NUREG/CR-6350
BNL-NUREG-52467

# A Technique for Human Error Analysis (ATHEANA)

## Technical Basis and Methodology Description

Prepared by
S. E. Cooper, SAIC
A. M. Ramey-Smith, NRC
J. Wreathall, WWG
G. W. Parry, NUS
D. C. Bley, WWG
W. J. Luckas, J. H. Taylor, M. T. Barriere, BNL

**Brookhaven National Laboratory**
**Science Applications International Corporation**
**Halliburton NUS Corporation**
**The WreathWood Group**

**Prepared for**
**U.S. Nuclear Regulatory Commission**

## AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555-0001

2. The Superintendent of Documents, U.S. Government Printing Office, P. O. Box 37082, Washington, DC 20402-9328

3. The National Technical Information Service, Springfield, VA 22161-0002

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the Government Printing Office: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grantee reports, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

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 can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852-2738, for 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 the American National Standards Institute, 1430 Broadway, New York, NY 10018-3308.

## DISCLAIMER NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

NUREG/CR-6350
BNL-NUREG-52467

# A Technique for Human Error Analysis (ATHEANA)

## Technical Basis and Methodology Description

Manuscript Completed: April 1996
Date Published: May 1996

Prepared by
S. E. Cooper, SAIC
A. M. Ramey-Smith, NRC
J. Wreathall, WWG
G. W. Parry, NUS
D. C. Bley, WWG
W. J. Luckas, J. H. Taylor, M. T. Barriere, BNL

Brookhaven National Laboratory
Upton, NY 11973

Subcontractors:
Science Applications International Corporation
Reston, VA 22090

Halliburton NUS Corporation
Gaithersburg, MD 20878

The WreathWood Group
Dublin, OH 43016

A. M. Ramey-Smith, NRC Project Manager

**Prepared for**
**Division of Systems Technology**
**Office of Nuclear Regulatory Research**
**U.S. Nuclear Regulatory Commission**
**Washington, DC 20555-0001**
**NRC Job Code L2415**

# ABSTRACT

Probabilistic risk assessment (PRA) has become an important tool in the nuclear power industry, both for the Nuclear Regulatory Commission (NRC) and the operating utilities. Human reliability analysis (HRA) is a critical element of PRA; however, limitations in the analysis of human actions in PRAs have long been recognized as a constraint when using PRA.

A multidisciplinary HRA framework has been developed with the objective of providing a structured approach for analyzing operating experience and understanding nuclear plant safety, human error, and the underlying factors that affect them. The concepts of the framework have matured into a rudimentary working HRA method. A trial application of the method has demonstrated that it is possible to identify potentially significant human failure events from actual operating experience which are not generally included in current PRAs, as well as to identify associated performance shaping factors and plant conditions that have an observable impact on the frequency of core damage.

A general process was developed, albeit in preliminary form, that addresses the iterative steps of defining human failure events and estimating their probabilities using search schemes. Additionally, a knowledge-base was developed which describes the links between performance shaping factors and resulting unsafe actions.

## CONTENTS

## CONTENTS (Cont'd)

APPENDICES:

# LIST OF FIGURES

## LIST OF TABLES

# EXECUTIVE SUMMARY

## Background

Probabilistic risk assessment (PRA) has become an increasingly important tool in the nuclear power industry, both for the Nuclear Regulatory Commission (NRC) and the operating utilities. The NRC recently published a final policy statement, SECY-95-126, encouraging the use of PRA in regulatory activities. Human reliability analysis (HRA), while a critical element of PRA, has limitations in the analysis of human actions in PRAs that have long been recognized as a constraint when using PRA. In fact, better integration of HRA into the PRA process has long been a NRC issue. Of particular concern, has been the omission of errors of commission - those errors that are associated with inappropriate interventions by operators with operating systems.

To address these concerns, the NRC identified the need to develop an improved HRA method, so that human reliability can be better represented and integrated into PRA modeling and quantification.

## Description of the Project

The purpose of the Brookhaven National Laboratory (BNL) project, entitled "Improved HRA Method Based on Operating Experience" is to develop a new method for HRA which is supported by the analysis of risk-significant operating experience. This approach will allow a more realistic assessment and representation of the human contribution to plant risk, and thereby increase the utility of PRA. The project's completed, ongoing, and future efforts fall into four phases:

1) Assessment Phase (FY 92/93, documented in NUREG/CR-6093)
2) Analysis and Characterization Phase (FY 93/94, documented in NUREG/CR-6265)
3) Development Phase (FY 95/96, documented in this report)
4) Implementation Phase (FY96, planned)

## Overview of the Results

The Analysis and Characterization Phase (documented in NUREG/CR-6265) developed a multidisciplinary HRA framework with the objective of providing a structured approach for analyzing operating experience and understanding nuclear power plant (NPP) safety, human error, and the underlying factors that affect them. The framework had to be multidisciplinary because the factors affecting human reliability and plant safety are based on many sciences. In the current Development Phase, which is the subject of this report, the concepts of the framework have matured into a working HRA method, with identified process steps. This working HRA method, albeit in preliminary form, has been expanded by using trial applications concluding in quantification of a human failure event.

## The ATHEANA HRA Method

The new HRA method, called ATHEANA (A Technique for Human Error Analysis), improves the ability of PRAs to:

- identify and characterize important human-system interactions and their likely consequences under accident conditions;

- represent the most important severe accident sequences that could occur;

- provide recommendations for improving human performance based upon characterizations of the causes of human errors.

In order to achieve these goals in the development of the new HRA method, ATHEANA, it was necessary to establish a new basis for HRA modeling, starting with the development of a better understanding of human performance in serious nuclear power plant accidents and their precursors. ATHEANA is based on a multidisciplinary framework that considers both the human-centered factors (e.g., performance shaping factors such as human-machine interface design, procedures content and format, and training) and the conditions of the plant that give rise to the need for actions and create the operational causes for human-system interactions (e.g., misleading indications, 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; the combined effect of performance *shaping* factors (PSFs) and plant conditions that create a situation in which human error is likely to occur is an "error-forcing context"

Considerable research was conducted on the various HRA elements of the ATHEANA framework. The representation of human error encompasses both the underlying mechanisms of human error and the consequences of the error mechanism, which is the unsafe action, whose consequences on the system are represented in the PRA model by the human failure event (HFE). The error mechanisms are behavioral and cognitive mechanisms causing human errors, that can be triggered by particular plant conditions and PSFs. When applied in the wrong context, error mechanisms can lead to inappropriate actions that can have unsafe consequences that lie within the PRA definition of accident scenarios. "Unsafe actions" are those actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition. Unsafe action does not necessarily imply that humans are a root cause; people are often set-up by circumstances and conditions to take actions that are unsafe.

In addition to the psychological developments discussed above, analyses of accidents and serious incidents have both confirmed the principles underlying ATHEANA and precipitated the identification and development of these principles. The results of these operational event analyses are formulated in a manner that supports use of ATHEANA. These results are captured in a database which has been developed for this project.

ATHEANA has been developed with the goal of being used in traditional PRA models. In other words, application of ATHEANA will not require major changes to the mechanics of how PRA models are constructed. Furthermore, ATHEANA will be usable by a PRA analyst, using input from experts such as those knowledgeable of plant design and operations, but will not need to rely on having extensive experience in human factors or psychology.

### Trial Application of the Concepts

A trial application of ATHEANA was conducted using the following process steps. (It should be noted that the quantification of a HFE based upon the likelihood of EFC's occurring represents a fundamental shift in the conduct of HRA.):

- identification of a human failure event (HFE)
- identification of an unsafe action associated with the HFE
- identification of an error-forcing context (EFC) associated with the unsafe action

- estimation of probabilities for each EFC
- quantification of the HFE using the estimated EFC probabilities

For the purposes of the trial application, a PWR small-break LOCA was selected. The specific PRA used in the trial application was the Surry Unit 1 NUREG-1150 PRA. An existing PRA was used so that comparisons could be made between the original PRA and the trial application. As is typical, the sample PRA only modeled human errors of omission. However, to demonstrate the value of ATHEANA, the success of the high pressure injection function was examined and ways in which the operators can fail this function were identified, based upon knowledge gained on the project to date from human factors research and event analyses. As a result, the HFE identified in the trial demonstration was "operators inappropriately terminate HPI". The unsafe action, associated with the HFE, that was selected for the demonstration was described as "Operators turn off operating HPI pumps, given the mistaken belief that the safety injection (SI) termination criteria given in procedures have been satisfied."

Actual plant procedures were used to identify an error-forcing context (EFC) that could induce the unsafe action and resulting HFE that were selected for the trial application. The EFC selected was: a stuck open power operated relief valve causing pressurizer level indication to read incorrectly, coupled with PSFs and errors in information processing. A quantification demonstration resulted in an HFE probability of 7.5E-4 and a core damage frequency of 1.5E-5. These calculations demonstrate that HFEs can be significant contributors to plant risk when considered under an appropriate EFC.

Findings

The trial application was a "proof of concept" for ATHEANA; it demonstrated that it is possible to identify and estimate the probabilities of HFEs (and associated EFCs) that have an observable impact on the frequency of core damage, and which are generally not included in current PRAs.

A general process was outlined that addresses the iterative steps of defining HFEs and estimating their probabilities using search schemes.

A knowledge-base was developed with the objective of describing the links between unsafe actions and error-forcing contexts, and is based on behavioral science theory and analysis of NPP events.

Future Work

There are several activities that are required to complete the development of ATHEANA. The most important of these activities is the development of the ATHEANA application tools. These tools are 1) the implementation guidelines, which is to be a "how to" document, and 2) the frame-of-reference (FOR) manual, which is a technical basis document. The precursors to these tools presented here have been based on trials of only a few relatively simple example scenarios. The search schemes, in particular, are rudimentary and need to be developed to a more comprehensive level. Hence, to validate the methodology, larger scale demonstrations should be conducted, perhaps including demonstration in a full scale PRA.

In addition to its intended use of providing more comprehensive HFEs and more accurate quantification, other valuable uses of the ATHEANA methodology should be examined, such as root cause analysis and a structured approach to incident analysis/investigation to identify and correct the underlying causes of human error.

## ACKNOWLEDGEMENTS

Her fellow co-authors wish to give Ann Ramey-Smith special thanks for her enduring NRC/RES project management, guidance, and support. Also, the encouragement and guidance of Joseph A. Murphy and Mark A. Cunningham continue to be constructive and are appreciated. In addition, Catherine M. Thompson is acknowledged for her contributions to the project.

We also extend our gratitude to our colleagues at Brookhaven National Laboratory who provided insights and constructive reviews of the work associated with this report: James C. Higgins and Robert E. Hall. Special thanks are given to Pamela L. Ciufo for her outstanding assistance in preparing the manuscript.

## ACRONYMS

| | |
|---|---|
| AEOD - | NRC Office of Analysis and Evaluation of Operational Data |
| ATHEANA - | A Technique for Human Error ANAlysis |
| AIPA - | Accident Initiation and Progression Analysis |
| ASEP - | Accident Sequence Evaluation Procedure |
| ATWS - | Anticipated Transient Without Scram |
| BNL - | Brookhaven National Laboratory |
| BWR - | Boiling Water Reactor |
| CADA - | Critical Action and Decision Approach |
| CBDTM - | Cause Based Decision Tree Method |
| CES - | Cognitive Environment Simulation (human performance model)) |
| CM - | Confusion Matrix |
| CREAM - | Cognitive Reliability and Error Analysis Method |
| DNE/EE - | Direct Numerical Estimation/Expert Estimation |
| EFC - | Error-Forcing Context |
| EFW - | Emergency Feedwater |
| EOC - | Error of Commission |
| EOO - | Error of Omission |
| EOP - | Emergency Operating Procedure |
| ESF - | Engineering Safeguards Features |
| ESFAS - | ESF Actuation Signal (or System) |
| FMEA - | Failure Mode and Effects Analysis |
| FOR - | Frame-of-Reference (manual) |
| HAZOP - | HAZard and OPerability Study |
| HCR - | Human Cognitive Reliability model |
| HEART - | Human Error Rate Assessment and Reduction Technique |
| HEP - | Human Error Probability |
| HRMS - | Human Reliability Management System |
| HSECS - | Human System Event Classification Scheme |
| HFE - | Human Failure Event |
| HMI - | Human-Machine Interface |
| HPI - | High Pressure Injection |
| HRA - | Human Reliability Analysis |
| I&C - | Instrumentation & Control |
| INTENT - | Human error rate assessment for INTENTion-based errors |
| IPM - | Information Processing Model |
| KB - | Knowledge-Based |
| LBLOCA - | Large-Break LOCA |
| LOOP - | Loss of Offsite Power |
| LOCA - | Loss of Coolant Accident |
| NRC - | U.S. Nuclear Regulatory Commission |
| NRR - | NRC Office of Nuclear Reactor Regulation |
| MAPPS - | MAintenance Personnel Performance Simulation model |
| MORT - | Management Oversight and Risk Tree analysis |
| MSFM - | Multiple-Sequential Failure Model |
| NPP - | Nuclear Power Plant |
| $N_2$ - | Nitrogen Gas |
| OAT - | Operator Action Tree system |

## ACRONYMS (Cont'd)

| | |
|---|---|
| ORCA - | Operator Reliability Calculation and Assessment |
| ORE - | Operator Reliability Experiment |
| PC - | Paired Comparisons |
| PHECA - | Potential Human Error Cause Analysis |
| PRA - | Probabilistic Risk Assessment |
| PORV - | Power (or Pilot) Operated Relief Valve |
| PRZR - | PRessuriZeR |
| PSF - | Performance Shaping Factor |
| PWR - | Pressurized Water Reactor |
| RB - | Rule-Based |
| RCS - | Reactor Coolant System |
| RES - | NRC Office of Nuclear Regulatory RESearch |
| RHR - | Residual Heat Removal |
| SAINT - | Systems Analysis of Integrated Networks of Tasks |
| SBLOCA - | Small-Break LOCA |
| SCSS - | Sequence Coding and Search System |
| SHARP | Systematic Human Action Reliability Procedure |
| SG - | Steam Generator |
| SI - | Safety Injection |
| SLIM - | Success Likelihood Index Methodology |
| SRM - | Sandia Recovery Model |
| SRV - | Safety Relief Valve |
| STAHR - | Socio-Technical Approach to assessing Human Reliability |
| TALENT - | Task Analysis Linked EvaluatioN Technique |
| $T_{AVE}$ - | Temperature, RCS AVeragE |
| THERP - | Technique for Human Error Rate Prediction |
| TMI 2 - | Three Mile Island Unit 2 |
| TRC - | Time-Reliability Correlation |
| UAC - | Unsafe Action of Commission |
| UAO - | Unsafe Action of Omission |

# 1. INTRODUCTION

## 1.1 Background

Probabilistic risk assessment (PRA) has become an important tool in nuclear power plant (NPP) operations and regulation. In particular, the U.S. Nuclear Regulatory Commission (NRC) has been using PRA methods as a basis for regulatory programs and analyses for over two decades. The NRC recently published SECY-95-126 providing the final policy statement on the use of PRA in NRC regulatory activities. In a June 6, 1994 memorandum from the NRC Executive Director of Operations (Taylor 1994) to the Commissioners, at least twelve major licensing and regulatory programs were identified that are strongly influenced by PRA studies. These programs include: licensing reviews of advanced reactors, screening and analysis of operational events, inspections of facilities, analysis of generic safety issues, facility analyses, and reviews of high-level waste repositories.

Human reliability analysis (HRA) is a critical element of PRAs, being 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 important aspects of human performance, constraining the extent to which NRC can rely on the results of PRA studies.

Limitations in the analysis of human actions in PRAs have long been 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), the Lewis Commission (NUREG-0400) identified five fundamental limitations in the methods used in the evaluation of "human factors" just six months before the Three Mile Island accident (Rogovin and Frampton, 1980). These limitations were: insufficient data, methodological limitations related to the treatment of timescale limitations, omission of the possibility that operators may make an accident worse, omission of the possibility that operators may perform recovery actions, and uncertainty in the actual behavior of people during accident conditions. In 1984, NRC again reviewed the technology of PRA, in NUREG-1050, and recognized several of the above HRA deficiencies were still relevant. This review concluded that:

> "...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 NRC's final policy statement on the use of probabilistic risk assessment methods in nuclear regulatory activities (SECY-95-126), 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...," thereby identifying another criticism of both PRA and HRA.

This report introduces a new HRA method called "A Technique for Human Error Analysis (ATHEANA)." ATHEANA is a result of recent efforts in the improved HRA project sponsored by the

Office of Nuclear Regulatory Research at the NRC. ATHEANA has been developed to address deficiencies identified in current HRA approaches, by:

- addressing errors of commission and dependencies,
- representing more realistically the human-system interactions that have played important roles in accident response, as evidenced by operating experience, and
- integrating recent advances in psychology with engineering, human factors, and PRA disciplines.

Previous efforts in this project examined human performance issues specific to shutdown operation (NUREG/CR-6093) and developed a multidisciplinary HRA framework to investigate EOCs and human dependencies (NUREG/CR-6265). To support ATHEANA, a more comprehensive data analysis approach and database has been developed for the review of operating experience, the "Human-System Event Classification Scheme (HSECS) Database" (Cooper et al., 1995).

## 1.2 Human-System Interactions in Real Accidents and Near Misses

The record of significant incidents in NPP operations shows a substantially different picture of human performance than that represented by human failure events modeled in PRAs. Human failure events modeled in current PRAs typically represent failures to perform required procedure steps. In contrast, human performance problems identified in real operational events often involve operators performing actions which are not required for 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 (NUREG-1250 and 1251) and Three Mile Island 2 (TMI-2) (Kemeny, 1979; Rogovin and Frampton, 1980), frequently leave the impression that the operator actions associated with these events were illogical and incredible. Consequently, the lessons learned from such events often are perceived as being very plant-specific and/or event-specific.

As a result of the TMI-2 event, there were numerous modifications and backfits implemented by all nuclear power plants in the U.S., including symptom-based procedures, new training, and new hardware. After the considerable expense and effort to implement these modifications and backfits, the kinds of problems which occurred in this accident would be expected to be "fixed." However, there is substantial evidence that there may be a persistent and generic human performance problem which was revealed by TMI-2 (and Chernobyl) but not "fixed": errors of commission involving the intentional operator bypass of engineered safety features (ESF). In the TMI-2 event, operators inappropriately terminated high pressure injection, resulting in reactor core undercooling and eventual fuel damage. In July 1995, NRC's Office of Analysis & Evaluation of Operation Data (AEOD) published a report entitled "Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features" (AEOD/E95-01), identifying 14 events over that past 41 months in which 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." Events analyses performed in support of the Improved HRA project (e.g., NUREG/CR-6265, HSECS database [Cooper, 1995) also have identified several errors of commission resulting in the inappropriate bypass of ESF.

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 which are not addressed in current PRAs. Examples of such complicating factors in operators' response to events are: 1) multiple (especially dependent or human-caused) equipment failures and/or unavailabilities, 2) instrumentation problems, and 3) plant conditions not covered by procedures. The fact that real events involve such complicating factors frequently is interpreted only as indication of plant-specific operational problems, rather than a general cause for concern.

In fact, the results of event analyses performed for this project and of parallel analyses performed for other projects (e.g., NUREG/CR-6208) show that the complicating factors in events can lead operators to take unexpected actions. In other words, operators do behave in rational, logical ways given the context of the specific event. The important contextual factors that contribute to the occurrence of undesired operator responses include the complications of hardware and instrumentation failures, unfamiliar plant conditions and configurations, and deficiencies in performance shaping factors such as procedures and training. As will be elaborated on in this report, unfamiliar plant conditions (sometimes the result of prior human-system interactions, such as maintenance scheduling errors) often place operators in cognitively demanding situations, requiring interpretations and departures from procedural guidance for successful accident response. Complications in such situations, such as misleading or failed indications, can trigger an incorrect mental model of the plant status and behavior. As a result, such event contexts can "set up" inappropriate operator actions, often taking the form of errors of commissions which lead to worsened plant states.

All NPP incidents that have been analyzed in this project involve significant contributions from the event context. Significantly, from a risk perspective, the two major accidents involving commercial power plants, Three Mile Island 2 and Chernobyl, were strongly influenced by the event context. When the insights regarding human performance from these operational events, both serious accidents and significant incidents, are generalized, four common characteristics emerge:

1) the plant behavior is outside the expected range;
2) the plant's behavior is not understood;
3) evidence of the actual plant state and behavior is not recognized; and
4) prepared plans are not applicable or helpful.

These characteristics capture the needed consideration of context as an error-driving factor and lead HRA analysts to the consideration of human errors which were previously considered incredible (e.g., errors of commission, especially bypass of ESFs). Hence, in order to be consistent with operational experience, ATHEANA must be able to identify, model, and quantify the probabilities of errors of commission which result from these characteristics.

### 1.3 Deficiencies in Current HRA Methods

The assessment of human reliability plays an important role in PRAs. This importance is consistent with operating experience in which humans historically have played key roles. However, both HRA and PRA have been criticized for not being able to model the human-system interactions in a consistent fashion based on real operating experience and the serious accidents which have occurred.

From the discussions in the previous section, it can be seen that, for an HRA method to correctly characterize the human-system interactions under accident conditions, it should be able to:

1) identify potentially significant human failures, including errors of commission and dependent human errors; and

2) guide the search for "non-nominal" (i.e., outside the range of conditions considered and expected by typical PRA models) accident conditions that enhance the likelihood of human failures; and

3) include the influences of deficiencies in procedures, training, etc. with respect to their applicability to "non-nominal" accidents.

The second and third of these requirements represent an "error-forcing context," or the confluence of complicating plant conditions and complicating human conditions which virtually guarantee human error. In order to provide error probabilities which are consistent with operational experience, the task of HRA quantification must be based upon the likelihood of such error-forcing contexts, rather than upon a prediction of random human error in the face of nominal conditions. Quantification of human failure probabilities based upon error-forcing contexts represents a fundamental shift in the conduct of HRA.

One of the major problems in advancing the state-of-the-art in HRA has been the miscommunication between experts in the several fields that are involved in human error in nuclear power plants and as modeled in PRAs. Engineers, operations experts, systems analysts, risk analysts, psychologists, human factors engineers, and behavioral scientists have each viewed "error" from the perspective of their particular discipline. All of these fields converge on the issue of how well humans interact with each other and the machinery of power plants. Consequently, an HRA method needs to provide a common language and framework to bring the disparate knowledge of these disciplines to bear on the common problem of improving HRA in the context and support of PRA.

In summary, HRA/PRA deficiencies and weaknesses include:

- lack of acknowledgement of the multidisciplinary nature of HRA
- lack of guidance for EOCs and dependency
- lack of focus on error-forcing context
- lack of formal guidance for performing HRA tasks
- lack of emphasis of the constraints imposed by existing PRA methods
- lack of formalized requirements for the interface between HRA and PRA
- lack of formal search schemes to identify candidate human failure events to include in PRA models

As identified in Appendix A, all current HRA methods possess some of the above attributes needed for the next generation HRA method, but none satisfies all of them. A few methods provide a means for defining a search scheme for actually identifying human failure events to include in PRAs; the others only provide a means for structuring and understanding already identified errors. None of the methods focuses on errors of commission and dependency, although several can be used to model these events using judgmental evaluation of the factors affecting these issues. None is based upon a multidisciplinary view of human reliability. Most importantly, none of the quantification approaches focuses on identifying or quantifying the likelihood of error-forcing contexts.

## 1.4 Overview of Improved HRA Project

The principal goal of this Improved HRA project is to take an incremental step toward incorporating more realism into HRA and, therefore, PRA as well. Consequently, previous and current work in this project have directly addressed the requirements of a next generation HRA method described above. Previous work in the project focused on the development of a multidisciplinary framework (NUREG/CR-6093 and

6265) which describes the relationship between HRA and PRA, as well as the crucial elements which influence human performance and reliability. Reviews of operational events initially assisted in the development of this framework as a guide to investigate important HRA issues, including errors of commission and human dependencies. With this basis, ATHEANA has been developed as described in this report. This development effort required a bridge to be made between the retrospective analysis of past operating events and the prospective analysis of potential events in support of PRA. Formation of this bridge was accomplished by:

- Applying the multidisciplinary HRA framework and lessons learned from retrospective analyses to a process for structuring and setting priorities in the search for human failure events and error-forcing contexts to be quantified.

- Focusing the task of HRA quantification on the search processes for error-forcing contexts.

- Quantifying the likelihood of an error-forcing context, rather than predicting random human error in the face of nominal conditions.

This initial description of ATHEANA occurs at a crucial point in the history of HRA. As identified above, criticism of HRA and PRA has been mounting for several years. At the same time, the NRC is planning for increased use of PRA in its regulatory activities (i.e., SECY-95-126). The successful development and demonstration of this new HRA method is expected to improve the way in which HRA is performed and regarded by its analysts and reviewers, and those who use the results of the PRA to guide their work.

### 1.5 Report Outline

The purpose of this report is to introduce and describe the current development status of a new HRA method, ATHEANA, that can be used to model post-initiator, human-system interactions in PRAs and that addresses the concerns expressed above.

Section 2 discusses the principles underlying ATHEANA, particularly the multidisciplinary HRA framework. The fundamental requirement underlying the development work is that the method be consistent with what has been learned about human behavior in accident situations. While the study of actual event descriptions gives insights that may be generalized, there are too few events to provide a comprehensive basis for model development. Consequently, this project has drawn from the cognitive science literature to develop conceptual models of error causes.

