to take a needed action	1. Training/practice - Lack of discipline or trained practices in responding to all parameters 1. Training - Lack of training or practice for responding to off-normal accident conditions (use of FRG procedures) 1. Procedures - Omission of clear response guidelines for unexpected plant conditions 2. Training - Lack of training in responding to failed parameters 2. HMI - Experience with unreliable performance of the relevant parameters 2,4,5&6. Training/practice - Are the operators trained to believe that their instruments are very reliable? Normal practice requires validation of critical parameters. 2,3,4,5,&6. HMI - Are there other indicators that might help the crew verify the accuracy of the large change in the parameter? Are they located where they can be easily seen by one or more crew members most of the time? 2,4,5&6. Workload - Could the operators' workload, pre-occupation with other parameters, or exceptions about what is occurring on the basis of the other parameters keep them from appropriately considering a large or out-of-normal range change in this parameters?
Lower or higher than expected value of parameter	Same as in two entries immediately above	Same as in two entries above + delayed action	Same as in two entries immediately above
Low rate of change in parameter	Same as small change in parameter	Same as small change in parameter	Same as small change in parameter
High rate of change in parameter	Same as large change in parameter	Same as large change in parameter	Same as large change in parameter

Table 9.16b
Error Mechanisms, Generic Error Types, and Potential Performance-Shaping Factors as a Function of Parameter Characteristics (Failures in Response Planning) (Cont.)

Parameter Characteristics	Error Mechanisms	Error Types	PSFs
Changes in two or more parameters in a short time	1. Need to search for a single common explanation for multiple changes 2.Simplifying 3. Saliency 4. Primacy 5. Availability	1. Delay in response while search is made for common explanation 1 - 5. Generation of incorrect response plans	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes
Delays in changes in two or more parameters	1. Need to search for a single common explanation for multiple changes 2.Simplifying 3. Saliency 4. Primacy 5. Availability	1. Delay in response while search is made for common explanation 1 - 5. Generation of incorrect response plans	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes
One or more false indications (one fits the other doesn't)	1. Need to search for a single common explanation for multiple changes 2.Simplifying 3. Saliency 4. Primacy 5. Availability	1. Delay in response while search is made for common explanation 1 - 5. Generation of incorrect response plans	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Lack of alternative displays to confirm validity of unexpected changes
Parameters indicate response for which insufficient resources are available or indicate more than one response option.	1. Impasse in how to proceed 2. Response dilemma introduced 3. Trade-offs	1 - 3. Generation of incorrect response plans 1 - 3. Failure to a needed response	1. Training - Lack of training for unexpected conditions and problem-solving 1. HMI - Displayed information insufficient for guiding fine tuning of response planning

10 ISSUE RESOLUTION

ATHEANA has been developed with the intention of providing a way to evaluate issues associated with human performance. Given the increasing emphasis of the NRC on risk-informed regulatory activities, this will frequently require the use of quantitative PRA-based models. The following sections describe the use of quantification methods and incorporation of their results into PRA models. It is not inevitable that the method will always be used in this way. In many cases, it may be practical to use more qualitative assessments to resolve an issue. However, the qualitative resolution of the issues will require many of the same kinds of assessments that are required in the quantification process described below. The quantification process is demonstrated in the example analyses in Appendices B - E.

10.1 Process for Issue Resolution

As discussed in Section 1 of this report, ATHEANA has been developed to provide a tool to help in resolving issues that involve human performance in high-technology environments. Section 1.4 provided examples of issues that might be addressed and Section 9.1 discussed what types of ATHEANA applications might be used. Issues may be addressed in several ways:

- qualitative analysis
- simplified quantitative analysis, typically using relative ranking of alternatives and simplified PRA models
- extensive quantitative analysis, typically using more formal quantitative methods and standard PRA models

For historical reasons, together with the recognition that many applications will involve quantitative analyses with standard PRA models, the development of ATHEANA has included appropriate detailed guidelines to perform quantification and PRA incorporation steps; these are provided in Sections 10.2 and 10.3. The following discussion concerns the process when these steps are not used.

The selection of the appropriate type of analysis is strongly influenced by the issue being evaluated (Step 1) and any restrictions on its scope imposed in Step 2 of the process. For example, if the issue is in the form: "Is there a way in which operators may be misled into turning off safety injection prematurely during a medium-break loss-of-coolant accident ?" then the analysis does not need to be quantitative. The process steps described in Section 9 present a qualitative basis for making such a judgement, since the question makes no reference to how frequently such an event (or others like it) may occur. The issue is resolved by the answer: "We found under the following conditions ... that operators can be misled into terminating safety injection prematurely during a medium loss-of-coolant accident."

Under more typical applications of ATHEANA, it is likely that the issue will be phrased in a way that requires some statement about the relative or absolute contribution to risk. In terms of the relative risk contribution, the analyst may be required to consider how likely a particular unsafe action is, given the existence of a particular error mechanism. When a quantified probability is not required, these judgments can be simplified to a relative rating of "high," "medium," or "low." Such final judgments may allow the issue to be resolved if it involves choices between alternatives (for example, is design A better than design B?) In such cases, a PRA framework allows the analyst to set out the parameters that underlie the relative likelihood(s) of the HFE(s) of interest, such as the likelihoods of the initiating event, the EFC, and the conditional probability of the unsafe actions. It is recommended that analysts performing qualitative assessments become familiar with the process for quantification described below, but recognize that in many cases the judgments described can be performed in a ranking process, rather than by assigning specific probabilities.

It is also recognized that some analyses may use simplified PRA models, or that no model exists, but a risk-based framework is needed to resolve the issue. In many cases, PRAs exist that represent to some level of accuracy the plant and the systems being analyzed; for example, IPE PRAs exist for all U.S. nuclear plants. Therefore, in very few cases will the analyst need to create a new PRA model, rather than adapt an existing model. However, some IPEs do not contain sufficient detail for all kinds of issues to be addressed. For example, simplifying assumptions may have been made about the types of dependence between the so-called frontline and support systems. In other cases, bounding assumptions may have been made for success criteria that are very pessimistic. Therefore, the analyst must consider what changes may need to be made to the PRA model to make it adequate for addressing the issue of concern. Establishing the connection between the issue of concern and the PRA model may have been started in Step 2 of the process. However, before incorporating the results of the ATHEANA analysis into an existing PRA model, the analyst must be sure that the model is appropriately sensitive to the changes.

10.2 Guidance for Quantification

ATHEANA requires a somewhat different approach for quantification from those used in earlier HRA methods. Where most existing methods have assessed the chance of human error occurring under nominal accident conditions (or under the plant conditions specified in the PRA's event trees and fault trees), quantification in ATHEANA becomes principally a question of evaluating the probabilities of specific classes of error-forcing contexts (EFCs) within the wide range of alternative conditions that could exist in the definition of the scenario, and then evaluating the conditional likelihood of the unsafe action occurring, given the occurrence of the EFC.

10.2.1 Formulation of Quantification

The foundation for quantifying human failure events is to consider three separate but interconnected stages in the process:

- the probability of the EFC in a particular accident scenario

- the conditional likelihood of the UAs that can cause the human failure event
- the conditional likelihood that the UA is not recovered prior to the catastrophic failure of concern (typically the onset of core damage as modeled in the PRA)

While this three-step quantification process is not conceptually different from the approach in other HRA methods, there are two aspects that set this method apart. First, both the UA and the failure to take a recovery action can be extremely dependent on the context; therefore consideration of these parts separate from the context and from each other is not valid. For example, when the operators, based on their assessment of the situation, believe a system is not needed and turn it off, it is very unlikely that they would revise their assessment if there was little change in the context that led to the initial termination. Even in the face of subsequent cues, the initial context often controls operator performance, as discussed later in this section and as illustrated in several of the events described in Appendix A.

Second, the relationship between the UA and the recovery opportunity is strongly dependent. For example, during the accident at TMI-2, the operators persisted in their belief that high-pressure injection should remain throttled for several hours despite contradictory indications (see the discussion of the TMI-2 event in Appendix A). In other words, once an erroneous action has taken place, the operators can persist in that belief even when the context changes; people are often very persistent in maintaining an erroneous belief (see the discussion on the psychological bases of ATHEANA in Section 4).