Section 3 describes the ATHEANA method and its application tools. Section 4 is an example application of the concepts discussed in Sections 2 and 3, and provides a proof of concept for ATHEANA.

Current developments in continuing work are described in Sections 5 and 6. The end product of this project will be an HRA method that can provide a means for identifying and defining human failure events for inclusion in a PRA model and an approach to the estimation of their probabilities. This is to be achieved through the establishment of guidelines for implementing ATHEANA and an accompanying information or knowledge base. Section 5 summarizes current developments in the knowledge-base, including the understanding of error causes from both psychological theory and operational experience, which will be used to identify new errors of commission and their associated error-forcing contexts to be modeled in PRAs. Section 6 discusses the process for implementing ATHEANA, based on the project team's experience in the performance of PRAs and supplemented by the experience gained during the exercise described in Section 4. Included in this process are search schemes for identifying, first, the human failure events to include in the PRA model, and secondly, the associated error-forcing contexts that are necessary for the quantification approach.

Section 7 summarizes the project status with the completion of the work described in the report and the expected future products of the project. References are provided in Section 8. Appendix A presents a brief review of current HRA methods and, as summarized in Section 1.3, demonstrates the need for the development of a new HRA method. Appendix B describes the multidisciplinary HRA framework.

# 2. PRINCIPLES UNDERLYING THE ATHEANA HRA METHOD

## 2.1 Introduction

The introduction of this report identified several requirements of an improved HRA method and described the characteristics of human-system interactions that have been seen in accidents and significant incidents at nuclear power plants. The most important of the identified requirements is to more realistically model human-system interactions, by incorporating the characteristics of serious accidents into both HRA and PRA. However, as noted in the previous section and described in Appendix A, the HRA methods presently used in PRAs do not adequately model these characteristics. Therefore, in response, NRC has undertaken this program to develop a new HRA method that will improve the ability of PRAs to:

- identify and characterize important human-system interactions and their likely consequences under accident conditions;
- represent the most important severe accident sequences that could occur;
- estimate the frequencies of these sequences and the associated probabilities of human errors; and
- provide recommendations for improving human performance based upon characterizations of the causes of human errors.

In order to achieve these goals in the development of the new HRA method, ATHEANA, it was necessary to establish a new basis for HRA modeling, starting with the development of a better understanding of human performance in serious nuclear power plant accidents and their precursors (i.e., significant operational incidents). Section 2.2 summarizes recent advances, especially in the behavioral sciences, which were used to develop this understanding and identify the most important influences on human performance, including contextual factors. This understanding has been captured, represented, and blended with the knowledge pertaining to the disciplines of PRA, engineering, and human factors in the multidisciplinary HRA framework, which is presented in Section 2.3. The multidisciplinary HRA framework has been used to analyze operational events, yielding further insights regarding the causes of operator errors compared with those produced by other approaches. These successful event analyses (examples of which are given in Section 2.4) confirm that the framework and the principles underlying the ATHEANA method provide a perspective of human performance that is consistent with real operational experience. Finally, Section 2.5 summarizes the impact of the new HRA requirements on the PRA model (within the constraints imposed by PRA modeling practices).

## 2.2 Advances in Understanding Human Performance

In order to develop an HRA method that achieves the aims of this project, it is necessary to develop a way to describe how human performance has influenced safety in power plants. As described in Appendix A, existing HRA methods* have to a large extent focused on only limited perspectives on human behavior, either as a "procedure reader-switch turner" component or as a "time-limited processor of information." Other methods, e.g., the Success Likelihood Index Methodology (SLIM) (NUREG/CR-

*For example, the Technique for Human Error Rate Prediction (THERP) (Swain and Guttmann, NUREG/CR-1278), the Human Cognitive Reliability (HCR) model (Hannaman, et al., 1984).

3518, 1984), provide no perspective on human behavior at all, leaving it to the analysts to provide their own view. Neither of these perspectives provides very useful insights as to how to change the setting in which the operators work in order to change significantly the level of assessed risk. As a consequence, the first major task in the development work for this project was to assemble and review the body of knowledge about how human interactions impact safety.

### 2.2.1 Human Errors Are Driven By Context

Recent work in the behavioral sciences (including work separately performed by Reason (1990) and Hollnagel (1993)) has contributed to the understanding of the interactive nature of human errors and plant behavior that characterize the accidents that have occurred. This understanding suggests that it is essential to analyze both the human-centered factors (e.g., performance shaping factors such as human-machine interface design, procedures content and format, and training) and the conditions of the plant that gave rise to the need for actions and created the operational causes for human-system interactions (such as misleading indications, equipment unavailabilities, and other unusual configurations or operational circumstances). This is in contrast to the existing HRA methods that consider principally the human-centered causes, with only an acknowledgment of plant influences through such simplistic measures as the time available for action.

The human-centered factors and the influence of plant conditions are not independent of each other. Rather, in many major accidents particular (unusual or non-nominal) plant conditions create the need for operator actions and, under those unusual plant conditions, deficiencies in the human-centered factors lead to errors on the part of people responding to the unusual plant conditions.

Therefore, typical evaluations performed in HRA assessments of performance shaping factors (e.g., procedures, human-machine interface, training) may not identify critical problems unless the whole range of possible plant conditions under which the controls or indicators may be required is considered. Unless the analysis of performance shaping factors (PSFs) is performed recognizing that plant conditions can vary significantly within the definition of a single PRA scenario, and that some of those plant conditions can be much more demanding of operators (both in terms of the plant conditions themselves and the limitations in PSFs such as procedures and training under those conditions), the analysis may fail to identify the most likely conditions leading to operator failure.

For example, a particular layout of indicators and controls may be perfectly adequate for the conditions assumed by the PRA analyst as the representative or nominal conditions to apply to a particular PRA scenario. These conditions may represent the most likely, uncomplicated conditions that lie within the PRA scenario definition. However, it is possible that there are other conditions that could arise during the same PRA scenario that would make the layout have an influence on the occurrence of operator errors in the accident response. If, under the nominal conditions of an accident scenario, an operator is required to perform a series of actions that are located on several control boards but are well-separated in time, the layout may be adequate. However, it is possible that under some subset of plant conditions for the same scenario, the dynamics of the plant require the actions be taken almost simultaneously. In this case, the layout is inadequate and might result in failure to perform the actions in time.

Simply stated, operator failure associated with a PRA scenario is more likely to result from "unusual" plant conditions represented within the definition of that scenario than from a random human error under the nominal conditions. Analyses of power plant accidents and near misses support this perspective, indicating that the influence of non-nominal plant conditions appears to dominate over random human errors. (See, for example, those performed by Reason and Wreathall for Volume 8 of NUREG/CR-1275, Reason (1990), NUREG/CR-6093, NUREG/CR-6265, and Section 2.4, below.)

This evidence from incident analyses is consistent with experience described by training personnel who have observed that operators can be forced to fail in simulator exercises by creating appropriate combinations of plant conditions and operator mindset. Examples of difficulties in operator performance in challenging simulator training situations has been demonstrated by Roth et al. (NUREG/CR-6208).

Therefore, to provide an effective tool for measuring and controlling risk, PRA must be able to incorporate realistically those human errors that are caused by off-normal plant conditions as well as those that occur randomly during nominal accident conditions. However, for PRA to incorporate errors caused by off-normal plant conditions, it is necessary to be able to identify what are the contexts that can force human errors, to be able to estimate how likely are these conditions, and to estimate what are the likely consequences in terms of inappropriate human actions or inactions. *Error-forcing contexts*, then, must be used both in the identification of human errors to be modeled as human failure events (HFEs) in the PRA model and in the quantification of the probabilities of these HFEs.

### 2.2.2 Contexts Trigger Error Mechanisms

The identification of error-forcing contexts, as described above, must be based on an understanding of the kinds of psychological mechanisms causing human errors that can be set up by particular plant conditions that lie within the PRA definitions of accident scenarios. One theory is that human errors occur (for the most part) as a result of combinations of influences associated with the plant conditions and its human factors characteristics that trigger error mechanisms in the plant personnel. These error mechanisms are often not inherently "bad" behaviors but are mechanisms that generally allow humans to perform skilled and speedy operations. For example, people often diagnose the cause of an occurrence based on pattern matching. In nuclear power plants, if operators had to analyze every scenario in a deep analytical manner, responses would be delayed long past the onset of plant damage. It is the fact that people (with the aid of training and procedures) can take short cuts in problem analysis and solution generation that normally result in speedy and reliable actions. However, when the scenario does not exactly match the rules or when fatigue or workload predispose excessive short-cutting, for example, errors can result. In other words, many error mechanisms occur when operators apply normally useful cognitive processes that, in the particular context, are "defeated" or "fooled" by a particular combination of plant conditions and PSFs, and result in a human error.

This theory of human errors has an extended pedigree in the behavioral sciences starting with Mach, who, in 1905 stated: "Knowledge and error flow from the same mental sources, only success can tell one from the other" (Mach, 1905). More recent proponents of this position include Senders and Moray (1991), Reason (1990), and Woods et al. (1994).

Error mechanisms are not observable in themselves; only their consequences as human errors can be observed. However, without an understanding of error mechanisms, the search for error-forcing contexts would be limited to searches for repeat events that were simply duplicates of earlier incidents where people had failed.

Hudson (as reported by Reason, 1990) coined the term "tokens" to describe the particular instances of factors and conditions that occurred in a particular incident. However, the tokens in a particular incident are particular representations of general classes of factors and conditions referred to by Hudson as "types". Reason observes that the common practice of "fixing" problems following an incident is to remove the particular token causes of the event without fixing the broader classes (the types) of causes. For example, an incident occurs and a human error is attributed to a deficient procedure. A token fix is to change that procedure to remove the immediate and direct cause of the error. To fix the type would involve analyzing *why* the procedure was deficient. Was there an insufficient review? Were the conditions under which the procedure was to be used not described fully or accurately? What programmatic changes could remove not only that one token flaw but remove other similar but undiscovered flaws in that and other procedures?

The search for *why* implies a set of root causes that can be evaluated for their contribution to the deficient procedure. In the case of procedure writing, the programmatic process to ensure good procedures is reasonably well defined and root causes can be described. In order to perform analyses of human errors, there must be a set of corresponding root cause descriptions of why errors can occur. By analogy with Hudson's usage, without these descriptions of the underlying error mechanisms and an understanding of the contexts that can force them to occur, the search for these error-forcing contexts will be limited to the token level. The token level would not be adequate for the purposes of risk assessment and risk management: to identify potentially significant accident scenarios and their more likely causes, before they occur.

Based on the above discussion, what is needed for the development of an improved HRA method is a process to identify the likely opportunities for inappropriately triggered mechanisms to cause errors that can have unsafe consequences. The starting point for this search is an HRA framework that seeks to describe the interrelationships between 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 through human interactions. Also, a practical set of tools for applying an HRA method to model post-initiator operator actions must be based upon principles in addition to those given in this and the previous section, especially since error mechanisms are not observables.

### 2.2.3 Behavioral Models Connect Error Mechanisms and Post-Initiator Operator Actions

The previous two sections explained how human errors are driven by error-forcing contexts through the triggering of error mechanisms. Since, as noted above, error mechanisms are not observables, additional explanation of how humans behave is needed to provide observable and auditable factors for HRA analysts to use in the identification of human errors, and their associated error-forcing contexts, to model as post-initiator HFEs in the PRA model. Behavioral models can provide this additional explanation and connect the concepts of human error, error-forcing context, and error mechanisms with post-initiator operator actions.

Post-initiator operator response can be divided into four stages: 1) detection that a situation has arisen, 2) diagnosis of the situation, 3) deciding what actions are required, and 4) implementation of these actions. One of the well-established models developed in cognitive psychology to describe information processing and problem-solving corresponds almost directly with these four stages: the Information Processing Model (IPM). The IPM model of human performance has been used in many applications. For example, it underlies the development of the Cognitive Environment Simulation (CES) human performance modeling (Woods et al., NUREG/CR-5213), and the more recent work by Roth et al. (NUREG/CR-6208). For more general discussions and implications of the information-processing perspective of human behavior, see Newell and Simon's (1972) book, *Human Problem Solving*. For a summary of this perspective's relationship to human reliability in nuclear power plant activities, see the review by Gertman and Blackman (1994), and the discussion by Kantowitz and Fujita (1990), among others.

The four stages of information processing in the context of abnormal events in nuclear power plants can be described as:

1) Detection: The onset of realization by operators that an abnormal event is occurring.

2) Situation Assessment: The operators' construction "...of an explanation to account for observed plant behavior; a mental representation of factors known or hypothesized to be affecting plant state. This mental model generates: expectations about other plant parameters, expectations about future consequences, explanation for observations, identification of unexpected plant behavior and search for explanations, and anticipation of potential future problems." (NUREG/CR-6208)

3) Response Planning: The activities associated with deciding upon appropriate actions to terminate or mitigate development of an accident sequence, given a particular situation assessment. Often (but not always) these actions are those specified in procedures. The activities involve: "...establishing goals, identifying/generating a response plan, evaluating/monitoring effectiveness of response plan, filling in gaps in response plan, and adapting response plan." (NUREG/CR-6208)

4) Response Implementation: The activities involved with the physical carrying out of the actions identified in the response planning stage. Activities do not necessarily require active intervention by operators. Activities can include simple monitoring of automatically-actuated equipment, or more extensive actions required to recover failed equipment.

In the IPM model, human errors are the result of underlying error mechanisms that limit the operators' abilities in detection, situation assessment, response planning, and/or response implementation. Many human errors can result from error mechanisms associated with each information processing stage. For example, operators may fail to open a valve in a task for several reasons. First, they may inadvertently skip a step in a procedure requiring the valve to be opened (a response implementation failure); second, they may misread the valve number in the procedure or on the valve identification label (for example, reversing two digits) and open the wrong one (an attention-related, response implementation failure); third, the operators' mental model of the plant's condition may lead them to select the wrong procedure (a situation assessment failure); fourth, they may perform the steps of the procedure out of the written sequence because they perceive that it is better to perform the task that way, and consequently fail to open the valve at the necessary time (a response planning failure). From the safety perspective and that of PRA modeling, the human failure event corresponding with all of these cognitive failures is defined as "Operator fails to open valve."

Different information processing stages are primarily associated with different kinds of human errors. For example, failures in situation assessment and response planning are typically associated with mistakes, whereas failures in detection and response implementation are typically associated with slips and lapses.

Consequently, the risk impact of the information processing stages is potentially different according to the risk impacts of the different types of human errors they induce.

It is recognized that the above descriptions and discussion are simplistic. Substantial research results are associated with individual aspects of each information processing stage; however, for the purposes of this program the descriptions given above provide a sufficient explanation of the issues that are important to the development of ATHEANA. Readers wanting to delve deeper into these areas are referred to Roth, et al.(NUREG/CR-6208), Wickens and Flach (1988), and Card, Moran, & Newell (1986).

It is also recognized that the information processing model is just one of many behavioral models which can provide useful insights regarding human errors and associated error-forcing contexts and error mechanisms. However, this project has initially focused on the IPM model because it provides useful insights regarding post-initiator human errors, especially mistakes that occur during situation assessment and response planning activities, which have been shown to be important in the analyses of simulator exercises performed by Roth et al.(NUREG/CR-6208) as well as various analyses of operational experience (e.g., NUREG/CR-6265).

## 2.3 Marriage of Behavioral Science with PRA, Engineering, and Human Factors: The Multidisciplinary HRA Framework

As reported in NUREG/CR-6265, a multidisciplinary HRA framework has been developed in order to guide the development of ATHEANA. This section provides a brief overview of the framework, emphasizing those aspects particularly relevant to the development of ATHEANA. Appendix B provides a more detailed description of the framework. 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 (e.g., NUREG/CR-6265, the HSECS report [Cooper et al., 1995], and Sections 2.4 and 5).

### 2.3.1 Concepts Underlying the Framework

The concepts described in Section 2.2 comprise the underlying basis of the framework; that human errors occur (for the most part) as a result of combinations of plant conditions and associated PSFs which trigger error mechanisms in plant personnel. In addition, the framework provides a means for applying the knowledge and understanding from the disciplines relevant to risk-significant human performance in nuclear power plant accidents: plant operations and engineering, PRA, human factors, and behavioral science. Existing HRA methods have addressed some but not all of these disciplines. In addition, the HRA framework developed for ATHEANA establishes relationships between these disciplines and new terminology to bridge the gap between them. In existing HRA methods, each discipline was considered mostly in isolation of the others, limiting the human performance insights that could be derived.

### 2.3.2 Framework Description

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

- error-forcing context
- performance shaping factors
- plant conditions
- human error
- error mechanisms
- unsafe actions
- human failure events
- PRA model
- scenario definitions

These elements are the minimum necessary set to describe the causes and contributions of human errors in, for example, major NPP events. The framework picture given in Figure 2.1 illustrates the interrelationships between framework elements.

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

### 2.3.3 Definition of Framework Elements

Brief definitions of framework elements are given below. More comprehensive discussion of the framework elements is given in Appendix B.

#### 2.3.3.1 Error Forcing Context

An *error-forcing context* (EFC) represents the combined effect of performance shaping factors (PSFs) and plant conditions that create a situation in which human error is likely. Analyses of NPP operating events reveal that the error-forcing context typically represents an unanalyzed plant condition that is beyond normal operator training and/or procedures. 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 a failure to recognize that evidence, resulting in subsequent mistakes (i.e., errors of commission), and ultimately, an accident with catastrophic consequences.

*Performance shaping factors* (PSFs) represent the human-centered influences on human performance. To date, the PSFs primarily used in this project are those identified in the Human Performance Investigation Process (HPIP) (NUREG/CR-5455):

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

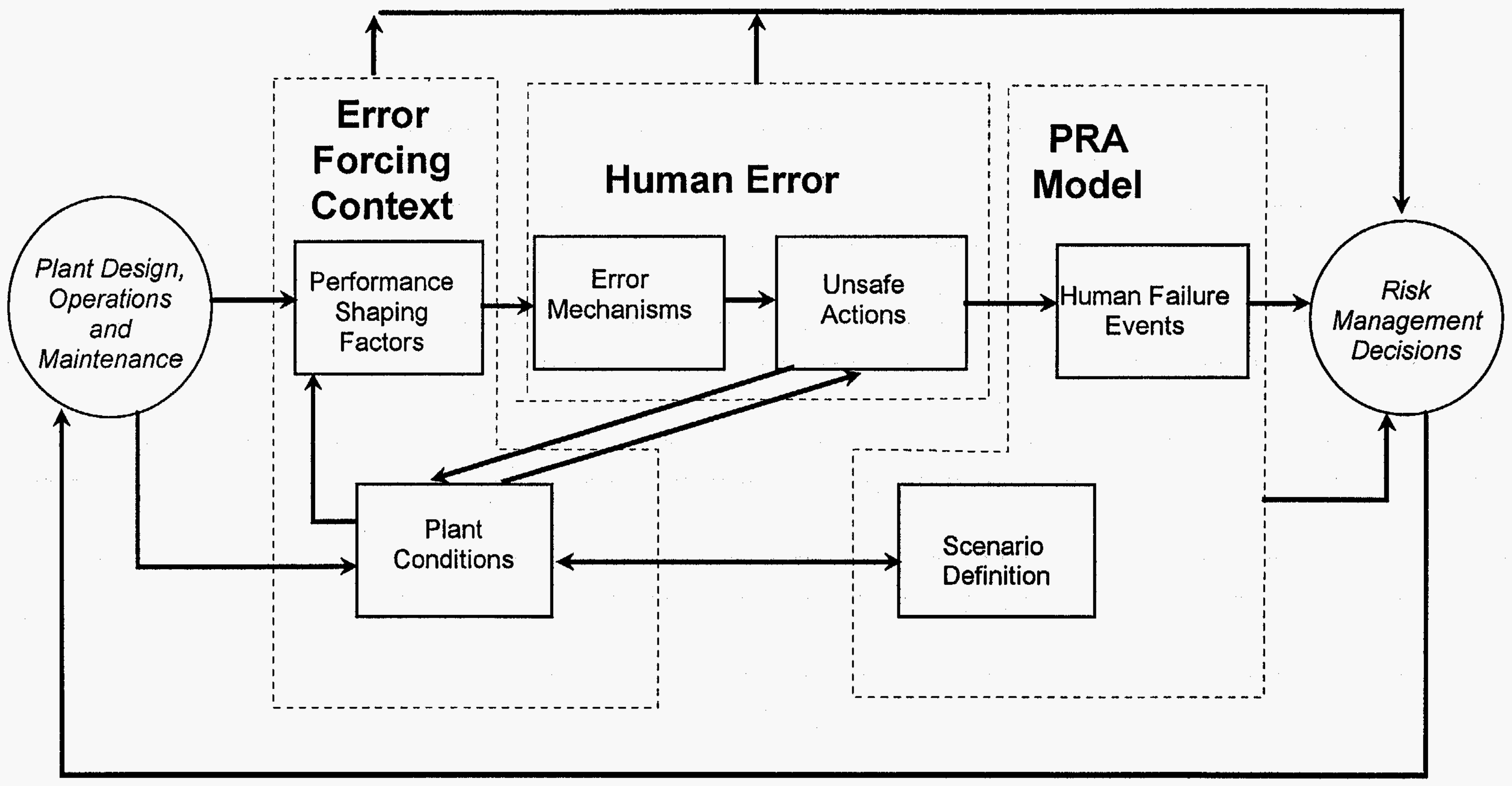

Figure 2.1 Multidisciplinary HRA framework

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) which influences, for example, a failure in situation assessment or response planning.

*Plant conditions* include plant configuration; system, component, instrumentation & control availability and reliability; process parameters (e.g., core reactivity, power level, and reactor coolant system temperature, pressure, inventory); and other factors (e.g., non-nominal and/or dynamic conditions) which result in unusual plant configurations and behavior. Some examples of non-nominal plant conditions include:

- A 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.

#### 2.3.3.2 Human Error

*Human error* can be characterized as a divergence between an action actually performed and the action that should have been performed, which has an effect (i.e., 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 same words refer to the underlying causes of the error. For the purpose of developing ATHEANA and to more fully integrate HRA with the requirements of 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 unsafe action.

*Error mechanisms* (see Section 2.2.2) are psychological mechanisms causing human errors that can be triggered by particular plant conditions and PSFs that lie within the PRA definitions of accident scenarios. These error mechanisms are often 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 that can have unsafe consequences. Different error mechanisms are influenced by different combinations of PSFs and plant conditions.

*Unsafe actions* are those actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition. The term "unsafe action" does not imply that the human was the root cause of the problem. Consequently, this distinction avoids any inference of blame and accommodates the assessment, based on 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 commit an error in the every-day sense of the term; they were doing what was the "correct" thing as it seemed to them at the time.

While not all unsafe actions identified in the analysis of operational events correspond to human failure events as defined in PRAs, in some cases, there is a direct correspondence. For example, operators terminating operation of needed engineered safety features would be an unsafe action, and should be incorporated as a human failure event in PRAs. More commonly though, unsafe actions represent a finer level of detail than most human failure events defined in PRAs.

Unsafe actions can be classified according to the simple taxonomy of unsafe action types developed by Reason (1990). These unsafe action types are slips and lapses, mistakes, and circumventions. Each type is distinct in its potential impact on safety and its causal factors.

#### 2.3.3.3 PRA Model

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

*Human failure events* (HFEs) are modeled in the PRA to represent the failure of a function, system, or component as a result of unsafe human actions which places the plant in a worse condition. A human failure event reflects the PRA systems analysis perspective, and in this context, can be classified as either an error of commission (EOC) or an error of omission (EOO). An error of omission typically represents the failure of an operator to initiate a required safety function. An error of commission represents either the inappropriate termination of a necessary safety function or an initiation of an inappropriate system. Examples of human failure events 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. As discussed later in Section 2.5.2, the HFE is defined so that it includes the failure to recognize and recover from an error before reversible plant damage occurs.

Human failure events may be associated with an event tree sequence, or with specific minimal cut sets generated by the solution of a PRA model, depending on what the HFE is supposed to represent. 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, therefore, is very much an iterative process.

PRA *scenario definitions* provide the minimum descriptions of plant state required to develop the PRA model and define appropriate human failure events. Examples of scenario definition elements include:

- initiating event (e.g., transients, small-break loss-of-coolant accident, loss of offsite power, etc.)
- 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
- systemic level
- component level

## 2.4 Confirmation of Principles from Analyses of Operational Experience

Analyses of accidents and serious incidents performed in this project have precipitated the identification, development, and ultimate confirmation of the principles underlying ATHEANA. In addition, as discussed in Section 2.4.2, independent analyses performed from other projects have confirmed and reinforced these principles. Since the basis of ATHEANA is fundamentally different from previous HRA methods, such confirmation also will be necessary to help future users of ATHEANA make the transition from focusing upon random human errors under nominal conditions to errors which result from error-forcing contexts comprised of non-nominal conditions and associated PSFs.

### 2.4.1 Confirmation from Analyses Using the Framework

Many events, including some non-nuclear power plant events, have been reviewed during the development of ATHEANA. These analyses have been performed using the multidisciplinary HRA framework as a guide to the important factors influencing human performance. In some cases, the events have been analyzed in detail, using event reports, and have been recorded in the HSECS database (Cooper et al., 1995). In other cases, relevant information has been extracted and used to support the development work.

Reviews of four events are used to illustrate the insights which have been gleaned from event analyses. All four events involve important post-initiator human errors, which are the focus on ATHEANA.* The four illustrative events are:

1) TMI-2: On March 28, 1979, a loss of feedwater transient (due to personnel errors outside the control room) and reactor trip occurred. Emergency feedwater (EFW) pumps started automatically but misaligned valves prevented flow to the steam generators. A maintenance tag obscured operators' view of indication showing that these valves were closed. A relief valve opened automatically, in response to increasing pressure and temperature, and stuck open. However, control room indication showed that the relief valve was closed. Operators failed to recognize that the relief valve is 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 3½ hours because of concerns of flooding the core and "solid" reactor coolant system conditions, resulting in significant core undercooling. Serious core damage resulted from open relief valve and reduced coolant flow. The event was terminated after a change of shift which diagnosed the open relief valve.

* Important human actions during the pre-accident and initiator phases of these events also occurred but are not addressed explicitly here.

2) Crystal River 3: 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, control room indication showed that the spray valve was closed. Operators failed to recognize that the spray valve was open. RCS pressure continued to decrease, resulting in a reactor trip. After reactor trip, RCS pressure continued to decrease, reaching setpoints for arming the engineered safety features (ESF) system. In violation of procedures guidance, operators bypassed ESF for 6 minutes, in anticipation of terminating the transient. Control room supervisors directed operators to take ESF out of bypass and the high pressure injection system automatically started. RCS pressure was controlled with high pressure injection. The pressure transient was terminated after the pressurizer spray line isolation valve was closed, on the suggestion from a supervisor that it might be helpful.

3) Salem 1: On April 7, 1994, a loss of circulating water and condenser vacuum transient and eventual reactor trip occurred due to a severe grass intrusion at the circulating water intake structure. A partial (i.e., only train A), erroneous safety injection (SI) signal was generated due to pre-existing hardware problems after reactor trip, requiring operators to manually position many valves that normally actuated automatically. Operators failed to control 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. Operators then terminated HPI. Due to operator inattention and pre-existing hardware failures, steam generator pressure increased concurrently with pressurizer level, causing the steam generator safety relief valves to open. Following the safety valves opening, a rapid depressurization occurred, followed by a second SI actuation and more pressurizer relief valve openings.

4) Oconee 3: On March 8, 1991, decay heat removal was lost for about 18 minutes during shutdown due to a loss of RCS inventory. The RCS inventory was diverted to the emergency sump via a drainpath created by the combination of a blind flange installed on the wrong sump isolation line and sump isolation valve stroke testing. Operators aligned residual heat removal pumps to the refueling water storage tank (RWST) in an attempt to restore reactor vessel level. When vessel level did not rise, operators isolated the RWST and sent an auxiliary operator to close the sump isolation valve. A total of about 14,000 gallons of coolant were drained to the sump and spilled onto the containment floor; 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 post-initiator errors of commission (EOCs). In TMI-2, the throttling of high pressure injection was an EOC which resulted in serious core damage. In Crystal River 3, the bypass of ESF was an EOC, preventing automatic injection of coolant into the reactor core. However, this operator action was recovered without core damage occurring. In Oconee 3, the alignment to the RWST, before isolating the drainpath to the sump, resulted in additional coolant being lost. Consequently, this action was an EOC which also was recovered before the event was terminated. In addition, three of these events (Crystal River 3, Salem 1, Oconee 3) involved EOCs which either occurred just prior to reactor trip or caused reactor trip.

Context played an important role in all of these events. In TMI-2, plant conditions which contributed to the event included the pre-existing misalignment of EFW valves and the stuck open relief valve. These conditions combined with negative performance shaping factors, including the maintenance tag obstructing position indication for the EFW valve, misleading relief valve position indication, 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 involved similar factors, especially the open spray valve and the associated misleading position indication. 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 position indication because the isolation valve (which ultimately created the drainpath) was racked out to perform stroke testing. Also, the erroneously-installed blind flange was a temporary obstruction which remained undiscovered despite several independent checks. Various instrumentation (e.g., reactor vessel level indication and alarms) indicated lowering reactor vessel level in the Oconee 3 event which operators discounted until field reports from technicians in containment confirmed that level was lowering 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 pre-existing hardware problems and which required operators to manually align several valves. Also, there was no procedural guidance regarding appropriate actions in response to SI train logic disagreement.

Application of the information processing model concepts to these events reveals that situation assessment was critical in all of these events. 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 rapid depressurization following steam generator safety valve openings. Finally, in Oconee 3, operators did not recognize that a drainpath to the sump existed until eyewitness reports were provided. These situation assessment problems involved either the sources of information (i.e., instrumentation) or their interpretation. In TMI-2, operators misread relief valve drain pipe temperature indication twice and attributed high in-core and RCS loop temperatures to faulty instrumentation, as well as being mislead by the control room position for the relief valve. Also, some key indications 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 indications, as well as the misleading spray valve position indication and (unsuccessful) cycling of the spray valve control, were taken as support of this hypothesis. In Oconee 3, operators suspected that decreasing reactor vessel level indication was due to 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.

### 2.4.2 Confirmation from Other Analyses

Several independent studies of accidents support the principles underlying ATHEANA, several of which have already been cited above. Recent discussions with those who have analyzed transportation and aviation accidents (e.g., NTSB/SS-94/01, 1994) and review of accidents at chemical plants (e.g., Kletz, 1984) indicate that an error-forcing context is most often present in serious accidents involving human operational control in these industries. Reason (1990) identified important contextual factors in several major accidents, including the accident at TMI-2 and the Challenger shuttle explosion in January 1986. Analyses of nuclear power plant incidents in Volume 8 of NUREG-1275 identified non-nominal plant conditions, and associated procedural deficiencies for these conditions, as strongly influencing 8 of 11 events which were significantly impacted by human actions. Of the 11 events, 6 involved errors of commission. The NRC AEOD report (AEOD/E95-01) "Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features" (1995) identified 14 events over the past 41 months in which ESF was inappropriately bypassed, all of which are errors of commission. NUREG/CR-6208 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 due to the plant conditions for the specific, simulated event being different from nominal). Also, in the 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 decisionmaking" errors (Beare et al., 1991).

## 2.5 The HRA/PRA Interface

ATHEANA has been developed with the expectation that it will be used in traditional PRA models. In other words, application of ATHEANA will not require major changes to the mechanics of how PRA models are constructed. However, in order to achieve the needed improvements in HRA and PRA discussed in Sections 1 and 2.1, there must be some impact on how HRA and PRA are performed. Also, the traditional PRA style poses several limitations and constraints. Some expected impacts and limitations are identified in the discussions below of the PRA structure, the definition of human failure events, and general specifications for performing HRA/PRA.

### 2.5.1 PRA Structure

There is a considerable variety in the way PRA analysts construct their plant logic models, although all have the common feature that inductive logic models called event trees are used to define the accident scenarios of interest. An event tree is a pictorial representation of the accident scenarios that can result from an initiating event. The scenarios are differentiated by the successes and failures of the events represented by the branch points in the event tree. These branches relate to the functions required to respond to the initiating event. The major discriminant between different approaches is in the detail which goes into the development of the event tree scenarios. Some analysts prefer to keep event trees fairly simple, with the branches of the trees representing successes and failures of critical safety functions; others prefer the branches to represent the successes and failures of the individual systems that can provide those functions; still others prefer that the branches represent successes and failures of trains of systems.

Other logic models, primarily fault trees, are used to model which combinations of component failures or unavailabilities lead to the functions, systems, or trains failing to perform their mission as specified in the success criteria associated with the event tree branches. The logic model events which represent the unavailability or failure states of the basic components are the basic events of the model. The basic events are the lowest level of decomposition in the model and therefore define the level of detail the model is capable of supporting.

Failures in human-system interactions are included in this set of basic events as events that represent specific failure modes of components, or of functions, that are a result of failures on the part of the plant personnel in their interactions with the plant. These HFEs may appear explicitly as event tree headings or they may appear in fault trees, depending on the impact of the failures, and the preference of the PRA analysts. The human-system interactions of interest may occur in the post-initiator, initiating event, or post-accident phases. It is the pre-initiating event failures that have been the focus of this project to date

In a PRA, a detailed scenario description, obtained by combining the event tree and fault tree decompositions, is given as a product of an initiating event and a set of basic events, and each set forms an accident scenario cut set. The set, or a subset, of the basic events that appear in the same scenario cut set as a human failure event define, to the extent they can, the boundary conditions under which the human-system interaction should be evaluated. However, event tree models are constructed in such a way that several cut sets may be associated with one accident sequence. A particular human failure event may appear in many of these cut sets and is therefore associated with several different sets of basic events. Thus, for a single HFE, there may be several different conditioning scenarios. For example, one cut set associated with an HFE may contain among others, the event, "pump A fails to start", whereas another cut set may contain the same events except that the "fails to start" failure mode is replaced by "pump A fails to run". This cut set may therefore represent a different plant condition, because, for example, the decay heat level is different. In fact the latter cut set is itself representative of a population of plant conditions, since a failure to run could occur at any time during the mission defined for the function for which the basic event is a contributing failure.

As another example, each initiator type addressed by event trees actually represents a variety of possible initiating events. In fact, one task of the PRA analyst is to appropriately group initiators to control the event trees to a manageable number. For example, typically, a PRA includes one generic event tree for transient events which represents many different actual initiating events, such as loss or reactor coolant flow, loss of feedwater, loss of condensate pumps, loss component cooling water, and steam line breaks. (See EPRI NP-2330 and NUREG/CR-3862 for additional examples.) Even these initiator categories are simply representative of a variety of possible plant conditions that could to reactor trip. Definitions of small, medium, and large loss-of-coolant accidents (LOCA) explicitly identify the range of break sizes relevant to each definition.

Event trees can be, and are, used to capture some of the temporal and causal relationships between failures, but solutions to accident sequences are still generally not defined precisely in this respect. Usually, when it is necessary to fix some variable, for example, the time to onset of core damage, a particular realization is chosen as a representative of the population of possibilities. In the first of the above examples, the time to onset of core damage would typically be based on the assumption that all cut sets lead to failure of the function at the time of the initiating event. In the example of the LOCAs, a representative size of LOCA would be used to evaluate the timing associated with the need to establish recirculation flow, for instance.

Some plant conditions may not be addressed. For example, instrumentation failures which can adversely impact operator response may not be explicitly modeled. In addition, it is also important to recognize that PRAs do not try to capture individual differences between, for example, nominally identical components, or between operating crews, but represent time averaged and population averaged reliability characteristics. These examples illustrate the ways in which the typical PRA scenario definitions do not explicitly address issues that might have an influence on identifying the error forcing conditions that might lead to errors of commission. Thus, an HFE, as it appears in a typical PRA, does not have clearly defined boundary conditions in terms of all the possible influences on operator behavior.

If the style of PRA models is not to be radically altered, the features of the traditional PRA modeling approach described above clearly place some constraints on the interface between the HRA method and

PRA model. As will be described in Section 3, the principal difference between ATHEANA and existing methods is the focus upon the identification and prioritization of the error-forcing contexts (EFCs). Some of these EFCs may consist of more finely defined initiating events, accident scenarios, and scenario timings, as well as complicating plant conditions. Since developing event tree or system fault tree models down to the level described by EFCs is likely to make PRA models intractable and very difficult to interpret, ATHEANA will still model human-system interactions at a functional level, with HFEs representing failure modes of components or plant functions. However, the quantification approach for ATHEANA will have to recognize the variability inherent in the definitions of the scenarios associated with the HFEs. The inclusion of previously unmodeled errors of commission identified through application of ATHEANA will require modifications to event trees and/or fault trees. If the plant functions impacted by these EOCs are already included in the PRA model, then these EOCs can be incorporated simply as additional failure modes of these functions. Also, in some cases, as is the practice now, event tree and fault tree structures will have to be altered to accommodate a human performance concern identified by application of ATHEANA.

### 2.5.2 Definition of Post-Initiator Human Failure Events

As stated above, HRA tasks performed using ATHEANA will define HFEs at a functional level, as is done using existing HRA methods. Also, application of ATHEANA will result in the identifications of previously unmodeled HFEs, especially EOCs, which will require definition. These requirements of ATHEANA are straightforward and easily addressed in user guidance. Three additional issues regarding HFE definition using ATHEANA are discussed below. Such issues will continue to be identified and addressed during the development of ATHEANA user tools described in future project reports.

As described earlier, an HFE may result from the occurrence of one of many unsafe acts, and each unsafe act may result from one of several error mechanisms and error-forcing contexts. Different error mechanisms may be associated with different phases of the response, due to different stages of information processing, such as the recognition of a need to respond (detection), situation assessment, response planning, and response implementation. The error mechanisms associated with these different phases may be influenced by different sets of PSFs and plant conditions (i.e., error-forcing contexts). This implies that HFEs defined by ATHEANA represents all associated unsafe actions, error mechanisms, and error-forcing contexts. However, ATHEANA will provide guidance on how to identify which error mechanisms and unsafe acts are the most significant for a given PRA scenario, based, for instance, on the occurrence frequency of the plant conditions and the relative strengths of the PSFs that might apply to that scenario.

An important feature of human-related failures that will be addressed by ATHEANA is the iterative, and therefore dynamic, nature of the human-system interactions. For example, Swain and Guttmann (NUREG/CR-1278), among others, describe accident response as involving a plan-execute-verify iteration or, as described in Section 2.2.3, an iteration in detection, situation assessment, response planning, and response implementation. For example, a post-initiator error may occur because of a slip on the part of a crew member, but it does not become a failure, as defined by PRA, unless it is allowed to remain uncorrected for long enough to cause an irreversible change in the plant status. Thus, an error is a failure of a process, not a point occurrence in time; ATHEANA will incorporate the possibility to recover from an error based on the feedback from the plant.

### 2.5.3 Specifications for HRA/PRA

Application of ATHEANA will require changes to the HRA/PRA process beyond PRA model structure changes and will require additional HRA tasks for identifying unsafe actions and error-forcing contexts. A few of these expected changes are discussed below. Further guidance will be provided in future project reports.

The most important objective of ATHEANA is to more realistically model human-system interactions. In particular, it is important that ATHEANA identify and model errors of commission (EOCs). Errors of commission represent the impact of incorrect operator responses and should not be modeled as non-responses which has been past practice. Since there is essentially an infinite number of incorrect responses, the method will provide the analyst with the means to identify, for a given scenario, which are the most likely and most consequential. Event tree analysts and system modelers, as well as knowledgeable plant personnel, will assist the HRA analyst in identifying potential EOCs and their error-forcing contexts (EFCs). The event tree analyst will also be involved in this identification task because PRA model structure changes may be required, as described in Section 2.5.1. As a consequence, the HRA analyst will be required to interact with other PRA analysts earlier in the performance of PRA tasks then previously required.

In addition to improving the modeling of human-system interactions in the areas addressed earlier (EOCs and dependencies, for example), ATHEANA will be a predictive model, not in the sense of predicting when an error might occur, but in the sense of being able to recognize the features of a particular scenario that has the potential for creating the context in which an error is likely to occur. The specific definition of such error-forcing contexts also will allow the HRA analyst to suggest "fixes" to potential human performance problems identified through the post-initiator HFEs which appear in dominant cut sets.

Finally, if ATHEANA is to gain wide acceptance within the PRA community, the following additional specification is suggested. ATHEANA will be usable by a PRA analyst, using input from experts such as those knowledgeable of plant design and operations. The analyst will not have to rely on having experience in human factors or psychology. Much of the relevant psychological input will be embedded in the structure of ATHEANA and in the procedures for its application. However, the analyst must understand the underlying psychological concepts sufficiently in order to apply ATHEANA.

# 3. GENERAL DESCRIPTION OF THE ATHEANA HRA METHOD

## 3.1 Introduction

Previous sections in this report identified important human performance issues which must be addressed in the ATHEANA HRA method if needed improvements in HRA/PRA are to be made. The issues which represent the largest departures from that 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, as illustrated by past operational events. As discussed previously, real operational events frequently include post-initiator errors of commission, which are minimally addressed in current HRA/PRAs and which are strongly influenced by the specific context of the event (i.e., plant conditions and performance shaping factors). In turn, the specific context of an event frequently departs from the nominal plant conditions assumed in PRAs to prevail during at-power operations at nuclear power plants.

Consequently, the HRA modeling approach adopted for ATHEANA must be a significant shift from current modeling approaches. In particular, to be consistent with operational experience, the fundamental premise of ATHEANA is that significant post-initiator human failure events, especially errors of commission, result from situations in which the context of an event (e.g., plant conditions, PSFs) virtually forces operators to fail. As a result, in ATHEANA, the definition of human failure events and their quantification are based upon the error-forcing context of the event. This premise is a significant departure from that of traditional HRA methods in which human failure events are defined and quantified as being the result of randomly occurring operator failures which take place under nominal operating conditions.

## 3.2 Characteristics of the ATHEANA Method

The ATHEANA modeling approach must involve more than simply a new quantification model. In particular, ATHEANA must provide better, more comprehensive approaches to the identification and definition of appropriate human failure events (HFEs), and the placement of these human failure events in the PRA model. As a result, new HRA activities will be required in the application of ATHEANA. These new activities will focus upon the identification of human failure events, unsafe actions, and their associated error-forcing contexts. In particular, HRA analysts will identify combinations of off-normal conditions and performance shaping factors, rather than nominal conditions, which strongly enhance the likelihood of unsafe actions. Analysts performing these identifications will be assisted by the understanding of the causes of human failures extracted from psychological literature and analyses of operational experience. In addition, it is expected these identification activities will require more interactions between HRA analysts and other PRA analysts and plant experts. Finally, quantification of the probabilities of corresponding HFEs will be based upon estimates of how likely or frequently the plant conditions and PSFs which comprise the error-forcing contexts occur, rather than upon assumptions of randomly occurring human failures.

Section 3.4 describes the resources needed to apply ATHEANA. Two of these resources are products which are currently under development. The first product will be a knowledge-base which summarizes the behavioral science perspective of human failure and the perspective gained from the analysis of operational experience. This knowledge-base will provide the basis and justification for ATHEANA and provide information to assist in identification activities. The second product will be a set of implementation guidelines to assist the user in applying ATHEANA.

In general, ATHEANA involves the same fundamental tasks which typically define a human reliability analysis. In terms of the functional elements of the PRA/HRA process, these tasks, shown generally in the sequence in which they are performed (although with the understanding that the definition of the HFEs is generally an iterative process), are:

1) plant familiarization and information collection,
2) identification and definition of HFEs,
3) incorporation of HFEs in the logic model,
4) screening analysis,
5) detailed HRA quantification, including uncertainty analysis, and
6) documentation of the process and its results.

In applying ATHEANA, the identification and definition of post-initiator HFEs which are errors of commission will be performed similarly to those identifications of errors of omission already addressed by existing HRA methods. Errors of commission will be identified and defined in terms of failed plant, system, or component functions. However, definitions of errors of omission (EOOs) are based upon failures of manual operator actions to initiate or change the state of plant equipment. Therefore, EOO definitions typically are phrased as "Operator fails to start pumps", for example. Errors of commission must be defined differently since, generally, post-initiator errors of commission result from one of the following ways by which operators fail plant, system, or component functions:

- by turning off running equipment
- by bypassing signals for automatically starting equipment
- by changing the plant configuration such that interlocks that are designed to prevent equipment damage are defeated
- by excessive depletion or diversion of plant resources (e.g., water sources)

As described above, application of ATHEANA also involves the identification and definition of unsafe actions and associated error-forcing contexts for each HFE. The identified error-forcing contexts (i.e., plant conditions and associated PSFs), and their underlying error mechanisms, are the means of characterizing the causes of human failures. Different causes will result in different unsafe actions. The general principles underlying ATHEANA described in Section 2, including the understanding derived from behavioral science and operational experience, must be applied in the searches for unsafe actions and error-forcing contexts. Sections 3.4 and 3.5 describe resources and future ATHEANA products which will assist analysts in using this understanding in identifying and defining unsafe actions and error-forcing contexts.

## 3.3 The ATHEANA Quantification Model

Quantification of an HFE using ATHEANA is based upon an understanding of the following:

- what unsafe action(s) can result in the HFE whose probability is being quantified?
- what error-forcing context(s) can result in the unsafe action(s) comprising the HFE

Each HFE can result from several different unsafe acts. In turn, each unsafe act can result from several different causes, observable only through an error-forcing context but also representing an error mechanism.

The above discussion leads to the following equation to be used in estimating an HFE probability:

$$P(E|S) = \sum_{\substack{\text{unsafe} \\ \text{act } i}} \sum_{\substack{\text{error-} \\ \text{forcing} \\ \text{context } j}} P_{ij}(S)$$

where, $P(E|S)$ is the probability of the HFE in scenario S, $P_{ij}(S)$ is the probability of unsafe action i resulting from EFC j in scenario S. The EFCs of relevance will be chosen such that they both lead to the initial error and the failure of recovery from that error, to be consistent with traditional PRA conventions for HFE definition. The $P_{ij}(S)$ can be decomposed into two contributions. The first contribution would be the probability of the plant conditions and PSFs associated with the EFC and second would be the probability of error given the EFC.

## 3.4 The Tools for Applying ATHEANA

In order to perform HRA quantification with the above equation, the HRA analyst needs guidance regarding:

1) what activities are required to make necessary definitions and identifications of HFEs, unsafe actions, and error-forcing contexts,
2) what knowledge is needed to make necessary definitions and identifications, and
3) what information is needed to make estimates of frequencies and likelihoods of error-forcing contexts.

These three needs correspond to descriptions of the ATHEANA application process, ATHEANA knowledge-base regarding causes of unsafe actions, and quantification data which can be used in applying ATHEANA. This section briefly describes each of these analyst aids.

### 3.4.1 The Application Process

The application process for ATHEANA is shown in Figure 3.1. As this figure shows, there are two main stages in the application of ATHEANA: 1) an identification and definition stage and 2) a quantification stage. The figure also shows that application of ATHEANA, particularly in the search for the error-forcing context and in quantification, will rely heavily on information sources. Information sources include information obtained through a detailed structured discussion with experts with knowledge of the plant design and operation, the expertise from the behavioral science and cognitive psychology disciplines, and the insights from past operational experience. This information will already be embedded in the ATHEANA knowledge-base which is discussed in Section 3.4.2. The process steps are summarized below.

Using ATHEANA, the HRA and event tree analysts will, as they have always done, first identify the plant functions required for response to each initiating event. The review of plant functions should include both those explicitly included in event trees and those implied in the accident progression (e.g., passive functions). In addition, certain automatic plant functions (e.g., automatic actuation of systems) are not always explicitly indicated in event trees. The HRA analyst, in conjunction with the event tree analyst and using the expertise of the plant experts, will then identify the specific failure modes of plant

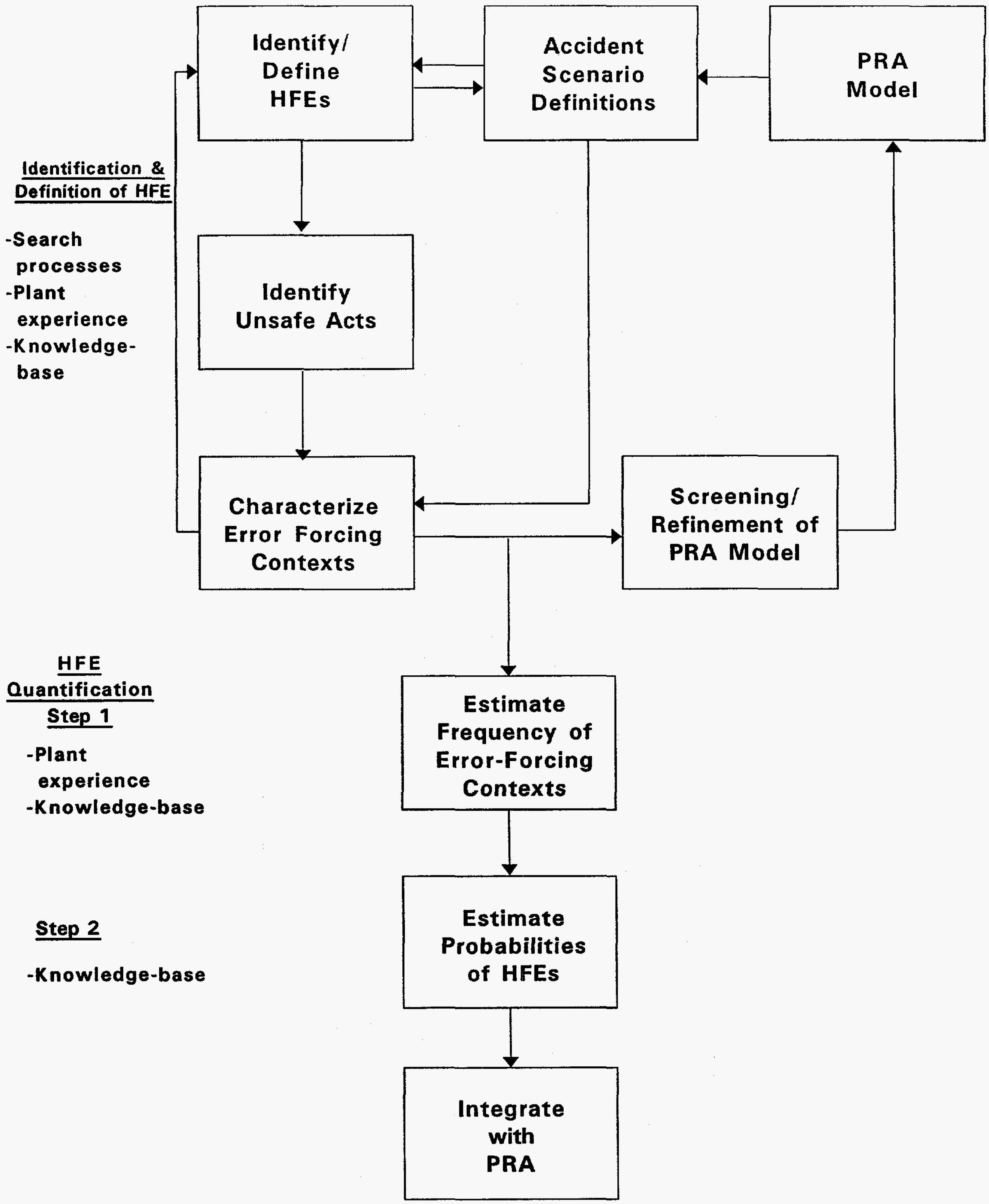
Identify/ Define HFEs
Accident Scenario Definitions
PRA Model
Identification & Definition of HFE
-Search processes
-Plant experience
-Knowledge-base
Identify Unsafe Acts
Characterize Error Forcing Contexts
Screening/ Refinement of PRA Model
HFE Quantification Step 1
-Plant experience
-Knowledge-base
Estimate Frequency of Error-Forcing Contexts
Step 2
-Knowledge-base
Estimate Probabilities of HFEs
Integrate with PRA

**Figure 3.1 ATHEANA application process flow diagram**

equipment which could result in the functional failures found in the first step. To address errors of commission in particular, it is critical that the HRA analyst become familiar with all of the plant functions and all opportunities for operators to interact with those functions, as well as the chronological sequencing of the functions that must be successful to respond to each initiator. This information will be used by the HRA analyst to identify opportunities for operators to fail these functions. The result of this first search will be a set of HFEs and associated PRA scenarios. The PRA model may require modification by including, for example, additional event tree branches or separate event trees in order to accommodate such HFEs. Also, HFEs may represent functional failures which require explicit representation not ordinarily considered in traditional event trees.