10.2.2 Quantification Process

The three basic elements considered in the quantification process are:
- the probability of the EFC
- the probability of the UA
- the probability of not recovering from the initial UA

Each element is discussed in turn.

10.2.2.1 Quantification of EFCs

The EFC represents the combination of plant conditions and performance-shaping factors that are judged likely to give rise to the UA. For applications of ATHEANA that are extending analyses of existing PRAs, parts of the EFC are often determined by the accident sequence path on an existing event tree. These subsets include the initiating event frequency, a partial loss of equipment, and subcategories of events in the event tree.

For example, suppose the analysis being performed is of human actions that terminate coolant injection during a medium loss-of-coolant accident (LOCA). The PRA will have an event tree showing core damage resulting from failure to achieve adequate coolant injection. The conditions

under which operators can terminate injection will be defined by one or more paths in the tree. Therefore, once the identification of an appropriate initiating event has occurred and the corresponding event tree is selected, the purpose of this step is to calculate the probability of the context arising, given an initiating event. In some cases, the EFC may occur within the definition of an accident sequence within the event tree. In that case, it may be appropriate to model the EFC as a subset of the accident sequence. In this case, the calculation of the probability of the EFC would be conditional and dependent on the occurrence of the accident sequence.

There are two separate though strongly related elements to the EFC as described earlier: the plant conditions and the performance-shaping factors. Each of these is described below.

Plant Conditions

Plant conditions encompass the physical state of the plant, the operability of equipment, and operations and evolutions that are under way. For example, plant conditions would include the initiating event and its influence on the plant. For many EFCs, the initiating event would only partially define the plant conditions. For example, in the case of a medium LOCA, the plant conditions might only apply to a narrower range of leak rates than those defined by the specification of the medium LOCA. In addition, they may include unusual failure modes or abnormal behavior of equipment modeled in the PRA and equipment not generally modeled in the PRA, such as the displays and related parts of the instrumentation and control systems.

In order to quantify the probabilities of these conditions, the ATHEANA team must gather plant-specific information. The information to be gathered depends on the EFC defined using the guidelines in Section 9. Information that might be required may include the following examples:

- frequencies of initiators (especially those defined in more detail than provided in the PRA)
- frequencies of certain plant conditions (e.g., plant parameters, plant behavior) within a specific initiator type
- frequencies of certain plant configurations, evolutions, etc.
- failure probabilities for equipment, instrumentation, indications, etc.
- dependent failure probabilities for multiple pieces of equipment, instrumentation, indicators, etc.
- unavailabilities of (especially, multiple) equipment, instrumentation, indicators, etc. due to maintenance or testing
- frequencies of restoration, calibration, and other latent human failures that result in failed (especially, multiple) equipment, instrumentation, indicators

- the probability of specific performance-shaping factors (PSFs) being present as defined in Steps 6 and 7; evaluation of additional complexity

The information needed to quantify the likelihood of the EFC using ATHEANA will depend upon the specific EFC elements identified in the search process. Since specific EFC elements and plant-specific information sources are not predictable, this section describes the collection of information in a general sense only. The ATHEANA team also must consider the plant-specific information resources that are available to them for quantification purposes.

There are several ways in which the ATHEANA team may derive information on plant condition and hardware (listed in order of preferred use):

(1) statistical analyses of operating experience
(2) engineering calculations (using assumptions, estimates, etc.)
(3) quantitative judgments from experts
(4) qualitative judgments from experts

Plant-specific operational experience (e.g., plant trip history, equipment failure histories, maintenance logs) is the principal source of statistically derived information. The ATHEANA team may have already derived some information (e.g., initiating event frequencies) for the purposes of the PRA. The team may use industry information (e.g., generic operational experience, vendor data) if plant-specific information is not available or is too sparse.

The ATHEANA team may use engineering calculations to derive EFC element probabilities or frequencies if operational experience is not available, either because the contextual factor rarely occurs or because data are not directly collected for a specific parameter or factor. Examples of such engineering are:

- the likelihood of equipment being demanded in certain situations (e.g., likelihood of a power operated relief valve (PORV) demand given a loss of offsite power transient)

- the probability of a fire spreading, once it has begun

- the time between loss of heating, ventilation, and air-conditioning (HVAC) systems and the occurrence of a room high-temperature alarm or actual temperature-related failures of equipment

In some cases, the ATHEANA team may use existing calculations (e.g., those performed to support the PRA, those used to support other engineering analyses or licensing submittals). In other cases,

new calculations may be performed or judgments made that are based on estimates using available information and simplifying assumptions.[1]

If data are not available to derive the necessary frequencies or probabilities, then the ATHEANA team should interview plant personnel in order to derive the inputs necessary for quantification. In order to elicit these expert judgments, the team should seek out the plant personnel with the appropriate topic-specific knowledge and experience. Often plant experts are unable to provide quantitative inputs directly in the form needed for quantification. The team should construct interview questions that allow the experts to use their knowledge bases. The team then will need to interpret the information provided and transform it into the form required for ATHEANA quantification. In some cases, plant-specific experts may be able to provide rough quantitative estimates based upon their past experience and knowledge that require little manipulation to transform them into inputs. In other cases, they may be able to provide only qualitative estimates that will require greater interpretation and manipulation (and probably some judgment on the part of the ATHEANA team) before producing the appropriate inputs for quantification.

Performance-Shaping Factors

Section 9.7.1 discusses two types of PSFs:

- PSFs that are triggered or activated by the plant conditions for the specific deviation scenario defined in Steps 6 and 7
- other PSFs that are not specific to the context in the defined deviation scenario

In many cases, activated PSFs will have a probability of occurrence equal to or nearly 1.0. It is critical that such activated PSFs be assessed only with respect to the context of the defined deviation scenario, and not the expected one or some other situation. For those situations in which the activated PSF is a given for the context, the probability of occurrence is 1.0. Appendices B through E contain examples of activated PSFs (such as no procedural guidance, training, or indications available for the specific context). Operator trainers or other knowledgeable plant staff should be consulted in estimating the probability of occurrence if the activated PSF is not a given. So far, there are several possibilities for the dominant factors to be considered in such an assessment. For example, within the range of conditions defined by the deviation scenario, the PSF may be a given for only a certain range of conditions. In such a case, if the frequency or probability of these conditions can be determined, then the activated PSF can be assessed. Another example would be the assessment of operator trainers that a negative PSF influences a certain fraction of the operating crews. Other possibilities for such PSF assessment will be highly dependent upon the specific deviation scenario and plant.

[1] As in any PRA analysis, assumptions should be documented. Also, if the associated HFE probability results in either a very high or very low value, the assumptions ought to be reexamined for overconservatism or oversimplification.

PSFs that are not specific (i.e., generic) with respect to context will still be plant specific.[2] First, analysts should verify that there are no plant conditions that would make the PSF more likely. If such is the case, then the analysts should consider adding these conditions to the EFC, following the guidance given in Steps 6 and 7.[3] For these cases, the analysts should follow the guidance given in the paragraph above.

If the PSFs are truly not tied to specific plant conditions, then operator trainers and other plant-knowledgeable staff should be consulted in assessing the likelihood for these PSFs. For those PSFs that are not triggered by the plant conditions, the focus of the identification of additional PSFs should be on those whose influence will be to increase the likelihood of the combination of the EFC and the UA. The addition of any non-triggered PSFs will inevitably reduce the probability of the EFC but will increase the probability of the UA, given the occurrence of the EFC. The net effect of these changes in probabilities can, in principle, either increase or decrease this combination. The analysis should focus on these PSFs where the combined probability increases. Clearly, some initial investigation is required to determine whether such a change is likely for candidate PSFs. The probability of some PSFs (e.g., suboptimal performance due to time of day or abnormal crew makeup) can be estimated from historical records (e.g., percentage of hours operated in early morning shifts, frequency of changes in the normal crew assignments). Other PSFs may be linked to a variety of factors, including informal rules (i.e., "the way we do things around here"), on-the-job training, operating and simulator experience, control room and plant design, etc. Like the assessments made for activated PSFs, these generic PSFs may or may not have a probability of occurrence equal to or nearly 1.0. In either case, the judgment of plant experts, coupled with that of the analysts applying ATHEANA, forms the basis for assessing the likelihood of these PSFs occurring.

10.2.2.2 Quantification of Unsafe Actions

There are three types of conditions that can determine how the probability of an unsafe action is estimated:

(1) The EFC is so compelling that the occurrence of the UA is virtually certain.

(2) The EFC is so noncompelling that there is no increased likelihood of the UA compared with the routine PRA context.

(3) The extent to which the EFC is compelling lies somewhere between these extremes.

---

[2] As noted in Section 9.7.1, analysts should be prudent in including such generic PSFs in the EFC. If such PSFs are judged to significantly affect the likelihood of the unsafe action occurring (i.e., the point of the next section, Section 10.2.2.2), then they should be included.

[3] This iteration in the ATHEANA process is normal and expected.

At this stage of development in ATHEANA, it is recommended that the analysis initially estimate the likelihood of an unsafe action occurring without demanding a high level of precision. In other words, for condition 1 above, the likelihood of the unsafe action occurring would be estimated at 0.5. Such a probability would be appropriate in those cases where the context faced by the operators seems entirely consistent with the operators' belief that the UA is the right thing to do in the circumstance. An example would be an event where plant information is failed or misleading, but meets procedural criteria for which there is limited or negligible redundancy, and the action is normal and expected for what the operators believe is happening. In other words, the context is overwhelmingly compelling.

For condition 2, the EFC may be considered exceptionally weak. In such cases it is recommended that the analysts use the HRA method that was used, for example, in the PRA that is being extended. In those cases where no PRA exists, the analyst is directed to the types of more traditional HRA methods, such as those discussed in Reference 10.1, which are not intended to be so focused on EFC-driven errors. (In practice, it may be that conditions that are not significantly error forcing would be identified and eliminated in the evaluations in Steps 6 and 7 of the process, which ask in effect, "Is this scenario worth considering further?")

In practice, many if not most of the contexts will fall between these extremes. In these cases, there are two possibilities for estimating the likelihood of the unsafe action given the context. These are:

(1) *Situations where experienced operator training staff have observed similar plant conditions in training and have observed a consistent fraction of crews taking the UAs being modeled.* In this case, the probability of the UA, given the plant condition, is estimated on the basis of the trainers' experience. Similarly, it is possible to poll or evaluate different crews in those cases where the action and the context are specific, but the factors that different crews may weigh are somewhat uncertain. Also, simulator trials for the UA and the associated deviation scenario can be developed and performed to inform the judgments of operator trainers if there is no relevant past experience.

(2) *Situations requiring estimation of the likelihood of a UA using modeling methods.* In this case, the analyst must employ one or more tools to provide a basis for quantification. Inevitably this will require some judgments to be made by the ATHEANA analysis team, as discussed below.

The preferred situation is one in which operator trainers can provide expert judgment as an input to the quantification of unsafe actions. However, if they are unable to provide this input (because there is no past experience or the operators, trainers, and simulator are unavailable), then modeling methods are the next best choice. Both of these approaches are discussed below.

Expert Judgment of Operator Training Staff

In those cases where the training staff have a body of experience to make judgments about the likelihood of unsafe actions because they have seen similarly challenging contexts, it is appropriate

to use this experience as a basis for quantification since it is plant and training specific. Also, simulator trials or talk-throughs of the specific EFCs may inform trainers sufficiently to make the necessary judgments.

Operator trainers are most able to provide quantitative or qualitative assessments because:

- They have the broadest knowledge base of plant-specific operating experience (i.e., their own and that of all shift and staff crews licensed at their plant).
- Because of their observations of simulator exercises and knowledge of actual operating experience, they know best how the operators at their plant perform.
- They have observed and collected statistics regarding failures in simulator exercises and, therefore, are likely to have some understanding of likelihoods for failures.
- They know how to create scenarios on the simulator that will cause operating crews to fail.

As discussed in Section 7, it is expected that training staff will be a part of the group of analysts performing ATHEANA. Also, it is expected that simulator exercises would be useful in the development of EFCs. Consequently, if the analysts have not yet used both of these resources in the ATHEANA process, they should do so now, if possible. Not only can simulator exercises support the trainers' judgments for quantification, but they can also be used to validate that the EFC is indeed challenging to operators and is likely to result in the predicted UA(s). Experience in applying ATHEANA documented in an earlier draft of this report (Ref. 10.2) showed that the training staff were invaluable in helping to define the EFC through development of the simulator trial and because of their knowledge and experience. In addition, actual performance of the simulator trial was valuable, informative, and even a little surprising to all analysts involved, including the trainers.[4]

In general, no new guidelines are proposed for performing this activity since several existing techniques are available for structuring the estimation of such probabilities [e.g., as those discussed by Seaver and Stillwell in NUREG/CR-2743 (Ref. 10.3), Budnitz et al. (Ref. 10.4), and Otway and von Winterfeldt (Ref. 10.5)]. In addition, the analyses provided in Appendices B through E and the early demonstration given in Ref. 10.2 can be used as illustrative examples of this approach to UA quantification.

Modeling Methods

In the second situation, where the analysts rather than the operator training staff must make some judgment of the likelihood of a UA, there are several approaches that can be followed. The following discussion provides two separate bases for estimating the probability. In both cases, what

[4] Based upon the results of the simulator trial performed in this early demonstration, the plant trainers decided to include this scenario in next year's training.

is required is a judgment about how relatively forcing or compelling the context is. That is, the end points of the range of possible probability values are known–they are a probability of 1.0 at one extreme and the human error probability estimated by a traditional HRA method that takes, at most, some minimal account of a "bad" context (e.g., time available or layout of a panel) at the other. Quantification of the UA in ATHEANA, therefore, must estimate where, relatively speaking, the influence exerted by the context lies. Figure 10.1 shows this concept as a graphic representation.

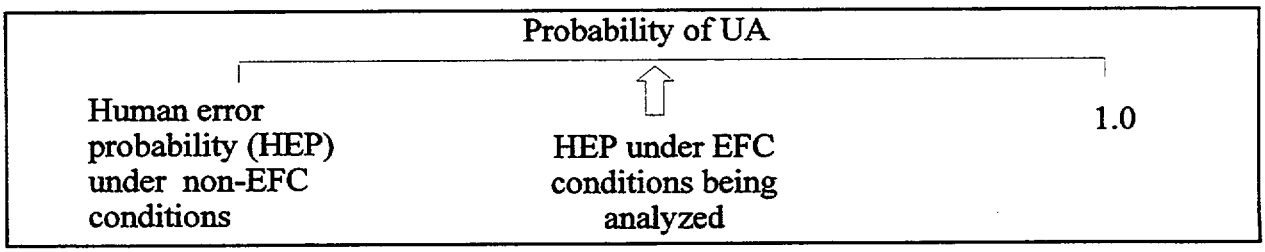


Figure 10.1 Representation of Estimation of UA Probability

In order to decide where the conditions being analyzed lie, the following guidelines are provided. It is recognized, however, that there are no absolute methods for making this judgment. The most important part of this process is for the analyst to explain the basis for the assessment, what factors are considered important, and why.

First, one HRA method, HEART (Ref. 10.6), does provide a basis for assessing the degree to which a context influences the likelihood of failure. The HEART method consists of two steps to quantify the likelihood of a UA. First, the analyst identifies a generic task description that most closely corresponds with the context of the action being analyzed. Generic task descriptions, together with their associated failure probabilities (both point value and uncertainty range), are shown in Table 10.1.

Following selection of the generic task description, there are a series of performance-shaping factors to use in adjusting the failure probabilities. (See Table 10.2.) Users wishing to use the HEART method should see Ref. 10.6 for details of applying the method in practice. In particular, use of HEART requires attention to the combinations of generic task descriptions and PSFs in Tables 10.1 and 10.2 to ensure that they do not "double-count" factors. For example, if the generic task description includes the condition that the task is "totally unfamiliar," then one does not also apply a factor for "unfamiliarity with the situation" since the effect of the EFC is already contained in the generic task probability. In addition, the application of the PSFs should be limited to the most significant two or three at the judgement of the analyst. Finally, and most obviously, the addition of PSFs to the generic task probability should be undertaken with care as the final probability of failure approaches 1.0. It is suggested that when the calculated probability exceeds 0.5 to 0.6, the analyst should carefully consider and limit the need for any additional factors. In addition, events with probabilities estimated in the range 0.1 and higher should be subject to a review process to ensure that the estimates are not overly pessimistic.