The HFEs identified above for inclusion in the PRA may result from one or more unsafe actions. In turn, plant-specific error-forcing contexts will be identified for each unsafe action. Identifications of unsafe actions and associated error-forcing contexts will be made using a search scheme coupled with a catalog of error causes included in the ATHEANA knowledge-base. Due to the consideration of different plant conditions and different PSFs associated with and encompassed by the definition of a particular scenario, the HFEs and their associated PRA scenarios may need to be redefined to reflect greater detail. For example, it may be important to model more than one HFE to represent the same human-caused hardware failure to represent differences in context which can be differentiated by a more detailed PRA scenario description. Even in current PRAs, such practices are not uncommon, reflecting, for example, different sequence and event timings.

The second stage is that associated with the estimation of the probabilities of the HFEs. This will be achieved in two steps. The first step is the estimation of the relative frequency of specific error-forcing contexts. In general, the frequency of a particular EFC is estimated by the combined relative frequency of the characteristic plant conditions (e.g., failed instrumentation) and associated PSFs. While the estimation of actual EFC frequencies clearly has to be determined on a case by case basis, the overall process for the estimation will be generic and will be described in guidance to the ATHEANA user. The second step is the estimation of the probability of a human error given a specific error-forcing context. User guidance will be provided for this estimation as well.

The application process is currently in the early stages of development. However, if the approach is to be efficient, it is clear that it will be necessary to define the process in such a way that HFEs can be screened and prioritized. Such screening or prioritization is likely to be based upon the EFCs associated with each HFE. Thus, the search for HFEs and EFCs will be somewhat iterative.

### 3.4.2 The Knowledge-Base

As described above, the ATHEANA knowledge-base consists of the understanding derived from the behavioral sciences and from past operational experience. The knowledge-base must accomplish three goals:

1) provide ATHEANA users with the information needed to obtain a general understanding of what operator errors occur in serious accidents and incidents (especially EOCs) and what strongly influences these errors to occur (i.e., error-forcing context),
2) provide the "reasons" why unsafe actions occur, which lead to the identification of error-forcing contexts, and
3) provide examples of unsafe actions and error-forcing contexts.

The first goal will be accomplished by explaining the principles underlying ATHEANA through discussions such as those provided in Section 2. As in Section 2, relevant psychological theory should be included and illustrated by insights from event analyses such as those summarized in Section 2.4 or those detailed in the HSECS report (Cooper et al., 1995).

The second goal is essential to leading the ATHEANA user from identified HFEs to the appropriate associated unsafe actions and EFCs. Structured information, which has embedded both psychological theory and operational experience, will provide ATHEANA users with the "reasons" for unsafe actions, as characterized by observable EFCs and underlying (but not observable) error mechanisms.

The third goal of the knowledge-base will be achieved by providing both generic and event-specific examples, generated from analyses of operational experience. This information is envisioned to consist of categories of plant conditions and PSFs, which make up the EFCs, as well as examples of unsafe actions and problems in different information processing stages.

### 3.4.3 Information Sources for Quantification

Guidance on how to estimate the probabilities of the HFEs will follow the philosophy underlying the equation introduced in Section 3.3 above. The estimation will focus on estimating the frequencies of each error-forcing context corresponding with each unsafe action. Then, the frequencies of all EFCs and unsafe actions will be multiplied by the probabilities of human error given each EFC and, finally, summed to obtain the HFE probability. Frequency estimates may be based upon some actuarial data but will almost certainly require a large element of expert judgment. Thus, application of ATHEANA will also require guidance on how to elicit expert opinion and on the choice of experts.

Potential actual data sources include:

- plant-specific and generic component failure statistics (e.g., frequencies of instrumentation failures or multiple or repetitive hardware failures) [NRC's sequence coding and search system (SCSS) (NUREG/CR-3905) is a possible generic data source.]

- plant-specific or generic operating practices (e.g., frequencies of instrumentation taken out of service for maintenance while at power, operations occurring with exceptions to limiting conditions for operation, plant evolutions while at power especially those performed during the evening and midnight shifts when human vigilance is low)

- results from engineering (e.g., thermal-hydraulic) calculations

- generic human performance data, such as that for variabilities in operating crews abilities to perform correct situation assessments reported by Roth et al. (NUREG/CR-6208)

Expert judgment is used whenever actual data cannot be obtained. Examples of experts include operators and plant operations, training, maintenance, and engineering (especially data trending) personnel.

## 3.5 Ongoing Development Work

The results of the development work to be performed during this project will be presented in two parts; a frame-of-reference (FOR) manual which describes the technical basis for the method and for the judgements needed to apply the method, and an implementation guidelines manual which will provide a step-by-step description of the method. The FOR manual will contain the ATHEANA knowledge-base while the implementation guidelines manual will provide guidance concerning the ATHEANA application process. A parallel to this separation of knowledge-base and process description is found in the Handbook of Swain and Guttmann (NUREG/CR-1278), of which Chapter 4 presents the basis of the method and Chapters 6-19 provide the data used by the method (together being equivalent to the FOR manual), and Chapters 5 and 20 describe the method (corresponding to the implementation guidelines). Both ATHEANA manuals are described briefly below.

The purpose of the implementation guidelines is to provide guidance to HRA analysts applying ATHEANA. The implementation guidelines will be expanded upon the description of the ATHEANA application process given in Section 3.4.1. In addition, the work described in Section 6 of this report is directed towards developing the implementation guidelines. Guidance will include how to use the FOR manual and other information sources (e.g., plant experts) as necessary in applying ATHEANA as well as how to perform specific ATHEANA application steps.

As stated above, the purpose of the frame-of-reference manual is to serve as the ATHEANA knowledge-base. The information provided in the FOR manual allows the analysts to make use of "lessons learned" in the development of ATHEANA without having to repeat the development process. As described in Section 3.4.2, the knowledge-base provided in the FOR manual is based on two sources of information which are:

- models of human errors and their causes, developed from a review of current literature in the behavioral sciences; and
- analyses of operational events that have involved significant contributions of human errors to the course of events.

In addition to the general principles described in Section 2, the work described in Section 5 of this report is directed towards developing the FOR manual.

# 4. TRIAL APPLICATION OF THE CONCEPTS

## 4.1 Introduction

This section documents a trial application of the ATHEANA method as described in Section 3. The trial application included, for a specific PRA scenario, the first demonstration of the following ATHEANA process steps (see Figure 3.1):

- identification of an human failure event (HFE)
- identification of an unsafe action associated with the HFE
- identification of an error-forcing context (EFC) associated with the unsafe action
- estimation of probabilities for each EFC
- quantification of the HFE using the estimated EFC probabilities

The goal of the trial application was to identify a new HFE that is not currently modeled in PRAs, but materially adds to risk, and to demonstrate how to quantify the probability of this HFE based upon the frequency of associated error-forcing contexts, using the quantification model given in Section 3. In particular, the intent was to identify an error of commission (EOC) that should be included in a PRA model which previously was not considered credible.

As mentioned in previous sections, a critical element in the new HRA method is the identification of unsafe acts and their associated EFCs. The trial application of ATHEANA paralleled the efforts described in Sections 5 and 6, triggering the development of search processes for HFEs, unsafe actions, and EFCs and the integration of the psychological and operational experience knowledge-bases with respect to error causes. As discussed in Section 6, and below, further refinement of the knowledge-base through integration of psychological theory and analysis of historical experience, is required for additional development of the search processes for unsafe acts and EFCs. Also, a frame-of-reference (FOR) manual will be developed to serve as the knowledge-base of psychological theory and historical experience for future applications of ATHEANA.

Section 4.2 discusses the resources (e.g., available experts, knowledge base for searches, PRA and plant information) used in the trial application. The selection of a PRA scenario, including the initiating event, is described in Section 4.3. Sections 4.4 - 4.7 describe the demonstrations of the key process steps in the new method: identification of an HFE, identification of an unsafe action, identification of an EFC, and quantification of the EFC, and resulting HFE probability. Section 4.8 recaps the key elements of the process for HFE identification used in the trial application. Section 4.9 summarizes the accomplishments of the trial application.

## 4.2 Trial Demonstration Resources

The trial application of ATHEANA was performed without benefit of several resources which will be available for future users of the method. Alternative resources used in the trial application are indicated below.

As described in Section 3, subject experts (e.g., plant operations, operator training, systems, thermal hydraulics, PRA) are needed for implementation of various steps in ATHEANA. For the purposes of the trial application, the ATHEANA development team served as both experts and HRA/PRA modelers.

The frame-of-reference (FOR) manual, which will be developed in future project work, was not available for the trial application. However, the HRA method development team was very familiar with the material that will comprise the FOR manual (e.g., concepts discussed below in Section 5, event analyses, including those given in Appendix C of NUREG/CR-6093, NUREG/CR-6265, the HSECS database, and Section 5).

The guidelines for applying ATHEANA also will be developed in future project work. The quantification model and the process diagram given in Section 3 served as the basic guide for performing the trial application.

Reference material used in the trial application included emergency operating procedures (EOPs) and the existing NUREG-1150 PRA for the Surry Unit 1 nuclear power plant. The quantification process described in Section 3 calls for a multi-stage elicitation process and could often involve detailed calculations. For the purposes of the trial application, this process was abbreviated. In general, quantification was performed based upon the development team's judgment. This judgment was supplemented by readily available generic data.

## 4.3 The Scenario: A PWR Small-Break LOCA

For the purposes of the trial application, the first step was to select a PRA scenario. (In an actual HRA/PRA application, each PRA scenario would be examined for candidate HFEs to add.) The team constrained this selection to full-power conditions. The specific PRA used in the trial application was the Surry Unit 1 (a PWR) NUREG-1150 PRA (NUREG/CR-4550, Vol 3). By using an existing PRA, comparisons between the original PRA and the trial application could be made easily. In addition to the NUREG-1150 reports themselves, considerable Surry-specific documentation (e.g., EOPs and abnormal procedures) was available to the project team because BNL performed the Surry low power and shutdown (LP&S) PRA (NUREG/CR-6144). Some project team members were already familiar with Surry's design, operations, and procedures due to their involvement in the LP&S PRA. Also, Surry's Individual Plant Examination (IPE) was available.

For the purposes of the trial application, the small-break loss-of-coolant accident (SLOCA) initiating event and event tree were chosen. SLOCA was selected because it can evolve into core damage if active systems do not perform adequately. Also, the SLOCA event tree typically has a simple structure (i.e., few plant functions and associated event tree headings) which was desirable in order to make the results of the trial application more clear.

Once the PRA scenario was chosen to be a SLOCA, the team focused its efforts on incorporating operational experience, especially event reports involving LOCAs and other accidents with similar characteristics (e.g., TMI-2, Dresden 2 (8/2/90), Fort Calhoun (7/3/92), and Crystal River 3 (12/8/91)). In future applications of ATHEANA, insights from operational experience will be represented in the frame-of-reference manual.

## 4.4 Identification of an Error of Commission HFE

The next step in the trial application was to identify a candidate HFE to model in the Surry SLOCA event tree. For the trial, the goal was to identify only one candidate HFE which would be investigated further to demonstrate ATHEANA. In an actual application of ATHEANA, the search for appropriate HFEs (including those not previously modeled) would include examination of all plant functions for each event tree, those both explicitly and implicitly modeled. Such searches are expected to result in the identification of several candidate HFEs. The undesired plant state which should ultimately result from the identified HFE is core damage. In lieu of consulting the material to be included in the FOR manual, the team reviewed current developments in the knowledge-base of error causes represented by the discussion given in Section 5.

In order to meet the objectives of the trial application (see Section 4.1), as well as those for developing ATHEANA, it was desirable for the HFE identified in the trial to be an error of commission (EOC).

The Surry Unit 1 SLOCA event tree (NUREG-4550, Vol. 3) was reviewed. In this event tree, few operator actions are required in response to a SLOCA and those modeled in SLOCA are errors of omission. Working backwards from plant end states through the event tree, and using associated EOPs, the team first considered events after cooldown, but the time available for performing actions and recovery is very long. Next, events during residual heat removal (RHR) or recirculation cooling were considered but they have similar time frames and PSFs to events after cooldown. Events associated with the switchover to recirculation or RHR offer more opportunity for operator failures, but these opportunities occur after operators already are committed to establishing a long term cooling path and are attentive to possible problems. Consequently, the team turned its focus on the high pressure injection phase of a SLOCA event. This priority was based on the judgement that errors associated with this function are more likely to lead to core damage.

Coincident with the review of the SLOCA event tree, the team reviewed various analyses of events which had been performed by the team over the course of the project. This review revealed that there have been some significant incidents in which high pressure injection (HPI) has been inappropriately throttled or terminated. Most notably, the accident at Three Mile Island 2 (Kemeny, 1979, Rogovin and Frampton, 1980) involved inappropriate throttling and securing HPI, which lead to core damage (and the worst accident to take place in the U.S. commercial nuclear power industry). A more recent event occurred at Crystal River 3 during startup involving inappropriately bypassing ESF and the automatic actuation of HPI (AEOD, 1992). Comparison of the cognitive processing which took place in both of these events revealed additional common elements in these two events; both involved failures in situation assessment which were caused, in part, by instrumentation problems that misled operators regarding the actual plant status and which persisted for some time in the event, despite contrary evidence (e.g., alternative plant indications).

Next, the requirements for success of the high pressure injection function in a SLOCA were reviewed with respect to the four basic ways in which operators can fail plant functions through errors of commission:

- Operators can turn off running equipment
- Operators can bypass the signals for automatically starting equipment
- Operators can change the plant configuration such that plant defenses are defeated
- Operators can deplete or divert plant resources (e.g., water supplies)

Of these options, all are viable failure modes for SLOCA, except for the bypass of HPI actuation (which is typically assumed* to occur either simultaneously or very quickly after reactor trip). However, based upon the reviews described above, the HFE chosen for the trial application was the inappropriate termination of HPI in a SLOCA (persisting to the point of core damage). For this first demonstration of ATHEANA, this HFE was assumed to be independent of other HFEs modeled in SLOCA scenarios (either those already modeled in the SLOCA event tree or other candidate HFEs which could be identified).

## 4.5 Identification of an Unsafe Action

As defined in Section 2, an unsafe action represents those actions inappropriately taken, or not taken when needed, that result in a degraded plant safety condition. Unsafe actions are defined with respect to people, their actions, inactions, and associated causes, in contrast to HFEs which are defined in terms of the impact on plant functions and equipment. Also, unsafe actions may correspond directly with the definition of an HFE but, more commonly, represent a "finer" level of detail. Consequently, several different unsafe actions could result in the same outcome with respect to the success of plant functions and, therefore, be associated with the same HFE. It is for this reason that a summation over all unsafe actions is included in the equation given in Section 3.2 for the ATHEANA quantification model.

For the trial application, the team chose one unsafe action associated with the HFE, "Operators (inappropriately) terminate HPI." At the time of selection, the error cause material represented in Section 5 was in the early phases of its development. Consequently, the identification of possible unsafe actions associated with "Operators terminate HPI" largely was based upon the general principles described in Section 2 and the "tokens" found in operational experience which are catalogued in Section 5. Also, for the purposes of demonstrating the capabilities of ATHEANA in the trial application, the selection of an unsafe action was constrained to "mistakes," or a purposeful yet erroneous actions, rather than "slips" which are commonly included in current PRA models. The experience of performing the trial application will be used to develop a more formal process for identifying unsafe actions, which will be addressed in the next demonstration of ATHEANA.

In practice, the identification of potential unsafe actions involves the development of a minimal description of the reasons why operators would take actions leading to the HFE. Such descriptions must conform with the fundamental ground rule of the ATHEANA: operators behave rationally. The search for candidate unsafe actions, then, amounts to the search for rational explanations for what current HRA/PRA modeling considers non-credible. For the HFE in the trial application, the first level of explanation for why "Operators terminate HPI" which corresponds with an EOC mistake is that they think it is the "right thing" to do, under certain circumstances or contexts as the operators perceive them. Plant indications, procedural instructions, operating practices, and training experience are examples of the resources used by operators in the information processing required for response to an event. As described in Section 2, problems in information processing can arise from hardware failures (e.g., instrumentation fails high) or human failures (e.g., operator misreads instrument) and manifest themselves in failures in detection, situation assessment, response planning, and response implementation. The team postulated a few different information processing problems and the possible combinations of resource "failures" (e.g., instrumentation failures, procedures incomplete) and human failures. The goal of such

* A more detailed investigation of candidate HFEs would relax this assumption and investigate possible unsafe actions and associated error-forcing contexts for pre-accident or latent errors.

postulations was to identify a rational way in which operators could get "off track" and not see the need for reactor coolant system (RCS) makeup (including long-term makeup). For example, if there is a decision point in EOPs for securing HPI, and if the plant conditions and PSFs influence operators to form a rationalization that gets "anchored" and followed, operators may turn off injection. If the rationalization or other factors could allow operators to miss, ignore, or misinterpret mounting evidence of loss of cooling, core damage would ensue. Note, that operators need not disregard mounting evidence forever, just long enough for core damage to occur. Real operational events show that substantial delays in the performance (or reversal of appropriate operator actions) can occur, when operators "know," incorrectly, what the state of the plant is.

The unsafe action finally selected by the team for the demonstration was described as "Operators turn off operating HPI pumps, given the mistaken belief that the safety injection (SI) termination criteria given in procedures have been satisfied." This description constrained the subsequent identification of an error-forcing context to searches of EOPs (especially with respect to SI termination criteria) and potential problems in the use of instrumentation that could lead operators down the wrong procedural paths. Furthermore, to fully satisfy the definition of the HFE, information processing problems must persist long enough for core damage to occur, despite accumulating and contrary evidence (e.g., plant indications). In order to achieve such persistence, the unsafe action defined above requires an associated error-forcing context that defeats (or "short circuits") accumulating and contrary evidence.

## 4.6 Identification of an Error-Forcing Context

Based upon the discussion above, there are at least three elements of an error-forcing context to be identified for the unsafe action and HFE defined in the trial application. First, a decision point must be identified in EOPs which directs operators to turn off operating HPI pumps. Secondly, plant conditions (including hardware operability and reliability) and PSFs which could convince operators that SLOCA conditions do not exist must be identified. Finally, plant conditions and PSFs which could cause operators to persist in their belief that SLOCA conditions do not exist must be identified. In some cases, the same plant conditions and PSFs which could satisfy the objectives of the second search also could satisfy the objectives of the third search.

*Procedure Search*

Using EOP 1-E-1 for Surry Unit 1, the team searched for an opportunity to secure operating high pressure injection pumps. In particular, the EOP was reviewed to identify the criteria for termination of SI and how those criteria could be misconstrued and result in an early termination of HPI. The termination criteria, identified from EOP 1-E-1 Step 6, for an acceptable termination of SI are all of the following (i.e., if conditions a, b, c, and d are met, then secure HPI):

a) RCS Sub-Cooling Margin (SCM) > 30°F
b) Secondary Heat Sink:

   - Total feed flow to INTACT SGs > 350 GPM
   - Narrow range level in at least one intact SG > 9%

c) RCS pressure - stable and increasing
d) Pressurizer Level > 11%

Given that all of these criteria are met, operators are directed to transition from 1-E-1, Step 7 into 1-ES-1.1, SI TERMINATION, Step 1. Operators are directed to terminate running HPI pumps in 1-ES-1.1.

Having identified a procedural path and associated guidance for HPI termination, the team next searched for the contexts (i.e., combination of plant conditions, PSFs) for which the interpretation of the above termination criteria could be difficult or misleading, and potentially result in a misinterpretation of the plant state and, consequently, a decision to terminate HPI prematurely. Some preliminary potential threats to the correct interpretation of the termination criteria were identified by the team and are described below.

*Plant Condition #1: Incorrect RCS Pressure Measurement (i.e., false high)*

An erroneously high output from the RCS pressure instrumentation would falsely indicate that both item (c), RCS pressure, and item (a), RCS sub-cooling margin, were met. Because there are multiple pressure instruments, two out of four must fail high, perhaps by common cause (e.g., miscalibration, drift).

With plant condition #1 in place, two of the four termination criteria are satisfied.

*Plant Condition/PSF #2: Unreliable Pressurizer Level Indication*

The team judged the chance of a common cause instrument failure, in addition to those associated with plant condition #1, to be unlikely. Consequently, the team searched for alternative types of combinations of plant conditions and PSFs.

One alternative is that the SLOCA is the result of a power-operated relief valve (PORV) being failed in the open position. When a PORV is stuck open, RCS inventory exiting the pressurizer causes the pressurizer level indication to read incorrectly. The example for this scenario represents, of course, the accident at TMI-2 and is the scenario used for HFE quantification in the trial application.

*PSF #3: Lack of mental clarity, etc.*

One final factor in the EFC for the unsafe action of the trial application was required. In order to fully convince operators that the HPI termination criteria are met and to persist in this belief until core damage, the team postulated a PSF/error mechanism combination associated with less than optimal information processing. Operational experience provides numerous examples of suboptimal performance, caused by broad range of factors including fatigue, stress, and early morning hours (i.e., performance is known to be at its lowest ebb between the hours of 2 a.m. to 6 a.m.).

In addition, Roth, et al. (NUREG/CR-6208) reported that some operating crews never correctly diagnosed the plant state in simulator experiments designed to investigate operator performance under cognitively demanding situations.

### 4.7 HFE Quantification

The quantification process described in Section 3 was carried out, using the judgment of the team and supplemented by readily available data. The purpose of the exercise was to demonstrate how to translate the EFC identified above into terms that are quantifiable.

Table 4.1 summarizes the quantification of the EFC developed for the trial application HFE. The table shows the initiating event and each of the elements for the HFE error-forcing context identified above. Estimates, generated based upon the development team's judgment, for the SLOCA frequency and the probability of each EFC element also are shown. In actual applications of ATHEANA, analysts will refer to generic (e.g., sequence coding search scheme (SSCS)NUREG/CR-3905) and plant-specific (e.g., component reliability reports) sources of data.

The SLOCA frequency was estimated with a generic, rough order-of-magnitude value rather than with any specific source. Consistent with the discussion above, the probability for unreliable pressurizer level instrumentation was estimated as the probability of the SLOCA being due to a stuck open PORV (i.e., half of SLOCAs are assumed to be due to stuck open PORVs). The probability of 2/4 pressure indicators failing high was estimated with the following equation for failure probability using the beta factor method of common cause failure modeling:

**Table 4.1 Quantification Demonstration Results**

| | Initiating Event | Error-Forcing Context | | |
|---|---|---|---|---|
| Event | SLOCA | Unreliable Pressurizer Level | 2/4 High Pressure Indicators Stuck High | Operators Believe HPI Termination Criteria Met And Fail to Recover |
| Frequency or Probability | $2 \times 10^{-2}$/year | 0.5 | 0.01 | 0.15 |
| Basis | Rough estimate for demonstration | Rough estimate for demonstration | Rough calculation | P(2 am - 6 am) as surrogate for lack of mental clarity |

$$\text{Failure Probability} = \beta\ (1/2\ \lambda\ t)$$

and using the following assumptions: $\beta = 0.1$, $\lambda = 10^{-5}$, and t = 18 months mission time. The failure rate corresponds to a relatively high value associated with Rosemount pressure transmitters (Carbonaro et al., 1991). Finally, the probability of "lack of mental clarity" was estimated as being the probability of the event occurring early in the morning (i.e., between 2 a.m. and 6 a.m.) - approximately one-sixth of a day.