Table 10.1 HEART Generic Task Failure Probabilities

Generic Task Description	Failure Probability
Totally unfamiliar, performed at speed with no real idea of likely consequence	0.55 (0.35 – 0.97)
Complex task requiring high level of comprehension or skill	0.16 (0.12 – 0.28)
Fairly simple task performed rapidly, or given scant attention	0.09 (0.06 – 0.13)
Routine, highly practiced, rapid task involving relatively low levels of skill	0.02 (0.007 – 0.045)
Shift or restore system to a new or original state following procedures, with some checking	0.003 (0.0008 – 0.007)
Completely familiar, well-designed, highly practiced routine task occurring several times per hour, performed by highly motivated, highly trained and experienced person who is totally aware of the implications of failure, with time to correct potential errors, but without the benefit of significant job aids	$4x10^{-3}$ (8×10^{-4} – $9x10^{-3}$)
Respond correctly to system commands even when there is an augmented or automated supervisory system providing accurate interpretation of the system state	$2x10^{-5}$ ($6x10^{-6}$ – $9x10^{-4}$)

Table 10.2 HEART Performance-Shaping Factors

Error-Forcing Context	Maximum Increase in Failure Probability
Unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel	17
Insufficient time available for error detection and correction	11
A low signal/noise ratio	10
A means of suppressing or overriding information or control features that is readily accessible	9
No means of conveying spatial and functional information to operators in a form they can readily assimilate	8
A mismatch between the operators' model and that imagined by the designer	8
No obvious means for reversing an unintended action	8
A channel capacity overload, particularly one caused by the simultaneous presentation of nonredundant information	6
A need to unlearn a technique and apply another that requires the application of an opposing philosophy	6
The need to transfer specific knowledge from task to task without loss	5.5
Ambiguity in the required performance standards	5
A mismatch between the perceived and the real risk	4
Poor, ambiguous, or ill-matched system feedback	4
No clear, direct and timely confirmation of an intended action	4

Table 10.2 HEART Performance-Shaping Factors (Cont.)

Error-Forcing Context	Maximum Increase in Failure Probability
Inexperienced operator	3
Impoverished quality of information conveyed by procedures and person to person interaction	3
Little or no independent checking or testing of outputs	3

The failure probabilities calculated using HEART are typically higher than the more traditional HRA values. For example, human error probabilities in those situations where the EFC is noncompelling very often lie in a range with a lower limit of 10^{-3} to 10^{-4}, as shown by the evaluations of IPEs in NUREG-1560 (Ref. 10.7), though events for which (for example) there is a limited time for actions may have significantly higher probabilities.

In the second approach, the following approach can be used to estimate where, in the range of EFC conditions portrayed in Figure 10.1, the conditions being analyzed lie, and an interval- or scale-based tool such as the success likelihood index method (SLIM) (Ref. 10.8) can be used to estimate the failure probability.

In applying this approach, there are several questions that must be answered. These are:

- Given the context, what is the likelihood of the error mechanism being triggered?
- Given the error mechanism being triggered, what is the likelihood of the unsafe actions occurring?
- Given the occurrence of unsafe actions, what is the likelihood that they will lead to the human failure event and consequential plant damage?

SLIM can be used for each of these steps, or the assessment can be performed as an integrated assessment. The example studies in Appendices B-E principally illustrate assessment in an integrated manner.

In reviewing the characteristics of challenging conditions in Tables 9.15b and 9.16b while developing the scenario deviations, the analysts will note that specific PSFs and plant conditions are associated with specific error mechanisms and conditions. In almost all the searches used in Section 9.6, the search focuses on error mechanisms through the use of Tables 9.15 and 16. (The exception is the search for error types in Section 9.6.6 and is discussed separately below.) The more such negative PSFs and plant conditions are present in the scenario, the more likely is the occurrence of the error mechanism and, potentially, the unsafe action. Therefore the first step in assessing the

likelihood is to judge which of the plant conditions and PSFs associated with the particular error mechanisms are most important, and second the degree to which these PSFs exist in the scenario being analyzed. Analysts experienced with SLIM will recognize that these kinds of judgments are commonly performed in such cases. Since in most cases there are only a few PSFs and plant conditions identified for a particular error mechanism, the SLIM rankings and weightings can be performed efficiently on these factors.

The second stage of the assessment, the likelihood of the unsafe action given the occurrence of the error mechanism, can be assessed, again using a ranking scale. As an initial input to the analysts' judgment, the following error mechanisms are considered potentially very likely to result in an unsafe action should they occur:

- tunnel vision
- fixation
- confirmation bias
- complacency
- satisfying
- incredulity
- simple explanation for complex problems
- garden-path events
- misleading information
- masking events
- high-tempo multitasking events

This ranking is based in the number and relative severity of events that have occurred that have involved the mechanisms.[5] Events in which these error mechanisms are present can be considered to have a high likelihood of the unsafe action occurring. (The extent to which the mechanism is likely to be present was assessed in the previous step, based on the plant conditions and PSFs.)

In addition, a few error mechanisms were considered to have a low likelihood of leading to an unsafe action in a nuclear power plant setting:

- limited discrimination
- reluctance
- impasse
- late changes in plans

The remainder are assessed as having a moderate likelihood of leading to an unsafe action in a nuclear power plant setting.

[5] Event analyses that have been performed to support ATHEANA, as well as independent analyses of nuclear and non-nuclear events by others (e.g., Refs. 10.9 through 10.12), are the basis for this statement.

In general, the suggested strategy for judging the likelihood of an unsafe action implies that if any of the more global mechanisms (such as those listed in Table 9.15a, Section 9) appear to be operative in a scenario, then the unsafe action can be judged to be likely.

10.2.2.3 Quantification of Recovery

The final stage of the assessment process is to assess the likelihood that the unsafe action will persist into the failure event and therefore cause the undesired outcome–usually core damage conditions in typical power-plant PRA contexts. This third stage focuses on several recovery issues that may prevent the unsafe action from continuing to the point of core damage. These issues are:

- the occurrence of alarms and other indications following the unsafe action that may raise questions as to the correctness of the actions taken or not taken
- opportunities for new crew members (i.e., those not involved in the unsafe action) to question the on-going response
- the potential for consequential changes in the plant state to lead to new alarms and indications

Analyzing the opportunities for each of these to lead to an effective recovery of the unsafe action and termination of the accident sequence requires a somewhat detailed assessment of what the time scale is for the remainder of the accident sequence, what cues will occur, and how these cues will be assessed in light of the initial error mechanisms and the resulting unsafe action. The example analyses presented in Appendices B - E show the level of detail that can be required to assess the opportunity for recovery. For example, the sequence of cues over time must be compared with the time available for recovery in the context of the initial and developing sequences. Then the analyst must evaluate the total probability of nonrecovery for the chain of cues that will develop during the available time. (Note that the length of this chain may be uncertain. If so, then quantifying nonrecovery for the various possible cue chains, weighted by each chain's likelihood of being the correct length, will be a strong measure of the overall uncertainty in quantification of the HFE.)

Quantification of the probability of nonrecovery for the chain of cues is conditional on the original EFC, the UA, and the revised context that arises out of the UA and consequent chain of cues. There is no formula for this process. The process relies heavily on judgment based on the knowledge used in the previous steps in the quantification.

An example from an earlier ATHEANA publication (Ref. 10.13) assists the analyst in assessing the significance of context in creating a strong dependent effect. The example is based on an event at Oconee 3 that occurred during shutdown conditions in 1991 (Ref. 10.14). Before stroke testing the decay heat removal (DHR) suction valve from the recirculation sump, an operator attached a blind flange to the drop line and verified it in place. This is the large line that is used for open-loop recirculation cooling following a LOCA. Immediately after the valve was opened, a reactor building

emergency sump high-level alarm was activated. The operator took no action because this is a small sump to collect minor leakage and it fills and is pumped down routinely. The operator did not suspect a connection with the valve manipulation on the RCS boundary. So the first cue came and went without being recognized as evidence of a problem.