Since all of the elements representing the EFC together define (and quantify) the HFE, the probability of the HFE is equal to the product of all the EFC probabilities shown in Table 4.1, i.e.,

$$\text{HFE Probability} = 0.5 \times 0.01 \times 0.15 = 7.5\text{E-}4$$

The EFC elements together with the SLOCA initiating event comprise a PRA cut set. In other words, if cut sets for SLOCA and the new HFE were generated by PRA quantification codes, then one cut set would consist of only two basic events: the SLOCA initiating event and the HFE. The frequency of core damage from the new scenario involving SLOCA and the newly identified HFE can be calculated as the product of all of the terms in Table 4.1:

$\varphi$ (core damage due to SLOCA and operators secure HPI) = $1.5 \times 10^{-5}$

The rough estimate given above is for illustration purposes only. In actual practice, more thorough modeling of each event and analysis of data sources would occur. Nevertheless, this rough order-of-magnitude calculation suggests that HFEs, which have no or negligible impact when only "nominal conditions" are considered, can be significant contributors to plant risk when considered under an appropriate EFC.

## 4.8 Summary of Trial Search Approach

The following summarizes the search process used to identify the new HFE and associated EFCs in this trial application as the initial step in formalizing a search strategy for general application. The search first focused on selecting a feasible HFE, then on identifying an EFC that can negatively impact any stage of the information processing model of operator cognition; i.e., detection, situation assessment, response planing, or response implementation. The steps followed can be summarized as follows:

1. For the initiating event chosen, the nominal success path of the event tree was reviewed to identify the highest priority possibility for an important, unmodeled HFE. High priority had two components. Firstly, the HFE must increase the chance of core damage. Secondly, the selected HFE should appear to the elicitation team to be more likely than other candidates, or at least must appear to be plausible. In the trial application the issues of time available for recovery, initial commitment of the crew, and crew attention were the factors that led the team to select the HPI phase of the SLOCA scenario.

2. For the function chosen, the applicable procedures were reviewed, and the event scenario was played out against those procedures taking into consideration both the expected normal progression of the scenario, as well as possible variations that could occur within the PRA definition of the scenario. As a result of this search, a plausible unsafe act, i.e., inappropriate termination of SI, was identified. The unsafe act was considered plausible in that there is a reason why, under some circumstances, the operators might be led procedurally to terminate SI.

3. The search for an EFC continued by attempting to identify a context that could provide a threat to situation assessment. Examples of contextual factors that were thought to be relevant included:

   - Decision criteria that may not be clearly met at the point in the scenario when the operators come to each criterion in the procedure

     - Equipment failures that mimic decision criteria

     - Potential cognitive failures that could mimic decision criteria

     - Anomalous plant conditions that could appear to be an expected event (but actually represent a different one); for example, in this trial application, a continuing LOCA exhibits some of the characteristics of a non-LOCA condition.

To identify the potential for such contextual factors, the following lines of investigation were followed:

Ways in which automatic signals or indications relevant to the appropriate decision criterion could be generated were identified [e.g., SI from LOCA (low reactor pressure), containment spray (high containment pressure); steam rupture (low $T_{AVE}$ and high steam flow); spurious actuation (above signals or manual signal generated spuriously)].

Searches were made for hidden system (e.g., I&C) interconnections that when combined with particular plant conditions could lead to, or influence, an erroneous situation assessment and thereby comprise an EFC. This could include a combination of: 1) ambiguous or misleading procedures; 2) faulty instrumentation either in the past or at present, e.g., a bad indicator, or a good indicator with correct reading but interpreted by the operators as a reading that cannot be true (confirmation bias or history effects); and 3) an extremely sensitive (unforgiving) plant condition e.g., two-phase mixture in the RPV or going solid in the pressurizer.

Searches were made for equipment failures that could affect the plant state during the scenario and thereby impact the operators' interpretation of the scenario. In these cases, an understanding of the thermal-hydraulics characteristics of the scenario in both the nominal and off-normal scenarios was essential.

Other potential activities that could be going on in the control room or plant that might potentially distract the operators while responding to the scenario (e.g., responding to management, NRC, or other authorities; additional related or unrelated failures; tests or other operational activities) were considered.

The search process as described above relied heavily on collective brainstorming; the process is not yet structured to lead analysts to the identification of HFEs and EFCs in a comprehensive way. Nevertheless, the trial application has demonstrated that it is possible to identify HFEs that are not generally included in current PRAs, and to identify EFCs that have a non-negligible impact on the estimation of core damage frequency. Thus, the trial application has demonstrated that, by developing and formalizing search procedures from the beginnings presented above, it is feasible to enhance the realism and comprehensiveness of PRAs in their treatment of human-system interactions.

## 4.9 Findings

Based upon both its limitations, and its success, the trial application was equivalent to a "proof of concept" for ATHEANA. The trial application demonstrated that it is possible to identify HFEs which are not generally included in current PRAs and associated error-forcing contexts that have an observable impact on the frequency of core damage in the PRA. Thus, applying these search techniques will improve the PRA by identifying additional risk-significant scenarios. However, the approaches demonstrated here identify single, specific token events. They only hint at the total impact of these human contributions to risk under rare, but trying conditions. Work must proceed by continuing to develop and apply the search process to additional and increasing complex PRA scenarios.

# 5. DEVELOPMENTS IN UNDERSTANDING THE CAUSES OF UNSAFE ACTIONS

## 5.1 Introduction

The most difficult task in applying the ATHEANA HRA approach is the identification of unsafe actions and associated error-forcing contexts for defined HFEs. This task requires that a connection be made between the causes of human errors and the observable influences on human performance. These observable influences are the error-forcing context elements (i.e., the plant conditions and associated PSFs). In addition, these EFC elements must be auditable so that predictions regarding likely human errors can be made.

As stated in Section 3, the ATHEANA frame-of-reference (FOR) manual will contain the knowledge-base regarding the causes of human error, taken from both psychological theory and operational experience. Specifically, the FOR manual will provide ATHEANA users with:

1) the information needed to obtain a general understanding of what operator errors occur in serious accidents and incidents (especially EOCs) and the role of error-forcing contexts in such events,

2) the "reasons" why unsafe actions occur, leading to the identification of EFCs, and

3) examples of unsafe actions and EFCs.

The discussions given in Section 2, which will be included in the FOR manual, provide some of the basic understanding specified in item 1 above. However, additional explanation and information is required to address the "reasons" for unsafe actions and to characterize unsafe actions and EFCs through illustrative examples. To address item 2, Section 5.2 below provides some examples of causal factors, including some traditionally defined error mechanisms, and Section 5.3 provides some generalized insights from operational event analyses regarding operator performance. Section 5.3 also provides some illustrative examples of unsafe actions and EFCs taken from operational event analyses. Section 5.4 briefly discusses the implications of the insights given in Sections 5.2 and 5.3 for HRA using ATHEANA. Overall, the information provided in these two sections is a precursor to what is expected to be included in the FOR manual, when it is developed in future project efforts.

## 5.2 Understanding Derived from Behavioral Science

In Section 2, understanding from behavioral science and related fields was drawn upon to establish the underlying principles of ATHEANA. Additional knowledge can be drawn from psychological theory to further develop the ATHEANA users' understanding of causes of human error. As stated earlier, error mechanisms, in the wrong context, can be considered "causes" of human errors. Also, different error mechanisms are associated with each of the four stages of information processing. Examples of error mechanisms and other causal factors are provided below for each information processing stage and are related to potential error-forcing context elements. It is expected that additional behavioral models will be used as information resources in the FOR manual as necessary to realistically represent post-initiator human performance issues.

### 5.2.1 Detection

Detection involves the first steps in people becoming engaged in problem resolution through the subsequent steps of situation assessment and response planning. Hence, failures in detection lead to a failure to start the situation assessment and response planning phases.

Error mechanisms that can lead to a lack of detection are those that cause an oversight of important annunciators, alarms, or other indications. Two principal error mechanisms have been identified as important in this phase of the information processing. These are: (1) salience bias; and (2) confirmation bias.

Salience bias is the tendency to give closer attention to the most prominent, the loudest, or the most "compelling" indications and to provide less attention to less compelling indications even though these less compelling indications may be important in diagnosing between different events. Such a tendency can be particularly important when events occur during "high tempo" operations when operators may be preoccupied by other activities and indications. They can involve situations where the annunciators or indicators are obscured by other, more prominent (physically or psychologically) indicators or controls. Such error mechanisms could also be the result of inadequately designed information systems where the annunciators and indicators fail to provide suitably compelling (or even discernible) information for the particular plant condition (for example, indications provided only by trends shown on slow-moving chart recorders).

Three particular combinations of plant conditions and PSFs can be seen to make the salience bias error mechanism more likely:

1. "High-tempo" or other activities (such as multiple concurrent tasks) that distract the operators from monitoring annunciators or other indications <u>and</u> indications that are less compelling or direct in getting the attention of the operators during the periods of distraction.

2. Events where the most important indications are obscured or not immediately visible from the location of the operators responsible for monitoring the plant. This situation could result from two conditions: poor interface design from the perspective of the operators' normal locations, or the operators working in a location away from the normal interface and therefore are unable to readily observe the indications.

3. Situations for which there are no significant and compelling annunciators, such as those events that arise slowly and involve the operators having to observe trends on dials or strip chart recorders.

### 5.2.2 Situation Assessment

Roth et al. (i.e., Figure 2.2 in NUREG/CR-6208) shows types of observable behaviors that result from situation assessment. Activities associated with situation assessment include activities to:

- search for explanations
- detect abnormal plant behavior
- identify problems (e.g., sensor failures, plant malfunctions)
- detect alarms/symptoms that had been missed
- explain observed symptoms

- check for evidence to confirm a hypothesis
- identify unexpected plant behavior

- ánticipate future problems

Situation assessment therefore includes all those activities by the operators to understand what the current condition of the plant is and that (in the post-initiator phase) some event has occurred (though not necessarily what has occurred), and to understand that actions may be necessary.

There are several different error mechanisms that may result in situation assessment problems. These include the availability and representativeness heuristics and recency bias. The availability heuristic is when a judgment is made on a readily recalled (most readily available) memory, such as a most recent similar event (recency bias) or when a pattern of failures that are somewhat similar has previously occurred or been emphasized in training. The representativeness heuristic is when a judgment is made on some part of the evidence that strongly "represents" a particular condition. For example, falling reactor coolant system pressure in a PWR start-up event can be the basis for operators believing that the reactor is being over-cooled even when other data suggest a loss-of-coolant accident.

In addition, there are error mechanisms that can result from the need to perform deeper analyses of the state of the plant beyond simple pattern matching, particularly when procedure-based responses have been tried but have failed. Reason (1990) describes the situation assessment/response planning activities when faced with the onset of a problem condition as starting out in the rule-based mode since people:

> "...are strongly biased to search for and find a prepackaged solution at the RB [rule-based] level *before* resorting to the far more effortful KB [knowledge-based] level, even where the latter is demanded at the outset... They do this by matching aspects of the local state information (the problem configuration) to the situational elements of stored problem-handling rules of the kind: *if (situation) then (system state), if (system state) then (remedial action).* Only when people become aware that successive cycling around this rule-based route is failing to offer a satisfactory solution will the move down to the KB level take place. And even here problem solvers are likely, at least initially, to be using 'workspace' processing to search for cues that remind them of previously successful rules, which could then be adapted to the present situation."

Therefore, the evaluation of situation assessment (and, later, response planning) must consider error mechanisms associated with knowledge-based processing.

As Reason (1990) discusses, error mechanisms associated with knowledge-based behavior can be different from those associated with other types of behavior. Examples include: limited searches for explanations of symptoms or limitations in working memory (*bounded rationality*); incomplete or inaccurate knowledge; and short cuts in reasoning caused by inappropriate use of analogies (such as *memory cuing* and *matching biases*). In addition, Woods et al. (1994), have further identified several issues associated with errors in the use of knowledge in cognitive processes. These include:

- inaccurate or incomplete mental models and knowledge flaws
- overconfidence despite incomplete knowledge
- "inert" (i.e., "known" but not accessible during the time of need) knowledge

### 5.2.3 Response Planning

The categories of observable behaviors associated with response planning identified by Roth et al. (NUREG/CR-6208) are to:

- identify goals
- evaluate appropriateness of EOP procedural path
- fill in gaps in procedures
- evaluate consequences of actions
- adapt procedures to situations
- catch errors

As with situation assessment, operators can (in almost all foreseeable cases) respond initially according to the guidelines in the procedures to the degree that procedures provide appropriate guidelines. In other words, the progression from rule-based to knowledge-based behavior described by Reason (1990) with respect to situation awareness also applies to response planning.

Reason has identified a spectrum of behaviors relating to the use of good "rules" (i.e., adequate procedures), bad "rules" (i.e., flawed procedures) and no "rules". He observes that, from the HRA perspective, there are two outcomes: successful performance, and unsuccessful performance. Unsuccessful performance, for example, can be the result of procedures that contain technical flaws or omissions - that is, the operators follow a correctly selected rule, but the rule is "bad". When implemented as written, these procedures either lead to an incomplete response to the event or an inefficient or delayed response. Unsuccessful performance also can occur when operators either have recognized that the procedures are inadequate and try to apply knowledge-based reasoning to the situation, or when the operators decide for some reason that the procedures should not be applied and leap directly to knowledge-based behavior. Tactical decisionmaking refers to this second class of behavior, where operators apply knowledge-based behavior in abnormal or accident scenarios because of perceived or real limitations in procedures. Therefore tactical decisionmaking applies in the cases of bad or non-existent rules. The successful outcomes involve effective knowledge-based behavior.

The cases involving bad or non-existent rules involve latent failures in the procedure-development process (that is, they are created before the event), though it is also recognized that to some degree all procedures contain some deficiencies or simplifications. Therefore, in the cases of bad or non-existent rules, the concern is to identify situations in which these deficiencies are most likely to occur. The following examples are based on earlier reviews of operational events, particularly those described in NUREG/CR-6093:

1) the procedures are temporary, as in the case of special test procedures or during low-power operations;

2) procedures have been recently revised or have never been implemented in an actual event; and

3) procedures used in training (particularly in the simulator) are different from those used in the plant.

### 5.2.4 Response Implementation

Response implementation typically requires three separate factors if there is to be a successful response: communicating instructions, accessing the required equipment, and selecting and operating the required equipment. None of these factors are error mechanisms in the traditional sense. Rather, they are examples of typical human engineering concerns. Additional human engineering concerns with respect to response implementation are expected to be considered in the development of the FOR manual.

Equipment required for accident response is typically controlled or manipulated from the control room and/or at the equipment location. In many cases, equipment required in the response phase is operated from the control room, in which case there are a limited number of potential problems with access. For example, some equipment requires keys to operate switches. These keys are under the administrative control of specific shift personnel. Under what conditions might access to these keys be difficult or impossible? How are administrative controls handled when designated personnel are not present in the control room (for example, when trouble-shooting?).

When equipment is located outside of the control room, its access can be of greater concern. The following are plant features and PSFs that could play a role in limiting, delaying, or otherwise confounding access:

- Access control systems. Under what plant conditions can the access control system(s) significantly limit timely access to the relevant equipment areas? For example, what is the relative probability of failure of access control under the accident conditions? (Loss of power, etc.)

- Access under accident conditions. Under what conditions can the accident scenario impede access to the relevant plant areas (radiation, heat or steam, etc.)?

The final stage of response implementation is associated in many cases with selection and operation of controls: the classic switch-selection and operation. Two examples of factors which can result in misselection or mis-operation are:

1) High tempo operations, multiple distractions, and other conditions which can result in operator inattention,

2) Equipment manipulations required in parts of the plant which are susceptible to wrong unit or wrong train errors (e.g., mirror-image vs. same-image layouts for multiple units; unit coding or labeling problems).

Two communication problems which can negatively impact response implementation are:

1) Lapses in communication. Data as communicated in verbal instructions become recalled incorrectly by the people implementing the instructions.

2) Inadequate hearing. Information or data sent by one individual are misheard by the intended recipient(s) (e.g., environmental noise, inadequate channels (radios, telephones).

## 5.3 Understanding Derived from Analyses of Operational Events

Previous project activities supporting the development of ATHEANA were focused upon understanding and explaining past operational events. Reviews of operational experience also assisted in the development of the trial application described in Section 4. In addition, retrospective event analyses were performed to demonstrate the use of the multidisciplinary HRA framework, and its underlying concepts and disciplines, to gain a better understanding and to develop and refine the framework to better reflect the reality represented by historical events. However, implementation of ATHEANA will require prospective analyses to identify what unsafe acts could occur which would result in human failure events to be modeled in the PRA. To ensure that ATHEANA is consistent with operating experience, these predictions must be consistent with what has been learned from past operational events. In addition, the specific contexts of past events must be generalized such that they can be applied and extrapolated to potential accident situations at other plants. At the same time, these generalizations must be detailed and specific enough to engender the identification and definition of unsafe actions and their associated error-forcing context(s) for defined HFEs.

Event analyses were performed to attempt to answer three questions: 1) what specific characteristics of error-forcing context elements (both plant conditions and PSFs) appear to strongly influence human performance in an accident, 2) what combination of EFC elements must occur together in order for an unsafe act to occur, and 3) which factors or combinations of EFC elements are not typically modeled in PRAs? In addition to being an input to the trial application, the identification of these individual factors and their combinations from event analyses represents a first step in the development of the knowledge-base which will be used to support searches for unsafe actions and associated EFCs and incorporated into the FOR manual.

Results from event analyses given in Section 5.3.1 below begins to address questions 1 and 2 above. Similarly, results given in Section 5.3.2 start to answer question 3. Analyses of three at-power events and two shutdown events were the basis for the results given in both these sections. The two shutdown events, Prairie Island 2 (2/20/92) (AIT, 1992) and Oconee 3 (3/8/91), (AEOD & AIT, 1991) were selected because they had been previously analyzed in earlier phases of the project and were known to contain many examples of factors which adversely effected human performance. The three at-power events, Crystal River 3 (12/8/91) (AEOD, 1992), Dresden 2 (8/2/90) (AEOD, 1992), and Ft. Calhoun (7/3/92) (AEOD, 1992), were selected primarily due to their similarity to the small-break loss-of-coolant accident (SLOCA) scenario which was chosen for the trial application (Section 4). In particular, both the Dresden 2 (AEOD, 1992) and Ft. Calhoun events were LOCAs and key features of the Crystal River 3 event (e.g., decreasing reactor coolant system (RCS) pressure, increasing RCS temperature, the need for high pressure injection) were similar to a SLOCA scenario.

### 5.3.1 Unsafe Actions and Important Error-Forcing Context Elements

First, the five events identified above were reviewed to identify important unsafe actions and EFC elements in past events, focusing upon how EFC elements (e.g., PSFs and plant conditions) impacted the four stages of information processing described in Section 2. Different examples of EFC elements were identified for each of the stages (i.e., detection, situation assessment, response planning, and response implementation). In addition, some elements (especially PSFs) were identified as being important but appeared to generally impact human performance, probably influencing multiple stages in information processing. For each stage (except detection), descriptions of types of unsafe actions were developed based on the analyses of operational events. These descriptions, while not representing a complete categorization, provide some additional means for discriminating between 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 which created the context, or some part thereof, for each category of failure have been identified. The results, summarized in Tables 5.3-1 through 5.3-5, 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, communications, human-machine interface (HMI), 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, procedural guidance not applicable to specific plant conditions).

Since there was more than one unsafe action 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 5.3-2, the first two EFC elements identified from the Dresden 2 event which cause operators to develop a wrong mental model of the plant are associated with one unsafe action, while the third and fourth EFC elements are associated with another unsafe action.

#### 5.3.1.1 Detection Problems

In general, problems in the detection of an accident or accident conditions are expected to be rare for at-power events. As shown in Table 5.3-1, only one of the five events (a shutdown event) analyzed included detection problems. Due to the number of alarms and other indications typically available during at-power operations, it is difficult to imagine a scenario in which operators would not be aware of the fact that something was wrong and that some sort of actions are needed. 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 5.3-1, 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) activated the instrumentation and procedural problems.

#### 5.3.1.2 Situation Assessment Problems

As shown in Table 5.3-2, four different situation assessment problems are illustrated:

1) operators develop wrong mental models of the plant state and plant behavior,

2) human interventions with the plant and its equipment (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,

3) wrong mental models can be strengthened by irrelevant information or the effects of (unknown) hardware failures, and

4) wrong mental models can persist in the face of contrary (and true) evidence.

Instrumentation problems are shown to be the predominant influence in all situation assessment problems included in Table 5.3-2. As shown by the contextual factors for the Crystal River 3, Dresden 2, and Ft. Calhoun events, wrong mental models are frequently developed due to instrumentation problems,

**Table 5.3-1 Examples of Problems in Detection**

| Human Impact | Contextual Influence | Event |
|---|---|---|
| Operators unaware of actual plant state, its severity, and continued degradation in conditions. | 1) Reactor vessel (RV) level instrumentation failed off-scale high due to unusual plant conditions (i.e., high $N_2$ overpressure).<br>2) Redundant RV level instrumentation readings require correction through hand calculations (and are performed incorrectly).<br>3) Procedures did not specifically address the high $N_2$ overpressure which 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 that 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 a various points during the draindown (some decreasing trend in overpressure was implied). | Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown. |

especially that associated with, and aggravated by, undiscovered hardware failures. Instrumentation also plays an important role in the confirmation of wrong mental models and in the rejection of information which is contrary to wrong mental models. Once operators develop a mental model, they typically seek confirmatory evidence (Reason, 1990). As shown in Table 5.3-2, when this model is wrong, several issues regarding confirmatory information arise and can further degrade human performance, for example:

1) information can be erroneous or misleading (e.g., field reports in the Crystal River 3 event),

2) plant indicators can be misinterpreted (e.g., sump alarms in the Oconee 3 event), and

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

In addition, operators often develop rational but wrong explanations for discounting evidence which is contrary to their wrong mental model. Table 5.3-2 provides some examples of such "rational" explanations for discounting or failing to recognize information which could lead to a more appropriate mental model of the plant state and behavior. Those "rational" explanations can result from indications

Table 5.3-2 Examples of Problems in Situation Assessment

| Human Impact | Contextual Influence | Event |
|---|---|---|
| Operators develop wrong mental model (or cannot explain) plant state and behavior. | 1) PRZR spray valve position indication inconsistent with actual valve position (due to pre-existing hardware failure and design).<br>2) No direct indication of PRZR spray flow provided. | Crystal River 3 (12/8/91), RCS pressure transient during startup. |
| | 1) Safety relief valve position indicating lights show the valve closed (although it has failed open).<br>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.<br>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.<br>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 RHR sump suction line despite two independent checks and one test.<br>2) Due to miscommunication, technician racked out then strokes RHR sump suction isolation valve (creating a drainpath 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).<br>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 5.3-2 Examples of Problems in Situation Assessment (Cont'd)

| Human Impact | Contextual Influence | Event |
|---|---|---|
| | 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.* | Dresden 2 (8/2/90), LOCA (stuck open relief valve). |
| Operators misinterpret information or are mislead by wrong information, confirming their wrong mental model. | 1) Erroneous report from technicians that one bank of PRZR heaters are at 0% power.<br>2) Cycling of switch for PRZR spray valve does not terminate the transient (because valve is broken). | Crystal River 3 (12/8/91), RCS pressure transient during startup. |
| | 1) Reactor pressure vessel pressure is less than the safety relief valve (SRV) setpoint (coupled with position indicating lights showing the SRV to be closed).** | Dresden 2 (8/2/90), LOCA (stuck open relief valve). |
| | 1) Reactor building normal sump high level alarm (interpreted as being the result of washdown operations). | Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown. |
| Operators reject evidence which contradicts their wrong mental model. | 1) Strip chart recorders show PRZR level increasing (which is inconsistent with RCS over-cooling and associated inventory shrinkage) but are not monitored.<br>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. |
| | 1) Indication of increased SRV tailpipe temperature (310°F).**<br>2) Back panel acoustic monitor shows red "open" light.** | Dresden 2 (8/2/90), LOCA (stuck open relief valve). |

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

**In the Dresden event, the wrong situation assessment regarding the SRV was temporary - within about one minute after actuation of the back panel annunciator, the shift control room engineer decides that the SRV must be open, and continues on a course of action associated with that correct situation assessment.

**Table 5.3-2 Examples of Problems in Situation Assessment (Cont'd)**

| Human Impact | Contextual Influence | Event |
|---|---|---|
| | 1) Reactor vessel (RV) level reading at 20" and decreasing. (Erroneous operation of the RV wide range level transmitter suspected.)<br>2) Health physics technician in reactor building verifies reduction in RV level and increasing radiation.<br>3) Operating 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.)<br>4) Evidence that RCS was not being filled and health physics technician notifies control room that there is 6"-12" of water on the floor near the emergency sump in the reactor building.* | Oconee 3 (3/8/91), loss of RCS and shutdown cooling during shutdown. |

that are not monitored (e.g., Crystal River 3), undiscovered hardware failures (e.g., Crystal River 3), and erroneous hypotheses that indications are not operating correctly (e.g., Oconee 3). Operators also tend to misinterpret indications of actual plant behavior consistently with their wrong mental 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).

Table 5.3-2 also illustrates other possible causes for situation assessment problems, especially the initial development of wrong mental models. In the Oconee 3 shutdown event, an undiscovered pre-accident human failure set up the draining of RCS to the sump which occurred when 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 operators' mental 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 inexperience are the likely causes for their inability to predict how the plant behaved in response to their inappropriate "corrective" actions.

### 5.3.1.3 Response Planning Problems

Five categories of response planning problems are shown in Table 5.3-3:

1) operators follow prepared plans which are not applicable for the specific situation to which they are responding,
2) operators follow prepared plans which are wrong or incomplete,
3) operators do not follow prepared plans,
4) prepared plans do not exist so operators rely upon knowledge-based behavior, and
5) operators inappropriately give priority to one plant function over another.

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

**Table 5.3-3 Examples of Problems in Response Planning**

| Human Impact | Contextual Influence | Event |
|---|---|---|
| Operators follow prepared plans (e.g., procedures), but these plans direct operators to take actions which 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 procedures revisions, regarding the re-start of RCPs without offsite power. (Wrong actions not taken because operator's prior knowledge and experience.)<br>2) Procedure does not contain sufficient detail regarding the tripping of condensate pumps - results in complete loss of condensate flow.<br>3) Early in event, procedures directed operators to close PORV block valves in series, making the PORVs unavailable as relief protection. (Later, during plant cooldown, operators recognize situation and re-open 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 which are inappropriate. | 1) Search for cause of pressure transient is based upon wrong situation assessment and does not discover open PRZR spray valve.<br>2) Operators increase reactor power (more than once) without understanding the cause of RCS pressure transient.<br>3) Operators bypass 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).<br>2) Emergency operating procedures for primary containment control and reactor control do not provide guidance for pressure control with one stuck open relief valve.<br>3) Classroom and simulator training typically used stuck open relief valve as the initiating event for an ATWS. Operators had not been trained for simpler event which occurred (i.e., stuck open safety relief valve followed by successful scram). | Dresden 2 (8/2/90), LOCA (stuck open relief valve). |

**Table 5.3-3 Examples of Problems in Response Planning (Cont'd)**

| Human Impact | Contextual Influence | 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 terminate 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, lack of training and procedural guidance, the shift engineer over-reacts to rising torus temperature and opens turbine bypass valves to reduce heat load, resulting in an unnecessary challenge to the reactor pressure vessel (RPV) pressure control safety function (i.e., excessive cooldown rate).<br>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). |

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 procedural deficiencies were revealed in this event, possibly all 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 which could have terminated the event sooner. Operators also inappropriately used procedural steps (intended for shutdown) for bypassing ESF and automatic actuation of HPI in this event. The justification for this bypass of ESF was that it was reversible and that 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., ATWS with stuck open relief valve). The last category of response planning problems shown in Table 5.3-3 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 regarding rising torus temperature, due to a lack of procedural guidance and their lack of experience and training.

### 5.3.1.4 Response Implementation Problems

Table 5.3-4 shows only three categories of response implementation problems identified in analyzed events:

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

**Table 5.3-4 Examples of Problems in Response Implementation**

| Human Impact | Contextual Influence | Event |
|---|---|---|
| Operators do not check all applicable sections of procedure before exiting - results in omission of important actions. | 1) Operators exit abnormal response procedure because SI termination criteria were met, so they miss 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.<br>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 an unisolable LOCA from the PRZR.<br>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 indications. Hence, two operators were required, one at each panel, in order to perform appropriate HPI control actions.<br>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). |

The Crystal River 3, Dresden 2, and Ft. Calhoun events illustrate each of these problems, respectively. In the Crystal River 3 event, operators transitioned from one procedure to another before the section that would have directed them to take actions which would have terminated the event. Also, operators are trained that it is good practice the 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 which were not appropriate. Finally, operators in the Ft. Calhoun event were hindered by hardware failures and design features which made performance of appropriate response actions difficult.

### 5.3.1.5 Generic Examples of PSFs

Table 5.3-5 is a collection of generalized PSF examples from the five events analyzed, illustrating principally how the more traditional PSFs can impact human performance.

1) human performance capabilities at a low point,
2) time constraints,
3) excessive workload,
4) unfamiliar plant conditions and/or situation,
5) inexperience,
6) non-optimal use of human resources, and
7) environmental factors and ergonomics.

Table 5.3-5 Examples of General Burdens on Cognitive and Physical Abilities

| Human Impact | Contextual Influence | Event |
|---|---|---|
| Human performance capabilities at a low point. | 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 impact 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.<br>2) Event occurred at the beginning of the shift, when awareness is typically high.* | 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 impacted by time constraints. | 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. |
| Excessive workload interferes with operators ability to perform. | 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 STA function of oversight, advice, and assistance to the shift engineer (SE) and, potentially, resulted in some loss of continuity in control room supervision's familiarity with the event circumstances.<br>2) The ability of the shift engineer (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. See "resources" below.) | Dresden 2 (8/2/90), LOCA (stuck open relief valve). |

* Positive, rather than negative, factor in event and on operators' response.

Table 5.3-5 **Examples of General Burdens on Cognitive and Physical Abilities (Cont'd)**

| Human Impact | Contextual Influence | Event |
|---|---|---|
| | 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 shutdown, 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.* | 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. |
| Aspect of the plant or its operation is "new" and unfamiliar to operators. | 1) First time electronic reactor vessel level instrumentation was used - its operation and design are not understood.<br>2) First time draindown was performed with such a high $N_2$ overpressure.<br>3) First time draindown was performed without experienced SE to support draindown operators.<br>4) Decay heat high (~6 MW) because only two days after shutdown. | Prairie Island 2 (2/20/92), loss of RCS inventory and shutdown cooling during shutdown. |
| Operators inexperienced | 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. |

* 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 5.3-5 Examples of General Burdens on Cognitive and Physical Abilities (Cont'd)**

| Human Impact | Contextual Influence | Event |
|---|---|---|
| Non-optimal use of human resources. | 1) When the shift engineer (SE) arrives in the control room, he relieves the shift control room engineer (SCRE), who was in the control room when the SRV opened and who diagnosed the open SRV, so that the SCRE can fulfill the STA role. After this change of duties, the SCRE was completely occupied with other activities (see "workload" above) so he was not able to perform his STA function of oversight, advice, and assistance to the SE and, potentially, resulted in some loss of continuity in control room supervision's familiarity with the event circumstances.<br>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 did not increase 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. | 1) Poor lighting in the area of the tygon tube made taking readings difficult.<br>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. |

In some of the analyzed events, PSFs had an important impact on human performance, particularly in relation to the plant conditions at the time of the event (e.g., excessive workload and poor use of human resources in Dresden 2, inexperience and "new" unfamiliar conditions in Prairie Island 2). In other events, it is not clear that the factors shown in Table 5.3-5 strongly influenced the outcome of the events. However, this table illustrates that such factors can distract operators from critical tasks or drastically hinder or inhibit their ability to perform.

### 5.3.2 Identifying Apparent Causes Not Normally Addressed in PRAs

Using the results of the event analyses documented in Tables 5.3-1 through 5.3-5, the ATHEANA development team generated a generalized list of important aspects of real operational events which are typically overlooked or dismissed in current PRAs. Table 5.3-6 summarizes some of the important lessons which were generated from the event analyses and which were, subsequently, used to support the trial application of ATHEANA. These lessons were used to help generate a broader perspective in the search for the error-forcing context associated with the HFE identified in the trial application described in Section 4. These lessons-learned also are important in developing guidance to simultaneously assist in identifying appropriate HFEs in PRAs which are consistent with operating experience and particularly in overcoming the mindset pervading current HRAs. Even amongst the project 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!"

The first six factors which are shown in Table 5.3-6 are all related to instrumentation problems and how such problems can impact operators and their situation assessment. The seventh factor is essentially a statement of how powerful a wrong situation assessment can be in operators' response to an accident. The eighth factor is relevant to response planning while the ninth factor is relevant to response implementation. The final factor shown in Table 5.3-6 is related to the creation of unusual plant conditions which can fail plant equipment, creating additional tasks for operators, and otherwise hinder the operators' ability to respond to an accident.

## 5.4 Implications of Unsafe Actions Causes for HRA

As illustrated by the results of event analyses shown in Tables 5.3-1 through 5.3-4, most human performance problems appear to be associated with situation assessment and response planning. This is not unexpected since detection problems are likely to be rare (as discussed above) and since many response implementation problems can be easily recognized and corrected. The work of Roth et al. (NUREG/CR-6208) confirms these results, indicating that the differentiator in operator performance is related to situation assessment and, perhaps to a lesser extent, response planning.

In order to meet the definition of a human failure event included in a PRA, unsafe actions must be defined such that actions to recover from them either do not occur or take place too late to avert irreversible consequences. For an unsafe action, there are two possible reasons why the recovery from an unsafe action may not take place: 1) initial problems in information processing must persist until safety is degraded or 2) the initial problem is compounded by or replaced by a new problem(s). Plant dynamics and its timing play an important role in the definition of unsafe action. Focussing upon situation assessment, in particular, the descriptions of causes associated with the above two recovery issues:

1) operators fail to make the appropriate situation assessment, and persist with that misunderstanding, or

2) operators make the appropriate situation assessment, but plant conditions or timing complicate operator performance such that actions cannot be taken in time to avert core damage.

As implied by the first description, it is important to distinguish between persistent failures in situation assessment which could lead to core damage and initial failures which can be later recovered. For example, the "operators (continue to) believe" that high pressure injection is no longer needed in the SLOCA trial application given in Section 4 represents a persistent failure which corresponds to cognitive processing problems identified by Roth et al. (NUREG/CR-6208) Historical experience provides many examples of recovered events (and evidence regarding the causes for these recoveries) but few examples

### Table 5-3.6 Factors Not Normally Considered in PRAs

1. Instrumentation does fail (or is caused to be failed) and fails in many ways, e.g.,
   - indication is high, low, lagging, stuck or miscalibrated
   - pre-accident failures (human and hardware-caused)
   - unavailable due to maintenance, testing, etc.
   - does not exist
2. Instrumentation problems which cause operators to not use it, e.g.,
   - recent or persistent history of reliability/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 indication which 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.
4. Operators typically will believe valve position indicators in spite of contradictory indications.
5. Operators can misunderstand how Instrumentation & Control (I&C) systems work resulting in erroneous explanations for their operation and indication.
6. A history of false/spurious/automatic actions will result in operator "conditioning" to expect these events (especially when re-enforced by management directives), thereby overriding the formal diagnosis required for a "real" event.
7. One plausible explanation can create a "group mindset" for an operating crew.
8. Operators will persist in the recovery of failed systems if, e.g.,
   - 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 (e.g., unexpected I&C re-setting difficulties).
10. Management decisions regarding plant configurations can result in defeated plant defenses and additional burdens on operators, e.g.,
    - 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

of persistent failures. NUREG/CR-6208 describe how some crews never "got it" (i.e., a persistent failure in situation assessment). If, as suggested in NUREG/CR-6208, statistics regarding how often operating crews form correct situation assessments for particular accident scenarios could be generated, then data developed from simulator (and other) events can be used in the quantification process developed in ATHEANA. Also, consistent with the bulk of historical events in which an initial mental model is developed which is revised in recovery, NUREG/CR-6208 describes how some crews "got it" later in the accident, providing a reminder of the importance of timing. NUREG/CR-6208 suggests that most operator crews get several chances to correctly assess the situation (then decide what to do and do it). It also suggests that, given enough time, operators will continue to review information, even looking at additional indications to support their hypotheses. This iterative nature in collecting and interpreting information is already evident in event analyses and is currently being addressed in the development of ATHEANA application tools.

The second description of causes of non-recovery recognizes that the speed at which operators form the correct situation assessment depends on many diverse things, including: 1) timing of the event and its associated alarms and indications, 2) information relied upon, such as indications and other sources of information such as field reports, and 3) PSFs, such as specificity of procedural guidance and training.

Once one of these descriptions is determined to be potentially applicable to an HFE, then error-forcing contexts which satisfy this description can be identified using insights from event analyses, such as those described above. For instance, generic examples from psychological theory and specific examples from real operational events, such as those shown in Tables 5.3-1 through 5.3-5, of contextual factors can be used to develop catalogs of factors which result in different types of information processing problems. However, the tables provided in this section must be supplemented by insights from additional behavioral models and by additional event analyses, including those which have already been performed (e.g., NUREG/CR-6265, HSECS database [Cooper et al., 1995] AEOD ESF Bypass report [AEOD/E95-01]).

# 6. DEVELOPMENTS IN THE PROCESS FOR APPLYING ATHEANA

## 6.1 Introduction

As discussed throughout this report, a critical step in the ATHEANA HRA method is the identification of the most important human failure events (HFEs) to include in the PRA. Previous approaches have allowed the HFEs to fall naturally out of the review of emergency operating procedures, primarily by asking the question: do the operators carry out the actions that their procedures demand? Severe, seemingly inexplicable errors, such as turning off operating safety systems, bypassing start signals, and defeating interlocks are not generally modeled. However, such errors have occurred and often for the best of reasons, namely, the operators' understanding and beliefs concerning the state of the plant and its likely response. One of the required tools for applying ATHEANA is a process which guides the HRA analyst in the search for important and appropriate HFEs to model in the PRA.

Furthermore, traditional approaches to the estimation of the probabilities of HFEs address the question: what is the chance that the humans err, given nominal conditions? The ongoing review of operating events throughout this project indicates that people commit serious mistakes, or actively decide to pursue the wrong course of action, when unusual or atypical conditions conspire to make error very likely. In every serious instance, the mistake was setup by both a complicating physical condition and a complicating human condition (negative performance shaping factor). For example, the plant is in an unfamiliar test configuration and it is 2:00 am. Or, a control system has been out of service for some time (so that the system is being operated manually) but procedures and simulator training are based on automatic actuation, and a more complicated event sequence than expected occurs. Under such conditions, operator failure becomes very likely. Thus, as described earlier, the search for the most risk significant scenarios and their associated HFEs requires a subtle flip in thinking, and involves the search for, and estimation of the likelihood of, the "error-forcing context", rather than predicting random human error in the face of nominal or best-estimate conditions. The concept of search schemes described in this section of the report has been developed with that aim in mind.

Risk-significant HFEs which must be modeled in PRAs include both the significant errors of omission, already identified in PRAs, as well as the new errors of commission (EOCs). For both classes of HFEs, the overall search scheme must address the special contexts that make errors likely; i.e., those combinations of complicating plant conditions and complicating performance shaping factors (PSFs), which together are referred to as error-forcing contexts (EFCs) that make clear thinking difficult. Note, that under the proper EFCs, the HFEs representing errors of omission that are commonly already included in PRA models may have substantially more risk significance than currently believed. Developing a search strategy for significant HFEs based on the consideration of plant conditions and negative PSFs is breaking new ground. At this stage of the project, the search schemes are somewhat conceptual and the details have not been worked out. However, the capability of generating specific cases to add to the PRA has been demonstrated and serves as the precursor to the ATHEANA implementation guidelines which will be developed in future project efforts. As the implementation guidelines are developed and the evidence from specific cases grows, observation of the underlying patterns will permit more thorough and more general identification of HFE/EFC combinations for quantification to be developed.

## 6.2 Defining and Identifying HFEs

Human failure events are the link between the system model (i.e., the PRA) and the HRA. They represent the impact of human failures on plant systems. Based on the experience of the trial application discussed in Section 4, searches for HFEs to include in the PRA will use the PRA structure, engineering analysis, event knowledge, and an identification of potential failures of plant defenses to focus the search for HFEs that can result from rational operator responses.

Current HRA techniques provide little if any concrete guidance for the identification of HFEs, particularly those involving EOCs. Where formal methods exist, current techniques concentrate on identifying errors of omission in response as guided by the appropriate abnormal and emergency operating procedures. In contrast, the ATHEANA method will provide a structured, iterative approach to identifying appropriate post-initiator HFEs to include in the PRA model, including HFEs that represent the results of inappropriate actions (e.g., EOCs) as well as inaction (e.g., EOO). This approach involves a progression from very top level descriptions associated with plant functions to increasingly detailed definitions of potential causes of human error. The goal of this HRA task from the perspective of the PRA model is the same as in current HRA methods, namely to identify and define HFEs with respect to the failure modes of plant equipment. From the perspective of the HRA analyst, however, application of ATHEANA may produce more detailed definitions associated with HFEs that involve different human failure modes than modeled in current HRAs, in particular by adding HFEs that represent the impact of errors of commission.

As in traditional HRA/PRA, the application of ATHEANA will define HFEs based upon the plant functions for each initiator, as specified in the PRA (either implicitly and explicitly). The definitions of HFEs may initially be given at a very high level. For example, "Operator fails Safety Injection" is the high level functional failure associated with the HFE evaluated for the small-break loss-of-coolant accident demonstration described in Section 4. However, depending on the need for more discrimination to handle dependencies, for example, more detailed definitions of specific human failure events can be generated by identifying the unsafe acts that can lead to specific equipment failure modes. For example, "Operator fails ESF" can be decomposed into the unsafe acts "Operator bypasses ESF" and "Operator terminates ESF early." In principle, such decompositions can be determined a priori since the failure modes for equipment are the same whether from human or other causes. Generally, post-initiator EOCs, defined in the context of the PRA logic model structure, will result from one of the following ways in which operators can fail plant functions:

- by turning off running equipment
- by bypassing the signals for automatically starting equipment
- by changing the plant configuration such that interlocks, or other defenses, that are designed to prevent equipment damage are defeated
- by excessive depletion or diversion of plant resources (e.g., water sources)
- by inappropriate initiation of a system
- by inappropriate system control (e.g., over/under-cooling)

The potential set of HFEs, particularly if defined in terms of unsafe acts, can become too large unless some sort of screening is performed. Screening of potential unsafe acts may be appropriate on the basis that the consequences of the failure are insignificant, on the basis that the plant design or configuration prevents the failure mode from being effected, or on the basis that it would require multiple errors that are truly independent. The last condition requires great care because of the potential for EFCs to create modes of dependence. An approach that used such screening approaches was reported in Julius et al., (1995).

Also, not all of these unsafe acts are applicable to every function; some may be precluded in some operational modes and others by design features. Others may be directly seen to be possible unsafe acts. For example, there may be standing orders to terminate a system by blocking the automatic initiation signals, which would make the second of the above unsafe acts appropriate.

## 6.3 Identifying Unsafe Actions and Associated Error-Forcing Contexts

In the prioritization and quantification of the probabilities of the HFEs, whether they are defined at a high level or at the level of an unsafe act, the HRA analyst will need to identify the potential different EFCs which can result in a specific unsafe act. For example, "Operator terminates ESF early" can occur for a variety of different reasons which can be logically explained and described by the combination of error mechanisms and error-forcing contexts. Examples of different causes for "Operator terminates ESF early" are:

- operator inadvertently skips one of the criteria for terminating ESF because of a badly structured procedure and because his workload is high at the time he is required to make the decision,

- operator misreads one of the instruments providing information required for one of the criteria because the normal instrument is unavailable, and the substitute is unfamiliar. Because of this, he erroneously determines that ESF termination criteria are met, and

- operator determines that termination criteria are met, but this determination is based upon faulty or failed instrumentation.

More detailed search schemes will be needed in order to identify the EFCs that might result in one of the unsafe acts associated with the HFEs. For example, searches of procedures can be performed to focus on identifying the specific events and plant conditions for which procedures provide ambiguous, misleading, or erroneous guidance that cause operators to place the plant in a worsened condition. Similarly, the reviews of control room instrumentation can be performed with a focus on the potential for instrumentation to be unavailable to provide needed information or to provide misleading or erroneous information. The absence of, wrong, or misleading information can be the result of instrumentation failures, unavailabilities, lack of redundancy due to either intentional actions (e.g., maintenance, operations being conducted under plant conditions for which instrumentation cannot be used) or inadvertent, pre-accident human failures (e.g., miscalibration), human engineering deficiencies, random failures, or inherent unreliability. Searches of past operating experience, both specific events and generalized insights, should be performed to remind the HRA analyst that "real" events often occur because of a simultaneous combination of multiple hardware and human failures which, even in hindsight, seem incredible (e.g., the twelve hardware failures or malfunctions, including multiple common cause failures, which occurred during the Davis-Besse "Loss of Main and Auxiliary Feedwater Event" (NUREG-1154). Like the reviews of plant functions that form the basis of the search for HFEs, the procedure, instrumentation, and data searches to identify EFCs for potential post-initiator EOCs must be performed in the context of specific initiators and specific plant conditions. Reviews for human engineering concerns may also be relevant. Examples of information sources which could be used to investigate plant conditions are: interviews with trainers (who, from training experience, especially with simulators, know how and what will cause operators to fail), knowledgeable plant staff (especially operations), past operating experience (generic and plant-specific), and thermal-hydraulic analyses (both plant- and vendor-specific).

The approach for identifying EFCs is based on two complementary perspectives: (1) an understanding of error mechanisms and their causes, to identify under what conditions people may be expected to fail (with a high likelihood) and how plant-specific activities and systems could give rise to the error mechanisms; and (2) plant engineering and operations, to identify particular activities and systems of the plant where vulnerabilities may result in core damage. As a parallel to the characterization of the search for HFEs as a human-centered failure-modes-and-effects analysis (FMEA), this search process for the error-forcing context can be characterized as a human-centered HAZOP (Kletz, 1974) analysis.

The first perspective is developed from both a theoretical and a historical basis. The multidisciplinary HRA framework develops a description of the connections between the HFEs, unsafe acts, and error mechanisms and their causes, using the body of knowledge represented by the discipline of behavioral science. Further analyses of operational events provide illustrative examples of combinations of plant conditions and PSFs which resulted in past significant events and which can be generalized and error mechanisms postulated. Together, the HRA framework developments and analyses of historical events provide the basic and general understanding of the elements comprising an error-forcing context which is necessary for the identification of significant events to include in PRAs. As discussed earlier, this knowledge-base will be documented in the ATHEANA FOR manual and the HRA analyst will be guided as to when and which FOR manual information should be used.

The second perspective for identifying EFCs is plant-specific and its associated search processes are focused upon identifying specific plant design features, system configurations, and operational practices that influence the EFCs.

In the trial application described in Section 4, following the identification of the HFE and a specific unsafe act (namely the premature termination of SI), the search proceeded along the following lines. The event scenario was interpreted in the context of the applicable procedure by identifying potential accident scenario transfers and, in particular, the decision criterion associated with termination of SI to understand how an incorrect decision might be set up.

The focus was on errors in situation assessment and the analysis was continued by:

- using thermal-hydraulics analysis to understand how the scenario should appear to the operators
- identifying the source of relevant automatic signals
- identifying potential equipment failures that can affect the scenario or the operators' interpretation of the scenario
- identifying human actions in the scenario that could influence a new set of plant conditions

- identifying other potential activities that may be going on in the control room
- identify hidden system (e.g., I&C) interconnections that when combined with particular plant conditions influence situation assessment.

In this way, a more complete understanding of the HFE and the specific unsafe action chosen for analysis was obtained. In particular, understanding was gained on how, in the nominal case, the event development should have appeared to the operators and the potential ways in which that information could become distorted or misleading, or even ignored. Behind each of the factors that could negatively impact situation assessment, there was an implicit model of the error cause. For example, for an error cause that can be classified as a misdiagnosis, i.e., a failure in situation assessment, there may be several different error mechanisms, each activated by a different set of EFCs.

The overall process followed can be characterized as an attempt to perform the following steps for each HFE:

- Identification of potential unsafe actions (and underlying error mechanisms), and
- Search for the EFCs that could result in the unsafe action (by activating the mechanism)

The next phase in this project is to generalize and formalize the search process into a set of questions that an analyst can use as the basis for a systematic identification of HFEs, unsafe acts, and EFCs which is based on the theoretical concepts and experience base that has been described in this report. This technique of asking a series of questions to structure the search is quite similar to the HAZOP approach developed in the chemical process industry (Knowlton, 1992). The HAZOP uses a multidisciplinary team to examine every aspect of a plant's design by asking questions based on a set of "guide words" that are established to test every conceivable deviation from design intent. The intent of the project team is to focus the questions directly on the identification of EFCs, rather than on error mechanisms which are not observable. The former are directly observable, whereas the latter are not. The error mechanisms are, however, used to help identify the factors that should go into defining the EFCs of concern, and are part of the justification of using the EFCs as surrogates for error causes.

The process described above is open-ended, since a large number of potential HFEs can be identified, and for each of them, EFCs could be developed at greater levels of detail. In order that ATHEANA represents a practical approach to the incorporation of HFEs in PRAs, and that only the risk significant human failures are included in the model, the search process will incorporate guidance for prioritization based on the likelihood and/or impact of the EFCs. In addition, since the EFCs need to be defined only to a sufficient level of detail that quantification of the HFE probabilities and their dependencies can be achieved, the search process will incorporate stopping rules that indicate when the appropriate level of detail has been achieved.

# 7. CONCLUSIONS

This report has introduced and described the ATHEANA HRA method and the first steps in the development of application tools for this new HRA approach. A general process has been developed that addresses the iterative process of defining HFEs and estimating their probabilities using search schemes. Some initial thoughts on search schemes have been presented. The process is supported by the development of a knowledge-base that describes the links between unsafe actions and error-forcing contexts, based on behavioral science literature and on an evaluation of the lessons-learned from major incidents involving human errors at power plants and in other high-technology industries (e.g., aviation). Finally, the ATHEANA method was demonstrated in a trial application, serving as a "proof of concept" for both the method itself and the principles underlying it.