A short while later the second cue occurred. The operator observed that the reactor vessel level had dropped to 20 inches and was decreasing. The following table lists the full chain of cues that were generated by this event. For purposes of discussion, assume that this is the list of cues developed by the analysts to support their recovery analysis:

Table 10.3 Potential Recovery Opportunities, Oconee, 1991

Accident Symptom or Cues
E_1. Reactor building emergency sump high-level alarm
E_2. Reactor vessel level reading at 20 inches and decreasing
E_3. Reactor building normal sump high level alarm
E_4. Reactor vessel ultrasonic low level alarm (i.e., no water in hot leg pipe nozzle)
E_5. High pressure in reactor building verifies reduction in reactor vessel level and increasing radiation
E_6. Low-pressure injection (LPI) pump A current fluctuating downward
E_7. Evidence that reactor coolant system is not refilling

Now the recovery analysis would ask, "What is the probability of nonrecovery (within the available time) given the original EFC, the UAs (which have not yet been completely described), and the changes in context as a result of the UA and the string of cues." Without a consideration of the EFC and changes in context, traditional approaches that assume that the associated nonrecovery probabilities are independent would generate a probability of nonrecovery that is very low indeed. In fact, the individual non-recovery probabilities $\overline{R_1}$, $\overline{R_2}$, ... would be expected to be quite low. The argument might proceed as follows:

> *The operators have stroked a valve on the RCS boundary that is protected by a temporary blind flange, potentially opening a path to containment. It is possible that they could consider E_1 as the normal result of leakage in containment, but it is a potentially significant cue and would be investigated. Let us assign a typical conservative non-recovery probability of 0.1.*
>
> *Now, when observation shows the reactor vessel level to be decreasing, it is nearly certain that the operators will close the sump valve. They have clear evidence of a loss of RCS inventory and will certainly respond to the loss of coolant. From*

THERP (Ref. 10.15) Table 15-3 for errors of omission in carrying out written produces, we estimate the probability of $\overline{R_2}$ as 3×10^{-3}. Thus the nonrecovery probability after E_2 is $\overline{R_1} \times \overline{R_2} = 3 \times 10^{-4}$.

As the analysis continues, it is probable that the most conservative value assigned to the individual nonrecovery factors is 0.1. Let us assume that our analysts' thermal-hydraulic analysis found that by the time cue E_6 arrived, damage would already be present. In that case, the total nonrecovery probability (through E_5) would be 3×10^{-7}. But this event actually continued through E_7 over a period of about 23 minutes before the operators decided to check the line that *they had opened* to the sump, as shown in Table 10.4. Previous circumstances set them up so that they were unable to view the sequence of events as evidence of what really occurred.

Table 10.4 Recovery Opportunities vs. Actions Taken

Accident Cues	Recovery Opportunity (Table 10.3)	Actual Recovery Response
Reactor building emergency sump high-level alarm	E_1	None
Reactor vessel level reading at 20 inches and decreasing	E_2	Erroneous operation of reactor vessel wide-range level transmitter suspected
Reactor building normal sump high-level alarm	E_3	Washdown operations suspected
Reactor vessel ultrasonic low level alarm (i.e., no water in hot leg pipe nozzle)	E_4	Investigation of cause begun Entered procedure AP/3/A/1700/07, loss of LPI in DHR mode
High-pressure in reactor building verifies reduction in reactor vessel level and increasing radiation	E_5	None
Low-pressure injection (LPI) pump A current fluctuating downward	E_6	Stopped pump Opened borated water storage tank (BWST) suction isolation valves
Evidence that reactor coolant system is not refilling	E_7	Reclosed BWST isolation valves NLO sent to close 3LP-19 or -20
Event stabilized		

10.2.3 Representation of Uncertainties

Uncertainties exist in the estimates of the probabilities of the EFC, the UAs, and the recovery. The probabilities of the plant conditions are largely derived from plant experience or other operating data in the same way that many other parameters are derived in the traditional quantification tasks of a PRA. The approaches used in those traditional approaches are similarly appropriate here. For those PSFs that are independent of the context, an approach to estimating the uncertainties in the plant experience or judgment can be used that is similar to that used for uncertainties in the probabilities of the plant conditions. For those PSFs that are inherently associated with the plant conditions (such as procedures that are not applicable in the plant conditions), in most cases these PSFs have a probability of 1.0, given the plant conditions, and do not have an associated uncertainty separate from that of the likelihood of the plant conditions themselves.

In the case of the UAs, as discussed earlier, there are three different ways in which to estimate the probabilities. Different strategies provide estimates in the uncertainties in each case. First, in those cases where the probability of the UA occurring is judged to be virtually certain, the recommendation is to use an uncertainty range of 0.5 to 1.0.

Second is the case where staff have a body of experience in training for similar scenarios in which a consistent fraction of crews commit the UA of concern. If the numbers of crews being evaluated and the number of times they commit the UA are recorded, these data can be used to develop an uncertainty distribution. If experienced individuals provide the estimates and there are no recorded data, then processes exist to generate an uncertainty distribution on the basis of their collective estimates.

With regard to the use of the HEART method, uncertainty ranges are provided for the probabilities of failure for the generic task descriptions. These should be used consistent with the guidelines of the HEART method itself.

10.3 Guidance for PRA Incorporation of HFEs

Defining the HFEs, particularly in relation to the PRA, has been previously covered in Step 4 of the ATHEANA search process documented in Section 9. This guidance regarding the incorporation of the HFEs into the PRA model addresses only post-initiator HFEs. Since it is assumed that all U.S. plants already have completed human reliability analyses (HRAs) as part of their IPE submittal, the focus of this guidance is the addition of ATHEANA-generated post-initiator HFEs to PRA models, and not the modification of currently modeled HFEs. Specifically, the focus is on new errors of commission that would be identified as a result of applying the ATHEANA search scheme.

Before providing guidance on the incorporation of such events into the PRA model, it is valuable to first provide an overview of a typical PRA model as a basis for understanding how that model may need to be modified.

10.3.1 Overview of the Typical PRA Model

There is considerable variety in the details of how different PRA analysts construct a PRA model for depicting nuclear power plant severe accidents. However, nearly all recent PRAs, including those performed in response to Generic Letter 88-20 and the IPE program, use inductive logic models called "event trees" in combination with deductive models called "fault trees."

An event tree is a pictorial representation of the possible sequences of events that can occur following some initial challenge to plant operation, called an "initiating event." These sequences are usually depicted by the success or failure of functions or systems that are significant in mitigating the effects of the initiating event. Necessary and sufficient combinations of functional and system successes lead to a successful plant response to an initiating event; while sufficient failures are predicted to lead to damage to the reactor core, fission product release, and possible containment failure and release to the environment.

Fault trees are mostly used to model plant responses at a lower, more detailed component level. Fault trees are deductive models that depict the combinations of failed equipment that must occur in order to fail the functions and systems of interest in the event trees. The basic events in the fault tree models represent the unavailability or failure states of plant equipment, with the models constructed at a level commensurate with available failure data.

"Quantifying" the PRA means calculating the predicted frequencies of the sequences of events that lead to core damage. This is accomplished conceptually by first determining the probabilities of failure of the functions or systems in the model. The combination of these probabilities with the expected frequencies of the initiating events determines the expected frequencies of the undesirable core damage sequences. The resulting solution process provides a series of expressions, each made up of the product of the initiating event and various basic event failures that together lead to damage to the reactor core. Each expression is called a cut set with each cut set having an associated frequency. Combining the frequencies of each cut set related to a single sequence yields an overall frequency for that sequence. Combining the sequence frequencies yields the overall expected rate of occurrence (usually expressed as a probability per year) of core damage.

Figure 10.2 is a simplified depiction of how the above modeling and data interrelate to form the PRA model. The extent to which the different modeling techniques are used and combined depends on such things as PRA scope and plant mode being analyzed (e.g., full power, refueling), analyst preference, and whether a detailed or only a screening analysis is required, among other factors. However, the above description, at least conceptually, encompasses the typical PRA modeling approach used by today's analysts.

10.3.2 Treatment of Human Failure Events in Existing PRAs

In order to address how to include the ATHEANA human failure events in the PRA model, it is first necessary to understand how PRA models typically incorporate human failure events. There are four

places where human failure events are typically incorporated into the PRA model. These are shown in Figure 10.3 by highlighting the human modeling interfaces with the basic PRA model depiction shown in Figure 10.2. Each interface is discussed below.