There are several activities that are required to complete the development of ATHEANA. First and foremost, the ATHEANA application tools, the implementation guidelines and frame-of-reference (FOR) manual, must be developed. The precursors to these tools presented in this report have been based on trials on only a few relatively simple example scenarios. The search schemes in particular are rudimentary, and need to be developed to a much more comprehensive level. Also, as with any new method, refinements are to be expected as the problems tackled become larger and more demanding. Thus, larger scale demonstrations, including perhaps application to a full scale PRA, are required to finalize the method development.

In the longer term, work related to supporting users of ATHEANA is required. This work should include supporting the analysis of future significant operational events to ensure that appropriate data are collected to supplement the FOR manual (or identify changes in the framework if necessary). It would also include provision for the sharing of data and experience through a user group, possibly including non-nuclear power experience and users.

## 8. REFERENCES

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

**AEOD** Human Performance Study Reports,

..., **Crystal River Unit 3**, December 8, 1991, *On-Site Analysis of the Human Factors of an Event (Pressurizer Spray Valve Failure)*, U.S. NRC: Washington, DC, January 1992.

..., **Dresden Unit 2**, August, 2 1990, *On-Site Analysis of the Human Factors of an Event (* Stuck Open Safety Relief Valve), U.S. NRC: Washington, DC, October 3, **1992**.

..., **Ft. Calhoun**, July 3, 1992, *On-Site Analysis of the Human Factors of an Event (Stuck Open Pressurizer Code Safety Valve)*, U.S. NRC: Washington, DC, September 25, **1992**.

..., **Oconee Unit 3**, March 8, 1991, *On-Site Analysis of the Human Factors of an Event (Loss of Residual Heat Removal Cooling)*, U.S. NRC: Washington, DC, May **1991**.

..., **Prairie Island Unit 2**, February 20, 1992, *On-Site Analysis of the Human Factors of an Event (Loss of Coolant and Residual Heat Removal Cooling)*, U.S. NRC: Washington, DC, March **1992**.

**AIT** (Augmented Inspection Team) Reports,

..., **Oconee Unit 3**, March 8, 1991, *Loss of Residual Heat Removal*, Report No. 50-287/91-008, U.S. NRC: Washington, DC, April 10, **1991**.

..., **Prairie Island Unit 2**, February 20, 1992, *Loss of Residual Heat Removal*, Report No. 50-306/92-005, U.S. NRC: Washington, DC, March 17, **1992**.

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

**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 Publishing Co.: New York, NY, **1991**.

**Card**, S.K., T.P. Moran, and A. Newell, *The Psychology of Human-Computer Interaction*, Lawrence Erlbaum: Hillsdale, NJ, **1983**.

**Cooper**, S.E., 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**.

**Dougherty**, E.M., **and** J.R. **Fragola**, *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, John Wiley & Sons: New York, NY, **1988**.

**Dougherty**, E.M., *Human Reliability Analysis - Where Shouldst Thou Turn?*, A Guest Editorial, **Reliability Engineering & System Safety**, Vol. 29, No. 3, pp. 283-299, Elsevier Science Publishers Ltd.: England, United Kingdom, **1990**.

**EPRI NP-1982**, *Evaluation of Proposed Control Room Improvements through Analysis of Critical Operator Decisions*, R.W. Pew, D.C. Miller, and C.S. Feehrer, Electric Power Research Institute: Palo Alto, CA, December, **1981**.

**EPRI NP-2330**, *ATWS - A Reappraisal, Part 3: Frequency of Anticipated Transients*, Electric Power Research Institute: Palo Alto, CA, **1982**.

**EPRI NP-3583**, *Systematic Human Action Reliability Procedure (SHARP)*, G.W. Hannaman, and A.J. Spurgin, Electric Power Research Institute: Palo Alto, CA, December **1984**.

**EPRI RP-2170-3**, *Human Cognitive Reliability (HCR) Model for PRA Analysis*, G.W. Hannaman, et al., Electric Power Research Institute: Palo Alto, CA, **1984**.

**EPRI TR-101711**, *A Revised Systematic Human Action Reliability Procedure (SHARP1)*, D.J. Wakefield, Electric Power Research Institute: Palo Alto, CA, December, **1992**.

**Gall**, W., *An Analysis of Nuclear Incidents Resulting from Cognitive Error*, presented at the 11th Advances in Reliability Technology Symposium, University of Liverpool, Elsevier Science Publishers Ltd.: England, United Kingdom, April 1990.

**Gertman**, D.I., **and** H.S. **Blackman**, *Human Reliability and Safety Analysis Data Handbook*, Wiley Interscience: New York, NY, **1994**.

**Gertman**, D.I., Blackman, H.S., Haney, L.N., Seidler, K.S., and Hahn, H.A., *INTENT: A Method for Estimating Failure Rates for Decision Based Errors*, **Reliability Engineering and System Safety**, Vol. 35, No. 2, pp. 127-136, Elsevier Science Publishers Ltd.: England, United Kingdom, **1992**.

**Haas**, P.M., D.W. Whitehead, and D.C. Bley, letter report entitled *Integrated HRA Methodology User Needs Assessment*, Sandia National Laboratories: Albuquerque, NM, August **1994**.

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

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

**Johnson**, W.G., *MORT, The Management Oversight and Risk Tree*, U.S. Atomic Energy Commission: Washington, DC, **1973**.

**Julius**, J.A., E.M. Jorgenson, G.W. Parry, and 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, Vol. 50 pp. 189-201, **1995**

**Kantowitz**, B.H., **and** Y. **Fujita**, *Cognitive Theory, Identifiability and Human Reliability Analysis*, Reliability Engineering & System Safety, Vol. 29, No. 3, pp. 317-328, Elsevier Science Publishers Ltd.: England, United Kingdom, **1990**.

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

**Kirwan**, B., *Human Error Identification in Human Reliability Assessment. Part 1: Overview of Approaches and Part 2: Detailed Comparison of Techniques*, **Applied Ergonomics**, Vol. 23, No. 5, pp. 299-318 (Part 1) and No. 6, pp. 371-381 (Part 2),: **1992**.

**Kletz**, T.A., *HAZOP and HAZAN - Notes on the Identification and Assessment of Hazards*, Institute of Chemical Engineers: Rugby, (England) United Kingdom, **1974**.

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

**Knowlton**, R.E., *An Introduction to Hazard and Operability Studies: The Guide Word Approach*, Chemetics International: Vancouver, Canada, **1992**.

**Mach**, E., *Knowledge and Error*, Reidel Publishing Company: Dordrecht, Germany, **1905**.

**Newell**, A., **and** H.A. **Simon**, *Human Problem Solving*, Prentice-Hall: Englewood Cliffs, NJ, **1972**.

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

**NUREG-1150**, Vol. 1, *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants - Final Summary Report*, U.S. Nuclear Regulatory Commission: Washington, DC, December **1990**.

**NUREG-1154**, *Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985*, U.S. Nuclear Regulatory Commission: Washington, DC, July **1985**.

**NUREG-1250**, Rev. 1, *Report on the Accident at the Chernobyl Nuclear Power Station*, U.S. Nuclear Regulatory Commission: Washington, DC, December **1987**.

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

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

**NUREG-1489**, *A Review of NRC Staff Uses of Probabilistic Risk Assessment*, PRA Working Group, U.S. Nuclear Regulatory Commission: Washington, DC, March **1994**.

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

**NUREG/CR-1278**, *Human Reliability Analysis with Emphasis on Nuclear Power Plants - Final Report*, A.D. Swain and H.E. Guttmann, Sandia National Laboratories: Albuquerque, NM, August **1983**.

**NUREG/CR-2743**, *Procedures for Using Expert Judgment to Estimate Human Error Probabilities in Nuclear Power Plant Operations*, D.A. Seaver and W.G. Stillwell, Idaho National Engineering Laboratory: Idaho Falls, ID, **1983**.

**NUREG/CR-3518**, Vols. 1 & 2, *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment*, D.E. Embrey, P. Humphreys, E.A. Rosa, B. Kirwan, and K. Rea, Brookhaven National Laboratory: Upton, NY, **1984**.

**NUREG/CR-3626**, Vols. 1 and 2, *Maintenance Personnel Performance Simulation (MAPPS) Model: Description of Model Content, Structure, and Sensitivity Testing*, A.I. Siegel, et al., Idaho National Engineering Laboratory: Idaho Falls, ID, **1984**.

**NUREG/CR-3862**, *Development of Transient Initiating Event Frequencies for Use in PRA* Idaho Engineering National Laboratory: EG&G Idaho, May **1985**.

**NUREG/CR-3905, Vol. 1**, *Sequence Coding and Search System (SCSS) for Licensee Event Reports - User's Guide*, N.M. Green and G.T. Mays, Oak Ridge National Laboratory: Oak Ridge, TN, April **1985**.

**NUREG/CR-4550, Vol. 3**, Rev. 1, *Analysis of Core Damage Frequency: Surry Unit 1 Internal Events*, R.C. Bertuccio and J.A. Julius, [of E.I. Services] for Sandia National Laboratories: Albuquerque, NM, April **1990**.

**NUREG/CR-4834**, Vol. 1, *Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP): Volume 1: Development of the Data-Based Method*, L.M. Weston, D.W. Whitehead, and N.L. Graves, Sandia National Laboratories: Albuquerque, NM, June **1987**.

**NUREG/CR-4772**, *Accident Sequence Evaluation Procedure (ASEP) Human Reliability Analysis Procedure*, A.D. Swain, Sandia National Laboratories: Albuquerque, NM, **1987**.

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

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

**NUREG/CR-5534**, *Talent Analysis Linked Evaluation Technique (TALENT) Procedures for Integrating Human Factors Expertise into the PRA Process*, J.E. Wells et al., Lawrence Livermore National Laboratory: Livermore, CA, **1991**.

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

**NUREG/CR-6144**, Vol. 2, *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1: Analysis of Core Damage Frequency from Internal Events During Mid-Loop Operations*, T-L. Chu, Z. Musicki, P. Kohut, D.C. Bley, J. Yang, B. Holmes, G. Bozoki, C. Hsu, D. Diamond, D. Johnson, J. Lin, R. Su, V. Dang, D. Ilberg, S.M. Wong and N. Siu, Brookhaven National Laboratory: Upton, NY, June **1994**.

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

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

**NUS-4159**, *Operator Action Trees (OATs), AN Approach to Quantifying Operator Error Probability During Accident Sequences*, J. Wreathall, NUS Corporation: Gaithersburg, MD, July **1982**.

**NUS-4531**, Rev. 3, *Human Cognitive Reliability (HCR) Model for PRA Analysis*, G.W. Hannaman, et al., NUS Corporation: Gaithersburg, MD, December **1984**.

**Phillips**, L.D., P. Humphreys, and D.E. Embrey, *A Socio-Technical Approach to Assessing Human Reliability (STAHR)*, Technical Report 83-4, Oak Ridge National Laboratory: Oak Ridge, TN, July **1983**.

**Potash**, L.M., M. Stewart, P.E. Dietz, C.M. Lewis, and E.M. Dougherty, *Experience in Integrating the Operator Contributions in the PRA of Actual Operating Plants*, in **Proceedings of the ANS/ENS September 1981 Topical Meeting on Probabilistic Risk Assessment, Port Chester, New York**, Vol. II, pp. 1054-1063, American Nuclear Society: La Grange Park, IL, **1981**.

**Reason**, J.T., *Human Error*, Cambridge University Press: Cambridge, MA, **1990**.

**Rogovin**, M., **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**.

**SECY-94-219**, *Proposed Agency-Wide Implementation Plan for Probabilistic Risk Assessment (PRA)*, U.S. Nuclear Regulatory Commission: Washington, DC, August 19, **1994**.

**SECY-95-079**, *Status Update of the Agency-Wide Implementation Plan for Probabilistic Risk Assessment (PRA)*, U.S. Nuclear Regulatory Commission: Washington, DC, March 30, **1995**.

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

**Senders**, J.W. **and** N.P. **Moray**, *Human Error: Cause, Prediction, and Reduction*, Lawrence Erlbaum Associates: Hinsdale, NJ, **1991**.

**Singh**, A.J., G,W. Parry, and A.N. Beare, *An Approach to the Analysis of Operating Crew Responses for Use in PRAs*, **Proceedings of PSA '93: Probabilistic Safety Assessment International Topical Meeting**, Clearwater Beach, FL, January 27-29, 1993, pp.294-300, American Nuclear Society: La Grange Park, IL, **1993**.

Swain, A.D., *Comparative Evaluation of Methods for Human Reliability Analysis*, GRS-71, Gesellschaft fur Reaktorsicherheit (GRS) mbH: Garching Köln, Germany, **1989**.

**Taylor**, J.M., *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**.

U.S. Nuclear Regulatory Commission, Office of Analysis and Evaluation of Operational Data (AEOD), Human Performance Study Reports - see "**AEOD**" above.

U.S. Nuclear Regulatory Commission, Office of Executive Director of Operations (EDO), SECY-94-219, SECY-95-079, and SECY-95-126 - see "**SECY**" above.

U.S. Nuclear Regulatory Commission, Regional Office, Augmented Inspection Team (AIT) Reports - see "**AIT**" above.

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

**Wickens**, C.D., **and** J.M. **Flach**, *Information Processing*, in **Human Factors in Aviation**, (E.L. Wiener and D.C. Nagel, Eds.), Academic Press: San Diego, CA, **1988**.

**Williams**, J.C., *A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance*, **Proceedings of the 1988 IEEE Fourth Conference on Human Factors and Power Plants, Monterey, California, June 5-9, 1988**, pp 436-450, Institute of Electrical and Electronics Engineers: New York, NY, **1988**.

**Woods**, D.D., 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), The Ohio State University, Wright-Patterson Air Force Base: Columbus, OH, December **1994**.

**Wreathall**, J., and Reason, J.T., *Human Errors and Disasters*, in **Proceedings of the 1992 IEEE Fifth Conference on Human Factors and Power Plants, Monterey, California, June 7-11, 1992**, Institute of Electrical and Electronics Engineers: New York, NY, **1992**.

# APPENDIX A

# HUMAN RELIABILITY ANALYSIS LITERATURE REVIEW

# CONTENTS

## LIST OF TABLES

## A.1 INTRODUCTION

This appendix presents a review of the currently available HRA methods which demonstrates their shortcomings in adequately modeling human response for PRA purposes and justifies the development work being performed by this project. To identify the inadequacies of the existing methods, it is first necessary to consider the intended user needs; i.e., what are the requirements of a fully adequate HRA method. With the needs in plain sight, the capabilities and deficiencies of existing methods can be identified.

## A.2 USER NEEDS

A number of users have been identified for an improved HRA method. The primary user and sponsor of the current work is the U.S. Nuclear Regulatory Commission (NRC), which seeks a more complete way to characterize, regulate and manage the risk from operating nuclear reactors and other activities that they are charged to regulate. Additional users include NRC contractors performing analyses in support of regulation, the owner-operators of facilities regulated by the NRC, owner-operators and regulators of other technological facilities, and HRA/PRA analysts and their expert advisors from related fields.

A set of user needs has been laid out by the NRC in documents relating to its policy on the use of PRA in regulatory activities (SECY-95-126 & SECY-94-219). In those documents , the NRC concludes "...that an overall policy on the use of PRA in nuclear regulatory activities should be established so that the many potential applications of PRA can be implemented in a consistent and predictable manner that promotes regulatory stability and efficiency." The policy has four elements:

- increase the use of state-of-the-art PRA,
- use PRA to reduce unnecessary conservatism; "existing rules and regulations shall be complied with unless revisions to these rules and regulations are made on the basis of the PRA insights",
- PRA should be as realistic as possible with data available for review, and
- use the NRC safety goals with appropriate consideration of uncertainties.

Both these current NRC policy documents and earlier reviews of PRA (e.g., NUREG-1050) reflect on the limits imposed on PRA by current HRA methods and look forward to a time that HRA methods can more fully support PRA applications goals.

Two years ago, when this work was focused on HRA for low power and shutdown conditions, a joint Brookhaven National Laboratory (BNL)/Sandia National Laboratories (SNL) letter report documenting user needs in HRA was prepared (Haas et al., 1994). The specific requirements listed in Table 2.1 were identified and discussed in that report.

During the intervening time, understanding of the factors influencing human reliability in serious accidents has matured through the study of operating events reported in BNL's NUREG/CR-6093, the development of the HRA framework and investigations of methods for the analysis of errors of commission (EOCs) and dependency reported in BNL's NUREG/CR-6265. This work, combined with efforts to develop a quantification process, has led to a restructuring of the priorities of user needs and to the identification of additional needs, including:

- Identification and prioritization of human failure events (HFEs) to include in PRA models. The complete set of HFEs should include both the errors of commission and errors of omission, and should address both those errors which occur in responding to plant disturbances and those which occur during routine activities

- Development of methods for describing the factors, including plant conditions and performance shaping factors (PSFs), that together create an error-forcing context (EFC), i.e., a context that enhances the likelihood of an error.

- Methods for searching for such error-forcing contexts

- Methods for estimating the likelihood of an EFC in the context of a PRA scenario

- Methods for identifying and quantifying the dependencies between HFEs in PRA models

## A.3 EXISTING HRA METHODS

Names and acronyms of methods and techniques related to the performance of an HRA are listed in Table A.2. Not all of these can be considered complete HRA methods, but all address some aspect of HRA. They are included to provide a summary of possibly relevant information. Most of these methods are summarized and evaluated in three references: Gertman and Blackman (1994), Kirwan (1992), and Swain (1989). Because those three documents provide a thorough guide to the literature, extensive references to the methods are not repeated here. The purpose of this section is to identify existing methods and highlight their capabilities vis-a-vis the user needs presented in the previous section, rather than to fully describe and evaluate the methods. The references to most of the methods and techniques in this appendix are contained in Table A.2.

Before identifying the existing methods and discussing how well they address the identified needs, it is helpful to add some structure to the list of methods. First, some of the "methods" are best called processes or structures for guiding the HRA process; e.g., SHARP1 and TALENT.

Next, following the argument presented by Kirwan (1992), it is helpful to draw a distinction between methods for identification of the human failure events (HFEs) and for quantification of those HFEs [i.e., P(HFE)]. A number of methods assist in HFE identification (although not for errors of commission), including CADA, CES, CM, HAZOP, HRMS, MAPPS, Murphy diagrams, PHECA, SHARP1, and THERP.

Finally, it is possible to roughly structure a taxonomy of methods for the estimation of the probabilities of HFEs as follows:

- Methods for manipulating subjective rankings (structured expert judgment) e.g., SLIM, STAHR, PC, CM

- Methods based on task analysis, e.g., THERP, ASEP

- Methods based on event sequence timing and logic, e.g., OAT, ORCA, TRC

- Data-based methods, e.g., HCR, HEART

- Simulation based methods, e.g., MAPPS, SAINT
- Identification of scenario specific PSFs, e.g., EPRI CBDTM

While some of the methods are favorably rated based on a particular author's criteria, Kirwan (1992), Gertman and Blackman (1994), and Swain (1989) identify five problems which are significant with respect to our needs:

- No methods except CES, HAZOP and SHARP1 provide a means for defining a search scheme for actually identifying the HFEs (THERP does find lower level or subsequent HFEs); the others only provide a means for structuring and understanding already identified errors;
- The methods for HFE identification and structuring focus more on being comprehensive than setting priorities for detailed analysis;
- There is little emphasis in the literature on defining HRA methods in the context of PRA (Gertman 1994), with the exception of that provided by Dougherty and Fragola (1988) and SHARP1;
- None of the methods organizes a multidisciplinary view of human reliability, with the possible exception of CREAM;
- Error-forcing contexts (EFCs) are not central to any of the methods. Although, HEART establishes a screening process on a related idea of "error-producing conditions," it lacks the required structure for identifying and quantifying the relevant EFCs. Additionally, CREAM recognizes that performance prediction is linked most strongly to context, but focuses on most likely, rather than most difficult, context.

These are serious problems that must be addressed as indicated below:

**Search Scheme**: A search scheme (or schemes) is (are) essential, especially for identifying errors of commission (EOCs) and potential dependencies between HFEs not previously modeled in PRAs. None of the methods address how to identify EOCs to model in PRAs.

**Comprehensive to the Exclusion of Being Focused**: The emphasis on comprehensiveness can be counter-productive to controlling the level of effort and to focusing the best thinking on the most important problems.

**PRA Context**: For those methods applied to PRA, analysts have found ways to integrate the HRA into PRA, but an early focus on this goal will help manage project resources to produce optimal results.

**Multidisciplinary Framework**: One of the major problems in advancing the state of the art in HRA has been the disarray in communications among experts in the several fields that are involved in human error in the power plants as modeled to support PRAs. Engineers, operations experts, systems analysts, statisticians, risk analysts, psychologists, human factors engineers, and other behavioral scientists have each looked on "error" from their own perspective. All these fields converge on the issue of how humans interact with each other and the machinery of power plants. They need a common language and framework to bring their disparate knowledge to bear on the common problem (NUREG/CR-6265).

**Error-Forcing Context**: Although a few of the methods flag the importance of context, none provides a practical search scheme for identifying and quantifying the error-forcing contexts (EFCs). Because of the importance we now attach to EFC, this point alone means that a new method is required. That perception of importance is based on the simple observation that every serious event in the analyzed operating histories involves both an error-forcing plant context (plant conditions and configuration) and an error-forcing human factors context (negative).

## A.4 SUMMARY

All methods possess some of the attributes needed for the next generation HRA method, but none satisfies all of them. None of these methods focus on EOCs and dependencies between human errors. Most importantly, none of the quantification approaches focuses on identifying or quantifying the likelihood of EFC.

Therefore, in conclusion, it is evident that a new approach for HRA is required in order to:

1) bring the best aspects of existing methods under one umbrella,
2) provide the analyst with on orderly approach for identifying human failure events (HFEs) and EFCs, and
3) elevate consideration of the multidisciplinary nature of the HRA problem and add structure to the judgmental aspects of HRA to obtain consistency and repeatability in the analysis.

Table A.1 User Needs Identified

| |
|---|
| **Dynamic Response**. Realistically represent the dynamic nature of the human-system interaction, including the situation-based response of the operators. |
| **Uncertainties.** Provide guidance and convenient means for identifying, evaluating, tracking and documenting assessment of uncertainties. |
| **Quantification.** Provide guidance for identification and realistic evaluation of:<br>- A limited set of the multiple performance shaping factors affecting human performance<br>- Plant conditions<br>- Errors of commission<br>- Dependencies |
| **Behavioral Science**. Account for the knowledge accumulated in the behavioral sciences. |
| **Consistent with Operating Experience**. Calibrated to be operating event driven and able to model actual operating history. |
| **External Data**. Maintain flexibility to accommodate data from external sources. |
| **Computerization**. Must be possible to implement in a computer-based system that can interface with PRA computer codes. |
| **User Acceptability**. Must meet user acceptance criteria if it is to attain widespread use:<br>- Realistic models (face validity) and results<br>- Appropriate level of complexity<br>- Scrutable and traceable<br>- Consistent and repeatable<br>- Easy to use<br>- Compatible with existing PRA framework<br>- Applicable by different users for different problems<br>- Minimize intellectual, personnel, time, and cost resource requirements |

## Table A.2 Methods Related to HRA
## (Revised version of NUREG\CR-6093's Table 2.4)

| Acronyms | Method | Reference* |
|---|---|---|
| AIPA | Accident Initiation and Progression Analysis | Swain (1989) |
| ASEP | Accident Sequence Evaluation Procedure | NUREG/CR-4772 (1987) |
| CADA | Critical Action and Decision Approach | Gull (1990) |
| CBDTM | Cause Based Decision Tree Method | Singh et al. (1993) |
| CES | Cognitive Environment Simulation | NUREG/CR-5213 (1990) |
| CM | Confusion Matrix | Potash et al. (1981) |
| CREAM | Cognitive Reliability and Error Analysis Method | Hollnagel (1993) |
| DNE/EE | Direct Numerical Estimation/Expert Estimation | Seaver and Stillwell (1983) |
| HAZOP | HAZard and Operability Study | Kletz (1974) |
| HCR | Human Cognitive Reliability model | EPRI RP-2170-3 (1984)<br>NUS-4531 (1984) |
| HEART | Human Error rate Assessment and Reduction Technique | Williams (1988) |
| HRMS | Human Reliability Management System | Kirwan (1992) |
| INTENT | Human error rate assessment for INTENTion-based errors | Gertman et al. (1992) |
| MAPPS | Maintenance Personnel Performance Simulation model | NUREG/CR-3626 (1984) |
| MD | Murphy Diagrams | Pew et al. (1981) |
| MORT | Management Oversight and Risk Tree analysis | Johnson (1973) |
| MSFM | Multiple-Sequential Failure Model | NUREG/CR-2211 (1981) |
| OAT | Operator Action Tree system | Wreathall (1982) |
| ORCA | Operator Reliability Calculation and Assessment | Dougherty (1990) |
| PC | Paired Comparisons | Swain (1989) |
| PHECA | Potential Human Error Cause Analysis | Kirwan (1992) |
| SAINT | Systems Analysis of Integrated Networks of Tasks | Swain (1989) |
| SHARP,<br>SHARP1 | Systematic Human Action Reliability Procedure | EPRI NP-3583 (1984),<br>EPRI TR-101711 (1992) |
| SLIM | Success Likelihood Index Methodology | NUREG/CR-3518 (1984) |
| SRM | Sandia Recovery Model | NUREG/CR-4834 (1987) |
| STAHR | Socio-Technical Approach to assessing Human Reliability | Phillips et al. (1982) |
| TALENT | Task Analysis Linked EvaluatioN Technique | NUREG/CR-5534 (1991) |
| THERP | Technique for Human Error Rate Prediction | NUREG/CR-1278 (1983) |
| TRC | Time-Reliability Correlation | Dougherty and Fragola (1988) |

*NOTE: The Swain (1989) Dougherty and Fragola (1988), Kirwan (1992), and Swain (1989), references here are secondary documents that have already summarized and evaluated the various methods. These secondary documents provide a thorough bibliography of the literature on the methods not directly referenced.

# APPENDIX B

# MULTIDISCIPLINARY HRA FRAMEWORK

# CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

## B.1 INTRODUCTION

As reported in NUREG/CR-6265, a multidisciplinary framework has been developed in order to guide the development of the new HRA method, ATHEANA. This section provides a brief overview of the framework, emphasizing those aspects particularly relevant to the development of the ATHEANA approach. 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.

It is the underlying basis of the framework that human errors occur (for the most part) as a result of combinations of influences associated with the plant conditions and its human factors characteristics that "trigger" error mechanisms in the plant personnel. These error mechanisms are often not inherently "bad" behaviors but are mechanisms that generally allow humans to perform skilled and speedy operations. For example, people often diagnose the cause of an occurrence based on "pattern matching". However, when applied in the wrong context, these mechanisms can lead to inappropriate actions that can unsafe consequences.

Given this basis for the "causes" of human error, what is needed for the development of ATHEANA is a process to identify the likely opportunities for inappropriately triggered mechanisms to cause errors that can have unsafe consequences. The starting point for this search is a framework that seeks to describe the interrelationships between error mechanisms, the plant conditions and performance shaping factors that set these mechanisms, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe.

The graphic description of the framework, illustrating the inter-relationships between unsafe human actions, their impact on the plant, the incorporation of their impact in the PRA model, and the influences of the plant conditions and PSFs on human reliability is presented in Figure B.1. The framework includes elements from the plant operations and engineering perspective, the PRA perspective, the human factors engineering perspective, and the behavioral sciences perspective, all of which contribute to our understanding of human reliability and its associated influences, and has emerged from the review of significant operational events at nuclear power plants (NPPs) by a multidisciplinary project team representing all of these disciplines. The elements included are the minimum necessary set 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 human factors, behavioral science 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 are representative of the understanding needed to describe the underlying causes of unsafe actions. The elements on the right side of the figure, namely the human failure events and the scenario definition, represent the PRA model itself. The unsafe action and human failure event elements represent the point of integration between the HRA and PRA model. The PRA traditionally focuses on the consequences of the unsafe action, which it describes as a human error that is represented by a human failure event. The human failure event is included in the PRA model associated with a particular plant state which defines the specific accident scenarios that the PRA model represents. Each of these framework elements are discussed below.

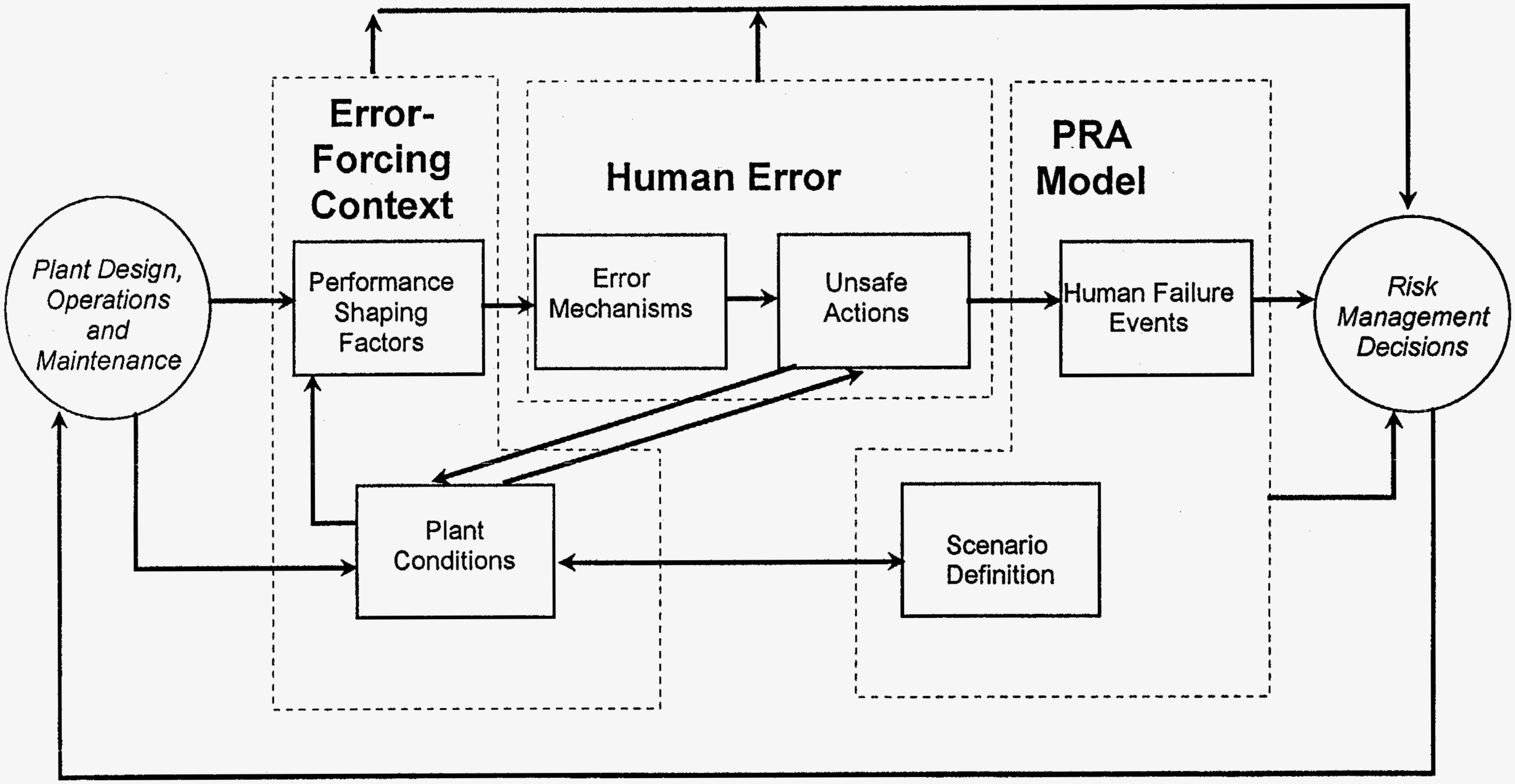

**Figure B.1 Multidisciplinary HRA framework**

## B.2 PRA MODEL

The PRA model identified in the framework is no different from that used in existing PRA methodologies. For the purposes of this project however, the PRA model is an "end-user" of the HRA process. The PRA model provides a means of assessing the risk associated with the NPP operation. The PRA model has, as its basis, logic models, consisting of event trees and fault trees, which are constructed to identify the scenarios that lead to unacceptable plant accident conditions such as core damage. The definition of scenarios is discussed in Section B.2.1.

Included in the structure of the logic models are human failure events (HFEs). When human performance issues are analyzed to support PRA, it is in the context of human failure events applicable to a specific accident scenario defined by the plant state and represented by a PRA logic model. The issues related to HFEs are discussed in Section B.2.2.

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 it is necessary to provide estimates for the probabilities of each of the events of the model, including the HFEs.

### B.2.1 Scenario Definition

PRA scenario definitions provide the minimum descriptions of plant state required to develop the PRA model and define appropriate human failure events. Examples of scenario definition elements include:

- initiating event (e.g., transients, small-break loss-of-coolant accidents (SLOCAs), loss-of-offsite power (LOSP) accidents, etc.)
- 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 (e.g., "small" event tree sequence)
- systemic level (e.g., "large" event tree sequence)
- component state level (cut sets)

Typically, the least detailed scenario definition is that corresponding to the event tree sequence, which identifies the function, or system, or system train status. The most detailed is that of the minimal cut set, which characterizes the accident scenario in terms of component states. However, at any chosen level of detail, the scenarios are defined in terms of a combination of an initiating event and events that represent various failure modes of the equipment and human interactions that are required to respond to the initiating event. As indicated above, the scenarios can be defined at a relatively high level which corresponds to a functional definition, and it is that level of description that is given by the "small" event tree sequence. Event tree sequences define which combinations of system or functional failures following an initiating event (such as a LOCA) lead to the unacceptable outcomes. However, for the purposes of analysis, it is more useful to decompose the description of the system or function failures down to the level of what are called "basic events." The set of basic events includes events that represent the different failure modes of the components and subcomponents that are required for the success of the systems or functions. Included in this set of basic events are events that represent human-caused unavailabilities of these components, systems, or functions. These are the human failure events discussed in detail below. Fault trees or other reliability logic models are used to identify the appropriate combinations or cut sets of basic events that lead to system or functional failures. The ways in which these basic events contribute to core damage scenarios is determined through the integration of the fault trees into the event tree structures.

Human failure events may be associated with an event tree sequence, or with specific cut sets, depending on what the HFE is supposed to represent. 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, therefore, is very much an iterative process.

### B.2.2 Human Failure Events

Human failure events are modeled in the PRA to represent the failure of a function, system, and/or component as a result of an unsafe (human) action(s) which results in a worsened plant condition. A human failure event reflects the PRA systems analysis perspective, and in this context, can be classified as either an error of commission (EOC) or an error of omission (EOO). An error of omission typically represents the failure of an operator to initiate a required safety function. An error of commission represents either the inappropriate termination of a necessary safety function or an initiation of an inappropriate system. Examples of human failure events 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 (ATWS), an EOO. The HFE definition implies a failure to recognize and recover from an error in the time available to successfully fulfill the plant, system, or component function.

In order to appropriately model and quantify the probability of the HFE, it is necessary to identify potential underlying error mechanisms and their associated error-forcing contexts. Since, at least initially, an HFE is defined in terms of its impact on the plant, a single HFE may represent contributions from multiple unsafe actions as will be discussed in the Section B.3.1.

## B.3 HUMAN ERROR

According to Senders and Moray (1991) human error can be characterized as a divergence between an action actually performed and the action that should have been performed, which has an effect (i.e., 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. The framework representation of human error encompasses both the underlying mechanisms of human error and the consequences of error mechanisms, which are the observable unsafe actions. This distinction highlights the associated elements of human error: error mechanisms and unsafe actions, both of which will be further discussed below.

### B.3.1 Error Mechanisms

The error mechanism element illustrated in Figure B.1 represents the cognitive characteristics of human information processing that influence the performance of an unsafe action. These cognitive characteristics can result in the performance of an unsafe action by interfering with an operators':

- detection (monitoring)
- situation assessment
- response planning
- response implementation

The failures in these information processing stages are the result of underlying error mechanisms that impact an operators.

For example, an operator may fail to open a valve in a task for several reasons. First, he may inadvertently skip a step in a procedure requiring the valve to be opened (a response implementation failure). Second, he may misread the valve number in the procedure or on the valve identification label (for example, reversing two digits) and open the wrong one (an attention-related response implementation failure). Third, the operator's mental model of the plant's condition may be wrong, leading him to select the wrong procedure (a situation assessment failure). Fourth, the operator may perform the steps of the procedure out of their written sequence because he perceives that it is better to perform the task that way and, consequently, fail to open the valve at the necessary time (a response planning failure). From the safety perspective and that of PRA modeling, the unsafe action for all of these cognitive failures is "Operator fails to open valve."

Different error mechanisms are primarily associated with different kinds of unsafe actions. For example, failures in situation assessment and response planning are typically associated with mistakes, whereas failures in detection and response implementation are typically associated with slips and lapses. Consequently, the risk impact of the error mechanisms is potentially different according to the risk impacts of the different types of unsafe actions they induce.

It is important to recognize that in most cases these error mechanisms are not intrinsically "bad" modes of human behavior, but rather they are inappropriate for the context in which they occurred. For example, several error mechanisms are associated with taking cognitive "short-cuts" in analyzing particular plant conditions. These are very common behaviors that allow humans to function in highly skilled ways. For example, if operators had to analyze every scenario in a "deep" analytical manner, responses would be long delayed past the onset of plant damage. It is the fact that people (with the aid of training and procedures) can take short cuts in problem analysis and solution generation that normally result in speedy and reliable actions. However, when the scenario does not exactly match the rules or when fatigue or workload predispose excessive "short-cutting", for example, errors can result. In other words, many error mechanisms occur when operators apply normally useful cognitive processes that, in the particular context, are "defeated" or "fooled" by a combination of plant conditions and PSFs and result in an unsafe action.

Error mechanisms are not observable in themselves; only their consequences as unsafe actions can be observed. They serve as mediators between the combined influence of PSFs and plant conditions (i.e., the error-forcing context (EFC)) and unsafe actions. The error mechanisms are included in the framework to explain why different groups of PSFs and plant conditions are associated with different types of unsafe actions, as well as their different importance to safety and risk. By examining these error mechanisms, it is possible to identify the particular impact PSFs and plant conditions have on human reliability and what EFCs should be represented in PRA human failure event definitions.

### B.3.2 Unsafe Actions

The unsafe actions element depicted in Figure B.1 represents those actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition. Unsafe action does not imply that the human was the root cause of the problem. Consequently, this distinction avoids any inference of blame and accommodates the assessment, based on 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 commit an error in the every-day sense of the term; they were doing what was the "correct" thing as it seemed to them at the time.

As has been elaborated in NUREG/CR-6265, there is a distinction between PRA human failure events, defined in terms of EOC and EOO, and the operational event data, defined terms of unsafe act of commission (UAC) and unsafe act of omission (UAO). The UACs and UAOs are human actions identified in historical event data that degraded plant safety. How they relate to the PRA human failure event representation of an EOC or EOO is dependent on the PRA model and associated plant state. This distinction is necessary because not all unsafe action identified in historical events are expected to be modeled as human failure events in the PRA. For example, several unsafe actions could be combined into a single human failure event, while others could be represented in initiating event frequencies or hardware failures.

While not all unsafe actions identified in the analysis of operational events correspond to human failure events as defined in PRAs, in some cases there is a direct correspondence. For example, operators terminating operation of needed engineered safety features would be an unsafe action and should be incorporated as a human failure event in PRAs. More commonly though, unsafe actions represent a "finer" level of detail than most human failure events defined in PRAs. They are often specific to the circumstances in a particular event. For example, in the operational event at Prairie Island Unit 2 in 1992, the unsafe actions included the erroneous calculations which led operators to fail to terminate draindown before suction to the residual heat removal (RHR) cooling loop was lost. The actual unsafe actions were two rule-based mistakes in level calculation while draining down the reactor pressure vessel. However, from the PRA perspective, the human failure event (defined in the context of a PRA model) would be an operator-induced loss-of-coolant accident (LOCA) during draindown to midloop, with a consequential loss of core cooling.

A particular attribute of unsafe actions is that they can be classified according to a simple taxonomy of unsafe action types developed by Reason (1990). These unsafe action types are slips and lapses, mistakes, and circumventions. Each type is distinct in its (1) potential impact on safety and (2) causal factors. Each type is summarized below.

Slips and lapses are unsafe actions where the outcome of the action was not what the person performing the action intended. Skipping a step in a procedure or transposing the numbers of an identification label are examples of lapses and slips, respectively. Both are errors associated with what Rasmussen (1981) has termed "skill-based" level of performance. This level of performance is associated with routine and highly practiced actions. The significance to risk of these unsafe actions seems to be quite small for the simple fact that these actions, not being as the "actor" intended, are often easily recognized by the person involved and (in most circumstances) easily corrected.

For unsafe actions where the action was as intended, there are two broad classes; mistakes and circumventions. Mistakes relate to intentional actions in which the intention is wrong. The mistake (erroneous intention) can be considered "rule-based" or "knowledge-based" depending on whether the task is demanding rule-based or knowledge-based performance. For rule-based performance, documented, task-specific instructions are being followed (usually contained in procedures for almost all NPP activities important to safety). A rule-based mistake therefore represents an unsafe action performed while following procedural guidance which is inadequate for, or technically correct but not applicable to, the current situation (e.g., procedure inappropriately selected based on an erroneous diagnosis). For knowledge-based performance, the person involved is relying on technical or specialist knowledge (as in generalized troubleshooting). A knowledge-based mistake therefore represents an unsafe action performed under unusual circumstances while relying on ingrained but deficient technical knowledge with no direct procedural guidance available.

Mistakes are perhaps the most significant to risk because they are being followed purposefully by the human who may have limited cues that there is a problem based on an erroneous diagnosis. Indeed, indications contradicting the erroneous diagnosis are often dismissed for example as "instrument errors." In many circumstances, it takes an outsider to the situation to identify the nature of the problem, as experienced at TMI-2 when the next shift of operators arrived.

Circumventions are intended unsafe actions, where a person decides to break some rule (even though the rule is known to them) for what seems to be a good (or at least benign) reason. The intention to ignore the known rule is usually based on the perception that the circumvention will have little or no impact on plant safety (for example, purposely reversing the steps in a procedure to simplify or shorten a task). Circumventions are potentially significant contributors to risk in that unanalyzed plant conditions can result from unexpected combinations of circumventions and other unsafe actions or equipment failures. However, a condition that seems to mitigate this potential is that the person committing the circumvention is (usually) aware of its occurrence and can take mitigating actions to restore safe operation of the plant. In the current environment in the nuclear industry, circumventions seem to be a rarely reported incident which may reflect a low rate of occurrence. However, recent simulation tests (NUREG/CR- 6208) indicate that they may be quite common, but not considered reportable. It should be noted that circumventions are distinct from acts of sabotage since they are not intended to cause damage.

## B.4 ERROR-FORCING CONTEXT

An error-forcing context (EFC) represents the combined effect of performance shaping factors (PSFs) and plant conditions that create a situation in which human error is likely.

An example is demonstrated by the February 1992 loss of reactor residual heat removal event at Prairie Island. In that event, a high $N_2$ overpressurization during reactor coolant system draindown two days after shutdown rendered draindown procedures and level instrumentation inadequate, resulting in an inevitable operator overdraining error. This example illustrates the significant influence an EFC has on human reliability. It is often observed in operating experience that deficiencies in PSFs (e.g., procedure and training limitations) are often inconsequential until particular plant conditions exacerbate the deficiencies, thereby creating a context that poses difficult challenges to human information processing and response implementation. Thus the EFC creates a situation which can activate a human error mechanism.

Recent discussions with those who have analyzed transportation and aviation accidents (e.g., NTSB, 1994) and review of accidents at chemical plants (e.g., Kletz, 1984) indicate that an error-forcing context is most often present in serious accidents involving human operational control in these industries. These contexts are not explicitly modeled in existing PRAs.

Analysis of NPP operating events reveals that the error-forcing context typically represents an unanalyzed plant condition that is beyond normal operator training and/or procedure 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 condition and PSFs are combined with internal psychological factors, they can lead to the refusal to believe evidence that runs counter to the initial misdiagnosis or a failure to recognize that evidence, resulting in subsequent mistakes (i.e., errors of commission), and ultimately, an accident with catastrophic consequences.

The following subsections discuss the PSF and plant conditions components of the error-forcing context.

### B.4.1 Performance Shaping Factors

As depicted in Figure B.1, performance shaping factors (PSFs) represent influences on both the occurrence and type of human error mechanisms during, for example, operations, testing, and maintenance activities. To date, the PSFs primarily used in this project are those identified in the Human Performance Investigation Process (HPIP) (NUREG/CR-5455) and pertain to procedures, training, communications, supervision, staffing, human-machine interface, organizational factors, as well as stress and 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) which influences, for example, a failure in situation assessment or response planning.

Given the differences between the possible error mechanisms that could be the cause of an unsafe action, the use of a single set of PSFs for all types of error mechanisms and unsafe actions is inappropriate. Rather, each error mechanism has a primary set of PSFs associated with it. Some basic relationships between error mechanisms and sets of PSFs are identified in Table B.1.

**Table B.1 Primary PSFs Associated with Each Information Processing Stage**

| Information Processing Stage | PSFs Examples |
|---|---|
| Detection Failures | Workload, Stress, human-machine interface (e.g., instrument displays), Environmental Conditions |
| Situation Assessment Failures | Training, Procedures, Communication |
| Response Planning Failures | Training, Procedures, Supervision |
| Response Execution Failures | Human-machine interface (e.g., controls layout), Procedures, Communication |

### B.4.2 Plant Conditions

The plant conditions element of the framework represents those plant factors that might have an influence on the operators' performance. These factors include: the plant configuration (e.g., system, component, or instrumentation & control status, both availability and reliability); process parameters (e.g., core reactivity, power level, and reactor coolant system temperature, pressure and inventory); and other factors including: off-nominal and/or dynamic conditions which result in unusual plant configurations and behavior. Some examples of off-nominal plant conditions include:

- A 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;
- Blind flange installed on wrong line in the March 1991 Oconee Unit 3 loss of reactor coolant system inventory event.

Plant configuration, relevant process parameters, recent performance history of equipment and instrumentation and off-nominal and/or dynamic conditions (which result in unusual or changing plant configurations and behavior) have all been reported in operating events (e.g., NUREG-1275, Vol. 8) to impact human performance (e.g., influence the importance of particular PSFs) and are relevant to both PRA accident scenario definitions and error-forcing context definitions. Consequently, plant conditions can influence the types of activities being performed, characterize the circumstances under which they are performed, and influence human reliability when performing them.

Plant conditions also play a critical role in developing the PRA model. For example, they are used to develop the scenario definitions associated with different initiating events, such as LOCA, LOOP, or ATWS events. The operating conditions captured by the scenario definitions represent system, equipment, and, sometimes, instrumentation availability and/or reliability which establishes what actions the operators should take and the resources available to perform the identified plant operations. Other aspects of plant conditions are not captured explicitly in scenario definitions as such but may play a significant role in determining which unsafe actions may occur and how likely they are to occur. One such aspect is the performance history of equipment and instrumentation (e.g., a leaky PORV or a frequently false positive radiation monitor) which have been found in operating events to influence human performance in both the initiation of, and response to, an event (e.g., TMI-2). Therefore, while those plant conditions that are encapsulated in the scenario definitions can be regarded as defining the boundary conditions for the HFEs, those that are not captured must be addressed by the HRA method itself.

Based on the analysis of operating events, most difficulties in human performance occur when an activity or task is being performed under unfamiliar plant conditions, rather than the design basis conditions typically assumed in, for example, task analyses by human factors engineers. The unfamiliar conditions then result in the normally adequate human factors design features (e.g., PSFs related to training, procedures, and HMI) being inadequate or even misleading during activities performed under the unusual conditions (e.g., high $N_2$ overpressurization in the 1992 Prairie Island event).

The implication of plant conditions on HRA is further illustrated in the following example. Draindown operations in a PWR refueling outage requires many manual actions by operators (often under conditions of limited indications and alarms), whereas maintaining a reactor at full power requires only a few manual actions (such as performing surveillance tests). To some degree these conditions are implicit in the plant state defined in the PRA. However, the specific human interactions with the plant are not typically defined in the PRA, especially for actions leading to initiating events or other EOCs.

NRC FORM 335
(2-89)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

# BIBLIOGRAPHIC DATA SHEET

*(See instructions on the reverse)*

1. REPORT NUMBER
**(Assigned by NRC. Add Vol., Supp., Rev., and Addendum Numbers, if any.)**

NUREG/CR-6350
BNL-NUREG-52467

2. TITLE AND SUBTITLE

A Technique for Human Error Analysis (ATHEANA)
Technical Basis and Methodology Description

3 DATE REPORT PUBLISHED

| MONTH | YEAR |
|---|---|
| May | 1996 |

4. FIN OR GRANT NUMBER
L 2415

5. AUTHOR(S)

S.E. Cooper, SAIC, A.M Ramey-Smith, NRC, J. Wreathall, WWG, G.W. Parry, NUS, D.C. Bley, WWG, W.J. Luckas, BNL, J.H. Taylor, BNL, M.T. Barriere, BNL

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION – NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000

9. SPONSORING ORGANIZATION – NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Systems Technology
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, D.C. 20555-0001

10. SUPPLEMENTARY NOTES

A. M. Ramey-Smith, NRC Project Manager

11. ABSTRACT *(200 words or less)*

Probabilistic risk assessment (PRA) has become an important tool in the nuclear power industry, both for the Nuclear Regulatory Commission (NRC) and the operating utilities. Human reliability analysis (HRA) is a critical element of PRA; however, limitations in the analysis of human actions in PRAs have long been recognized as a constraint when using PRA.

A multidisciplinary HRA framework has been developed with the objective of providing a structured approach for analyzing operating experience and understanding nuclear plant safety, human error, and the underlying factors that affect them. The concepts of the framework have matured into a rudimentary working HRA method. A trial application of the method has demonstrated that it is possible to identify potentially significant human failure events from actual operating experience which are not generally included in current PRAs, as well as to identify associated performance shaping factors and plant conditions that have an observable impact on the frequency of core damage.

A general process was developed, albeit in preliminary form, that addresses the iterative steps of defining human failure events and estimating their probabilities using search schemes. Additionally, a knowledge-base was developed which describes the links between performance shaping factors and resulting unsafe actions.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Failure Mode Analysis, Human Factors Engineering, Knowledge-Base Operations Research, Performance, Probabilistic Estimation, Reactor Operation, Reactor Safety.

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

*(This Page)*

Unclassified

*(This Report)*

Unclassified

15. NUMBER OF PAGES

16. PRICE

Printed
on recycled
paper

Federal Recycling Program