10.3.2.1 Human-Induced Initiating Events

The first place in the PRA model structure where human failure events are included (albeit implicitly) is in the identification of the initiating events and their expected frequencies. For a typical at-power PRA, initiating events include such challenges to the plant as turbine trips, loss of feedwater, steam generator tube rupture, loss of offsite power, loss-of-coolant accidents, inadvertent flow diversions during shutdown, earthquakes, etc. Many of these initiators can be induced by human failures, such as inadvertently causing a reactor scram during a half-scram test of the reactor protection circuitry. Since the frequencies of such initiating events induced by human failure are accounted for in the frequency for each class of possible initiators, oftentimes these events are not specifically modeled in the PRA. This is done for three reasons: first, it is assumed (even if implicitly) that there is little or no dependence between the cause of the initiating event and how plant staff will respond to subsequent events. Second, depending on the scope and objectives of the analysis, usually the PRA analyst only requires the initiating event frequency for the analysis and it is not necessary to understand why or how the event is initiated. Third, in at-power PRAs, the human contribution to initiators is often considered to be small compared with that of hardware failures.

10.3.2.2 Human Failure Events in Event Trees

Oftentimes the event trees in the PRA model explicitly depict human failure events in the logic. Figure 10.4 provides an illustration. There is no industry-wide accepted rule or standard as to when to include such events in the event tree structure. However, this is usually done when the human action of interest is a key part of numerous sequences in the event tree and the action is not particularly associated with a specific system or equipment item, but instead has functional repercussions regarding whether there is a successful recovery or whether core damage occurs. Sometimes, such events must be included in event trees to highlight the human failure event as a potentially important part of the entire sequence of events that might occur. In current PRAs, these human failure events nearly always involve errors of omission, such as failure to depressurize the primary system when a steam generator tube is ruptured, failure to initiate feed and bleed, or failure to provide coolant level control in a boiling-water reactor (BWR) anticipated transient without scram (ATWS).

10.3.2.3 Human Failure Events in Fault Trees

Such human failure events may be modeled in the appropriate fault trees if the action of interest is more easily associated with a specific system or equipment item in the plant, and failure of that action can contribute to the failure of that system or equipment to perform its desired function. Figure 10.5 provides an illustration. Here the analyst attempts to define all the ways that human

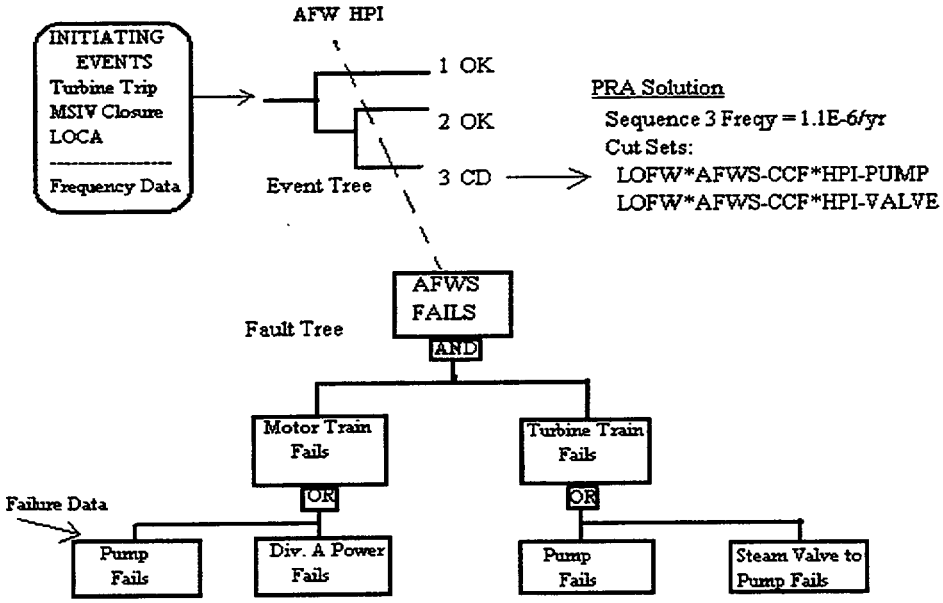


Figure 10.2 Overview of PRA Modeling.

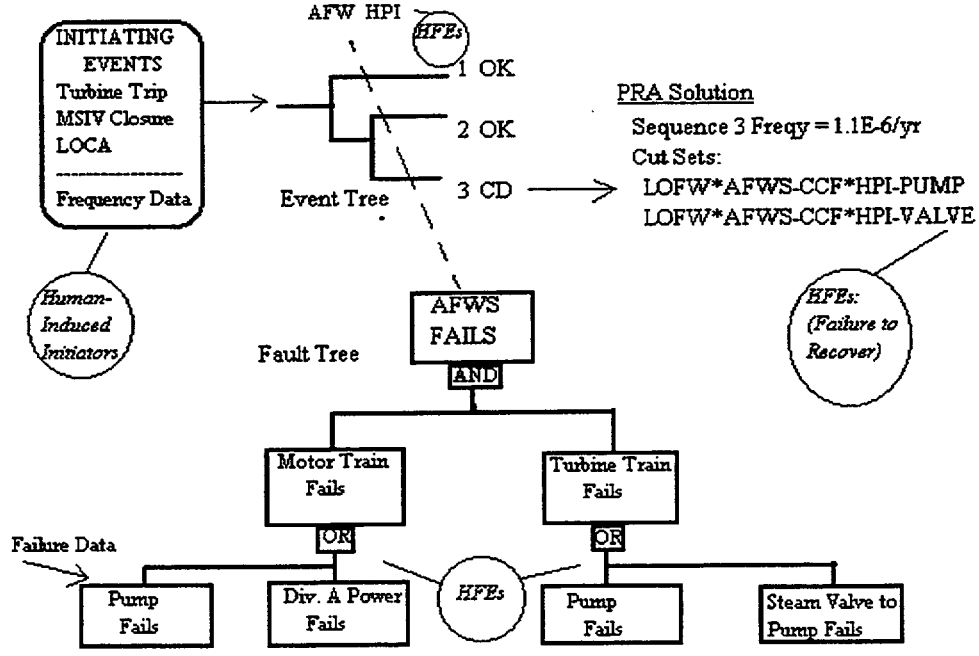


Figure 10.3 Overview of PRA Modeling with HFE Interfaces Shown.

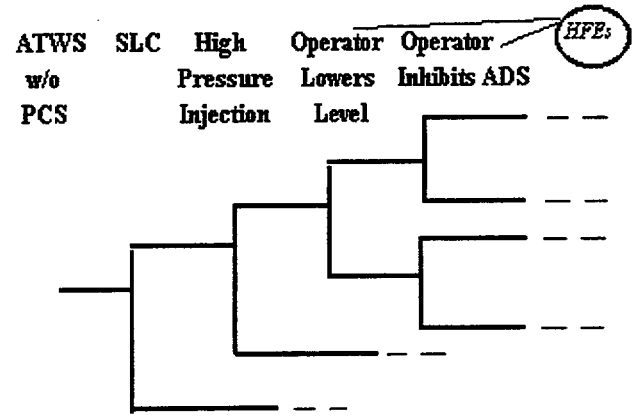


Figure 10.4 Illustration of HFEs in Event Trees

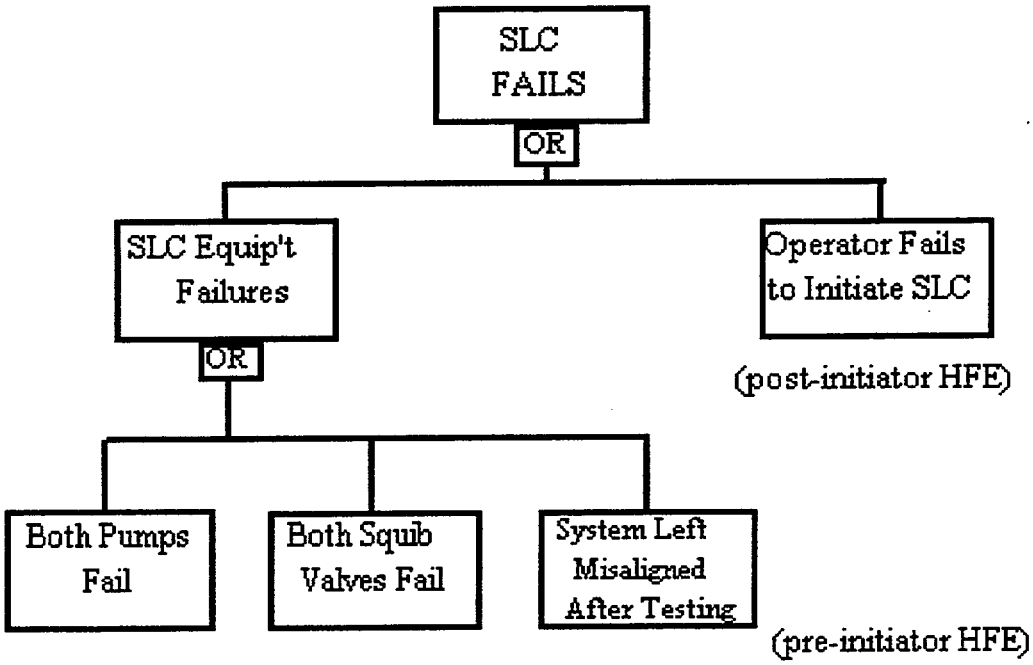


Figure 10.5 Illustration of HFEs in Fault Trees.

failures can credibly contribute to failure of the system or equipment of interest and estimates the probability of that failure, eventually in the context of each sequence in which the failure of that system or equipment plays a role. The human failure events in the fault trees tend to include the following:

- so-called pre-initiator errors involving omissions in maintenance, testing, or calibration activities that leave the equipment in a nondetected failed state so that the equipment cannot respond properly when an initiating event occurs

- post-initiator events such as that shown in Figure 10.5 involving omissions in responding to sequences of events following an initiating event

10.3.2.4 Failures to Perform Specific Recovery Actions

Not every combination of equipment failure that leads to core damage can be predetermined before the model is solved, and for other calculation and modeling efficiency reasons, a variety of failure-to-recover events are added to the PRA model during the last stages of quantification. This involves analyst examination of the sequence cut sets derived from solution of the PRA model, and on the basis of the combinations of failures in each cut set leading to core damage, the analyst postulates reasonable recovery actions that can be taken by the plant staff to change the outcome from core damage to successful mitigation of the accident. Failure to take the desired recovery actions is included in the PRA model. This is done by adding events representing such failures to the sequence cut sets, thereby accounting for the probability that the plant staff will not be able to find a way to avert the core damage outcome by performing an action not explicitly included in the original model. Examples of such failure-to-recover events and how they are implemented in the model cut sets are shown in Figure 10.6.

10.3.3 Incorporating ATHEANA Human Failure Events in the PRA Model

The following sections offer recommendations on how to incorporate the ATHEANA-defined human failure events in an existing typical PRA model.

10.3.3.1 Human-Induced Initiating Events

Since plant and industry experience data are used to identify and quantify the frequencies of most initiating events, no general requirement exists regarding the decomposition of initiators into those that are human induced and those that are not. Nor is it necessary to model how such human-induced initiators might occur. Examination of actual experience can provide these insights and hence, by using a modeling and quantification approach like ATHEANA, it is oftentimes not necessary to build or quantify the PRA model.

Sequence Cut Sets Before Recovery:

TMFW * AFWS-CCF * HPI-CCF
TMFW * AFWS-CCF * SWS-CCF
TMFW * AFWS-HVAC * HPI-CCF

Sequence Cut Sets after Recovery:

TMFW * AFWS-CCF * HPI-CCF * OPER-DEP-COND
TMFW * AFWS-CCF * SWS-CCF (no recovery action)
TMFW * AFWS-HVAC * HPI-CCF * OPER-DOOR

where: TMFW = initiator; loss of main feedwater
AFWS-CCF = common-cause failure of AFWS
HPI-CCF = common-cause failure of HPI for feed and bleed
SWS-CCF = common-cause failure of service water
OPER-DEP-COND = operator failure to depressurize and use condensate for steam generator feed
OPER-DOOR = operator failure to open doors of AFWS rooms for ventilation

Figure 10.6 Illustration of Failure-to-Recover Events in Cut Sets.

However, this applies only when there is little or no dependence between the cause of the initiating event and how the plant staff will respond as the sequence of events unfolds. If there may be a relationship between the initiating event and subsequent staff response, the ATHEANA process will help uncover such relationships through identification and definition of error-forcing contexts. In such cases, it may be desirable to develop or modify existing PRA models to add specific initiator-causing HFEs found to be of potential interest using ATHEANA (i.e., some HFEs may be analyzed as separate initiating events).

10.3.3.2 Human Failure Events in Event Trees

This is the portion of the model where incorporation of the ATHEANA process will often take place. Because the highest priority HFEs defined by ATHEANA tend to lead directly to the undesired outcome (i.e., core damage for nuclear plants), the event tree structure is the ideal portion of the PRA model to incorporate such HFEs. These events should be identified considering the initiating event being addressed, the related successes and failures associated with the undesired sequences containing the HFEs, and the possible error-forcing contexts accounted for using the ATHEANA process. The HFEs should be defined so as to capture errors of commission (of highest priority) and errors of omission that are missing from the present PRA model and that would cause the undesired overall effect. For example, core cooling in the form of feed-and-bleed may not be successful because the operator fails to initiate it (a form of omission that is usually found in current PRAs) or

because the operator prematurely stops feed-and-bleed, thinking that it is no longer required (an error of commission to be added using ATHEANA).

The specific location of the ATHEANA HFEs in the event tree is largely a matter of analyst preference. However, as is done currently in placing events in event trees, the expectation is that the placing of an additional ATHEANA HFE in an event tree will depend on how it relates chronologically to the demand of functions and systems involved in responding to the initiating event, where its inclusion will provide the most efficient analysis of all the possible sequences depicted by the event tree and the logical dependencies of other events to the HFE in the sequence.

In addition, it may be desirable or even required that if subsequent successes or failures in a sequence would significantly alter treatment of the incorporated HFE (e.g., by providing new cues for action), the event tree may need to include multiple HFEs that are similar. However, definition and/or quantification would be different because of possible differences in timing, the plant status, etc.

Figure 10.7 illustrates one possible way to incorporate ATHEANA HFEs into a PRA event tree. In this illustration, the incorporation accounts for human failure to initiate or otherwise maintain the required function (in this case-core cooling) until a successful outcome is achieved. In this case, the HFE is included by adding a separate event tree branch that leads directly to core damage. The HFE must obviously be defined in such a way that the undesired outcome will be a direct result.

10.3.3.3 Human Failure Events in Fault Trees

At least conceptually, incorporation of the ATHEANA method into the event trees may allow elimination of some of the high-level, functional, or system-related HFEs currently modeled in the fault trees as post-initiator errors. This is because the anticipated ATHEANA HFEs will include within their scope and definition those events (typically only errors of omission) currently in the PRA fault trees. For example, "failure to align the enhanced flow mode of control rod drive (CRD) injection" in a BWR PRA may be an existing human failure event in the fault tree for the CRD system. An ATHEANA-defined HFE involving the "failure to ensure adequate injection (regardless of the system)" added to the event tree would eliminate the individual CRD human failure event in the CRD fault tree since such a failure would be encompassed by the broader ATHEANA HFE definition. However, the pre-initiator HFEs and some equipment-specific post-initiator HFEs will remain in the fault trees.

While the ATHEANA development to date has not been aimed at addressing events such as pre-initiator HFEs, the scope, definition, and quantification of these events already in the PRA could be different. Not only would the current errors of omission be considered, but these HFEs could also include errors of commission taking into account error-forcing contexts that may cause the undesired pre-initiator or equipment-specific HFE. Note that the development of ATHEANA has not focused on these types of events, but instead is on the broader events directly leading to core damage, as discussed in the event tree subsection.

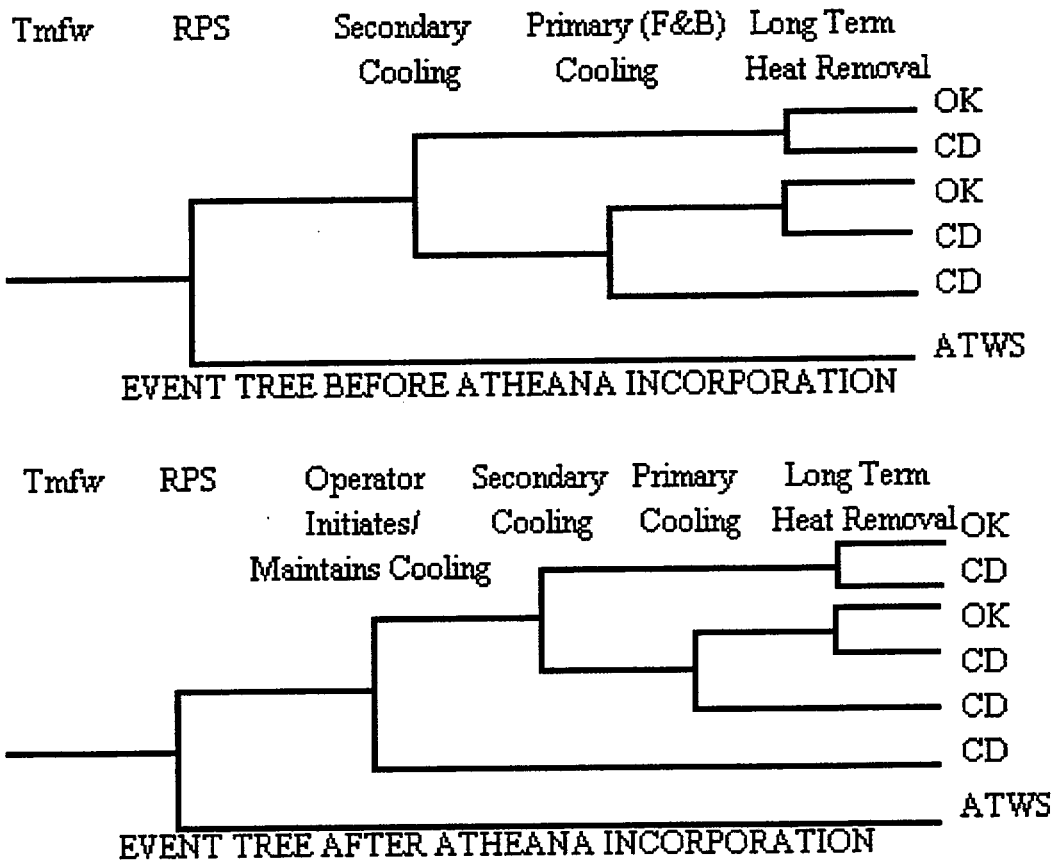


Figure 10.7 Illustration of Incorporating an ATHEANA HFE in an Event Tree.

10.3.3.4 Failures to Perform Specific Recovery Actions

As with the fault trees, some of the recovery events normally added to the cut sets after initial solution and quantification of the PRA model may be eliminated, but only when the ATHEANA HFEs are broadly defined to include failure to recover from the original error, as is intended with the ATHEANA process. For example, "failure to switch over to an alternative water source " could be an existing recovery event added to cut sets involving loss of a primary water source. However, if an ATHEANA-defined HFE has been added to the model which involves the "failure of ensuring an adequate water supply (including consideration of switching to an alternative source when necessary)", then the existing recovery event is no longer needed, since the broader-defined ATHEANA event already encompasses the recovery failure.

Until the initial solution of the PRA model is obtained, all possible recovery considerations may not become evident. Some recovery events may therefore still need to be applied as is currently done.

10.3.3.5 Overall Sequence Quantification Considerations

As with the current PRA practices, the analyst should exercise care in the final quantification of the accident sequences. The ATHEANA incorporation process may reduce the overall number of different HFEs in the model and the number of times multiple HFEs appear in the same cut set (because of the broadly defined HFEs often identified using ATHEANA). However, entire elimination of multiple HFEs in the same cut set may not be possible. When this condition does occur, the analyst must still address the same issues of dependencies among the HFEs in a cut set during final sequence quantification using existing HRA/PRA technology.

10. 4 References

10.1 ASME, A Proposed National Standard: Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, Draft Released for public review and comment, ASME RA-S-1999, draft edition #10, February 1, 1999.

10.2 U.S. Nuclear Regulatory Commission, Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA), Draft report for comment, NUREG-1624, U.S. Nuclear Regulatory Commission, May 1998.

10.3 D. Seaver and W.G. Stillwell, *Procedures for Using Expert Judgment to Estimate HEPs in Nuclear Power Plant Operations,* NUREG/CR-2743, Idaho National Engineering Laboratory, Idaho Falls, ID 1983.

10.4 R.J. Budnitz, G. Apostolakis, D.M. Boore, K.J. Coppersmith, C.A. Cornell, and P.A. Morris,, *Recommendation for Probabilistic Seismic Hazard Analysis Guidance on Uncertainty and Use of Experts*, NUREG/CR-6372, Lawrence Livermore National Laboratory, Livermore, CA, April 1997.

10.5 H. Otway, and O. von Winterfeldt, "Expert judgement in risk analysis and management: Process, context and pitfalls." *Risk Analysis* pp. 12(1): 1992.

10.6 J. C. Williams, A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance, Paper presented at 1988 IEEE Fourth Conference on Human Factors and Power Plants, IEEE, 1988.

10.7 U. S. Nuclear Regulatory Commission, *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance,* NUREG-1560, U.S. Nuclear Regulatory Commission, Washington, DC, December 1997.

10.8 D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea, SLIM-MAUD: *An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment,* Brookhaven National Laboratory: NUREG/CR-3518, Upton, NY, 1984.

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

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

10.11 R. J. Mumaw and E. M. Roth, How to be more devious with a training simulator: Redefining scenarios to emphasize cognitively difficult situations. *In 1992 Simulation MultiConference: Nuclear Power Plant Simulation and Simulators*, 1992.

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

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

10.14 U.S. Nuclear Regulatory Commission, *Oconee Unit 3, March 8, 1991, Loss of Residual Heat Removal*, Regional Augmented Inspection Team Report No. 50-287/91-008, U.S. Nuclear Regulatory Commission, Washington, DC, April 10, 1991.

10.15 A.D. Swain and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque, NM, August 1983.

11 PERSPECTIVE ON ATHEANA

The techniques for performing risk and reliability assessments have significantly improved over the past few decades. These assessments have become effective tools for identifying and understanding the nature of risks associated with modern technologies such as nuclear, chemical, air and surface transportation. However, in spite of the valuable information gained from such analyses and the improvements made to these modern technologies, few people, including most analysts, genuinely believe that these analyses provide a comprehensive understanding of the related risks and serve as accurate indicators of future accidents.

The reason for this criticism is in part due to the general belief that human reliability analysis techniques are still relatively immature, and our experiences demonstrate that the risks of severe accidents in these technologies are likely to involve a key human contribution as evidenced by Three Mile Island, Chernobyl, the Air Florida crash, etc. Hence, if the risks of severe accidents are going to be successfully managed or reduced, the human element of the risk must be better understood and estimated, and ways must be found to (a) maintain or improve the chances for correct operator intervention and (b) avoid introducing conditions that will enhance the chances of operator error.

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

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

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

ATHEANA provides a structured way to investigate how conditions of the technology and influences on operator performance may coexist in ways that could set up operators to carry out critical unsafe acts that may lead to undesired consequences. Methods have been developed for performing both retrospective analyses of past events and prospective analyses of potential future events. While structured, these methods allow for flexibility in their implementation and take advantage of the knowledgeable brainstorming creativity of the analysts.

ATHEANA provides an approach for more effectively combining the possible conditions of the technology with considerations that govern human performance so as to identify circumstances that could be more error forcing (i.e., make operators more likely to fail). It does this by building on the

principles and techniques of human behavioral science and HRA methods that have come before it. It has also benefitted from a prior peer review which is summarized in Appendix F.

The examples of prospective analyses and retrospective analyses provided here demonstrate the use of ATHEANA and illustrate the kinds of observations and findings that are possible when this approach is used. These types of results can provide users of ATHEANA with a better understanding of why humans may perform unsafe acts in certain situations.

It is the authors' hope that application of ATHEANA will provide users with new insights into the human contribution to risk, and therefore be useful in identifying ways to lessen the chances or consequences of severe accidents in the future.